A Dichotomy in p-adic Dynamics: Measure-preservation of 1- Lipschitz functions vs Bernoullicity of expansive functions

Sangtae Jeong

Department of Mathematics

Inha University

stj@inha.ac.kr

Sixth International Conference on p-adic Mathematical Physics and its Applications
CINVESTAV, Mexico City, October 23rd-27th 2017

2017. 10. 24

Outline

1. Goal of the Talk and Introduction
2. Non-Archimedean dynamical systems on two local rings: $\mathbb{Z}_p$ vs $\mathbb{F}_q[[T]]$
3. Two bases of Mahler and van der Put
4. Conjecture A and known results
5. Lemmas for Main Theorem and its proof
6. Bernoullicity of p^α-Lipschitz functions on $\mathbb{Z}_p$
7. Root existence of 1-Lipschitz functions on $\mathbb{Z}_p$

Goal of the Talk and Introduction

• We introduce basics of dynamics on non-Archimedean local rings ($\mathbb{Z}_p$ or $\mathbb{F}_q[[T]]$). Non-Archimedean dynamical systems are classified as a dichotomy between 1-Lipschitz functions and expansive functions.

• We formulate a conjecture for the measure-preservation of a 1-Lipschitz function on $\mathbb{Z}_p$ in Mahler's expansion.

• In this talk, we provide evidence for this conjecture by verifying that it holds for a wider class of 1-Lipschitz functions that are uniformly differentiable modulo p on $\mathbb{Z}_p$ of $N_1(f) = 1$.

Goal of the Talk and Introduction

- We introduce basics of dynamics on non-Archimedean local rings ($\mathbb{Z}_p$ or $\mathbb{F}_q[[T]]$). Non-Archimedean dynamical systems are classified as a dichotomy between 1-Lipschitz functions and expansive functions.

- We formulate a conjecture for the measure-preservation of a 1-Lipschitz function on $\mathbb{Z}_p$ in Mahler's expansion.

- In this talk, we provide evidence for this conjecture by verifying that it holds for a wider class of 1-Lipschitz functions that are uniformly differentiable modulo p on $\mathbb{Z}_p$ of $N_1(f) = 1$.

Goal of the Talk and Introduction

• We introduce basics of dynamics on non-Archimedean local rings ($\mathbb{Z}_p$ or $\mathbb{F}_q[[T]]$). Non-Archimedean dynamical systems are classified as a dichotomy between 1-Lipschitz functions and expansive functions.

• We formulate a conjecture for the measure-preservation of a 1-Lipschitz function on $\mathbb{Z}_p$ in Mahler's expansion.

• In this talk, we provide evidence for this conjecture by verifying that it holds for a wider class of 1-Lipschitz functions that are uniformly differentiable modulo p on $\mathbb{Z}_p$ of $N_1(f) = 1$.

Goal of the Talk and Introduction

• Also we formulate a conjecture for a Bernoullicity of expansive maps on $\mathbb{Z}_p$ in Mahler's expansion and then verify that this conjecture holds for a wider class of expansive maps satisfying certain assumptions.

• If time permits, we will use the results of Yurova and Khrennikov to provide a generalized Hensel's lifting lemma for 1-Lipschitz functions on $\mathbb{Z}_p$ in terms of Mahler's coefficients.

Goal of the Talk and Introduction

- Also we formulate a conjecture for a Bernoullicity of expansive maps on $\mathbb{Z}_p$ in Mahler's expansion and then verify that this conjecture holds for a wider class of expansive maps satisfying certain assumptions.

- If time permits, we will use the results of Yurova and Khrennikov to provide a generalized Hensel's lifting lemma for 1-Lipschitz functions on $\mathbb{Z}_p$ in terms of Mahler's coefficients.

Non-Archimedean dynamical systems

What are non-Archimedean dynamical systems?

• Non-Archimedean dynamical system is made up of a triple (R, f, μ) where

$-R$: a compact discrete valuation domain with a uniformizer π;

i) $\mathbb{Z}_p$ is the ring of p-adic integers.

ii) $\mathbb{F}_q[[T]]$ is the ring of power series in one variable T over a finite field $\mathbb{F}_q$.

$-f$: a measurable(continuous) function $f : R \to R$.

$-\mu$: a normalized measure on R so that $\mu(R) = 1$.

• Recall that the measure of a ball $a + \pi^n R$ is defined as its radius; $\mu(a + \pi^n R) = 1/r^n$, $r = \#R/(\pi)$, where r is given by

$$r = \begin{cases} p & \text{if } R = \mathbb{Z}_p; \\ q & \text{if } R = \mathbb{F}_q[[T]]. \end{cases}$$

Dichotomy: 1-Lipschitz functions vs expansive functions

Fix a nonnegative integer α.

• **[Definition]** r^α-Lipschitz functions on R :

We say that $f : R \to R$ is r^α-Lipschitz if one of the equivalent statements is satisfied:

(1) $|f(x) - f(y)|_\pi \leq r^\alpha \cdot |x - y|_\pi$ for all $x, y \in R$.

(2) $f(x) \equiv f(y) \pmod{\pi^n}$ whenever $x \equiv y \pmod{\pi^{n+\alpha}}$ for any integer $n \geq 1$.

(3) $f(x + \pi^{n+\alpha} R) \subset f(x) + \pi^n R$ for all $x \in R$ and any integer $n \geq 1$.

(4) $|\Phi_1(f) := \frac{1}{x}(f(x+y) - f(y))|_\pi \leq r^\alpha$ for all $x \neq \in R$ and all $y \in R$.

(5) $||\Phi_1(f)||_{\sup} \leq r^\alpha$ for all $x \neq 0 \in R$.

Then, every r^α-Lipschitz function induces reduced functions, for all integers $n \geq 1$

$$f_{/n} : R/\pi^{n+\alpha} R \to R/\pi^n R,$$

$$x + \pi^{n+\alpha} R \mapsto f(x) + \pi^n R.$$

Dichotomy: 1-Lipschitz vs expansive functions

[**Definition**] • $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be a 1 -Lipschitz function if $\alpha = 0$, p^α-expansive/Lipschitz if $\alpha > 0$.

• Examples of 1-Lipschitz functions on $\mathbb{Z}_p$.
1. $\mathbb{Z}_p[x]$.
2. $\mathbf{B}(\mathbb{Z}_p)$:= the set of locally analytic functions of order 1 from $\mathbb{Z}_p$ to itself.
3. $Udm(\mathbb{Z}_p)^{(1)}$:= the set of 1-Lipschitz, uniformly differentiable modulo p functions on $\mathbb{Z}_p$ of $N_1(f) = 1$.

• Examples of p^α-expansive functions on $\mathbb{Z}_p$.
1. $\binom{x}{n}$ is a $p^{\lfloor \log_p(n) \rfloor}$-expansive function.
2. Fermat quotient map on $\mathbb{Z}_p$ defined by $F(x) = \frac{x^p - x}{p}$ is a p-expansive function.
3. The generalised Collatz map $\phi_{p,q}(x)$ is p-expansive, where

$$\phi_{p,q}(x) = \begin{cases} \frac{x}{p} & \text{if } p \mid x \\ \frac{qx - \varepsilon_0(qx)}{p} & \text{otherwise} \end{cases}$$

Dichotomy: 1-Lipschitz vs expansive functions

[**Definition**] • $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be a 1 -Lipschitz function if $\alpha = 0$, p^{α}-expansive/Lipschitz if $\alpha > 0$.

• Examples of 1-Lipschitz functions on $\mathbb{Z}_p$.
1. $\mathbb{Z}_p[x]$.
2. $\mathbf{B}(\mathbb{Z}_p) :=$ the set of locally analytic functions of order 1 from $\mathbb{Z}_p$ to itself.
3. $Udm(\mathbb{Z}_p)^{(1)} :=$ the set of 1-Lipschitz, uniformly differentiable modulo p functions on $\mathbb{Z}_p$ of $N_1(f) = 1$.

• Examples of p^{α}-expansive functions on $\mathbb{Z}_p$.
1. $\binom{x}{n}$ is a $p^{\lfloor \log_p(n) \rfloor}$-expansive function.
2. Fermat quotient map on $\mathbb{Z}_p$ defined by $F(x) = \frac{x^p - x}{p}$ is a p-expansive function.
3. The generalised Collatz map $\phi_{p,q}(x)$ is p-expansive, where

$$\phi_{p,q}(x) = \begin{cases} \frac{x}{p} & \text{if } p \mid x \\ \frac{qx - \varepsilon_0(qx)}{p} & \text{otherwise} \end{cases}$$

Basic Facts in π-adic dynamical systems

For two cases $(R, \pi, |?|_\pi) = (\mathbb{Z}_p, p, |?|_p)$ or $(\mathbb{F}_q[[T]], T, |?|_T)$
[Definition] (1) A function $f : R \to R$ is measure-preserving if $\mu(f^{-1}(M)) = \mu(M)$ for each measurable subset $M \subset R$, especially, $M = a + \pi^n R (n \geq 0)$.

(2) A measure-preserving function $f : R \to R$ is called ergodic if it has no proper invariant subsets, i.e., if, for an invariant measurable subset $M \subset R$, i.e., $f^{-1}(M) = M$, either $\mu(M) = 1$ or $\mu(M) = 0$ holds.

Proposition 1
Let $f : R \to R$ be a 1-Lipschitz function.
Then $f : R \to R$ is measure-preserving.
$\Leftrightarrow$ its reduced functions $f_{/n} : R/\pi^n R \to R/\pi^n R$ are bijective for all integers $n \geq 1$.
$\Leftrightarrow$ f is an isometry; $|f(x) - f(y)|_\pi = |x - y|_\pi$ for all $x, y \in R$.
$\Leftrightarrow$ f is onto.

Basic Facts in π-adic dynamical systems

For two cases $(R, \pi, |?|_\pi) = (\mathbb{Z}_p, p, |?|_p)$ or $(\mathbb{F}_q[[T]], T, |?|_T)$
[Definition] (1) A function $f : R \to R$ is measure-preserving if $\mu(f^{-1}(M)) = \mu(M)$ for each measurable subset $M \subset R$, especially, $M = a + \pi^n R (n \geq 0)$.

(2) A measure-preserving function $f : R \to R$ is called ergodic if it has no proper invariant subsets, i.e., if, for an invariant measurable subset $M \subset R$, i.e., $f^{-1}(M) = M$, either $\mu(M) = 1$ or $\mu(M) = 0$ holds.

Proposition 1

Let $f : R \to R$ be a 1-Lipschitz function.
Then $f : R \to R$ is measure-preserving.
$\Leftrightarrow$ its reduced functions $f_{/n} : R/\pi^n R \to R/\pi^n R$ are bijective for all integers $n \geq 1$.
$\Leftrightarrow$ f is an isometry; $|f(x) - f(y)|_\pi = |x - y|_\pi$ for all $x, y \in R$.
$\Leftrightarrow$ f is onto.

Equivalent statements for ergodic functions

Proposition 2

A 1-Lipschitz function $f : R \to R$ is ergodic if and only if its reduced functions $f_{/n} : R/\pi^n R \to R/\pi^n R$ are transitive for all integers $n \geq 1$.
(• transitive = forming a cycle by repeating f)

Proposition 3

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be an onto(MP-preserving) 1-Lipschitz function. Then the following are equivalent:
(1) f is minimal, meaning $\mathcal{O}_f(x)$ is dense in $\mathbb{Z}_p$ for every $\in \mathbb{Z}_p$.
(2) f is ergodic.
(3) f is conjugate to the translation $t(x) = x + 1$ on $\mathbb{Z}_p$.
(4) f is uniquely ergodic, meaning there is only one ergodic measure.

Equivalent statements for ergodic functions

Proposition 2

A 1-Lipschitz function $f : R \to R$ is ergodic if and only if its reduced functions $f_{/n} : R/\pi^n R \to R/\pi^n R$ are transitive for all integers $n \geq 1$.

($\bullet$ transitive $=$ forming a cycle by repeating f)

Proposition 3

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be an onto(MP-preserving) 1-Lipschitz function. Then the following are equivalent:

(1) f is minimal, meaning $\mathcal{O}_f(x)$ is dense in $\mathbb{Z}_p$ for every $\in \mathbb{Z}_p$.

(2) f is ergodic.

(3) f is conjugate to the translation $t(x) = x + 1$ on $\mathbb{Z}_p$.

(4) f is uniquely ergodic, meaning there is only one ergodic measure.

p^α-Bernoulli functions:=$(p^{-\alpha}, p^\alpha)$-locally scaling functions

Definition

We say that for a positive integer α, a p^α-expansive function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is p^α-Bernoulli if, for all $x, y \in \mathbb{Z}_p$ such that $x \equiv y \pmod{p^\alpha}$,

$$|f(x) - f(y)| = p^\alpha |x - y|.$$

Examples of Bernoulli functions on $\mathbb{Z}_p$:

1. $\binom{x}{p^\alpha}$ is p^α-Bernoulli.
2. Fermat quotient map $F(x) = \frac{x^p - x}{p}$ is p-Bernoulli.
3. The generalised Collatz map $\phi_{p,q}(x)$ defined by

$$\phi_{p,q}(x) = \begin{cases} \frac{x}{p} & \text{if } p \mid x \\ \frac{qx - \varepsilon_0(qx)}{p} & \text{otherwise} \end{cases}$$

is p-Bernoulli.

p^α-Bernoulli functions:=$(p^{-\alpha}, p^\alpha)$-locally scaling functions

Definition

We say that for a positive integer α, a p^α-expansive function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is p^α-Bernoulli if, for all $x, y \in \mathbb{Z}_p$ such that $x \equiv y \pmod{p^\alpha}$,

$$|f(x) - f(y)| = p^\alpha |x - y|.$$

Examples of Bernoulli functions on $\mathbb{Z}_p$:

1. $\binom{x}{p^\alpha}$ is p^α-Bernoulli.
2. Fermat quotient map $F(x) = \frac{x^p - x}{p}$ is p-Bernoulli.
3. The generalised Collatz map $\phi_{p,q}(x)$ defined by

$$\phi_{p,q}(x) = \begin{cases} \frac{x}{p} & \text{if } p \mid x \\ \frac{qx - \varepsilon_0(qx)}{p} & \text{otherwise} \end{cases}$$

is p-Bernoulli.

Dynamical properies of p^α-Bernoulli functions

Theorem (Kingsbery et al.)

If f is a p^α-Bernoulli function on $\mathbb{Z}_p$, then f is topologically and measurably isomorphic to $S^{(\alpha)}$, where $S^{(\alpha)}$ is the αth iterate of the shift map S on $\mathbb{Z}_p$ defined by $S(x) = \frac{x - x_0}{p}$, where $x = x_0 + x_1 p + \cdots$,

Definition

Two functions $f : \mathbb{Z}_p \to \mathbb{Z}_p$ and $g : \mathbb{Z}_p \to \mathbb{Z}_p$ are said to be topologically isomorphic if there exists a homeomorphism $\Phi : \mathbb{Z}_p \to \mathbb{Z}_p$ such that, for all $x \in \mathbb{Z}_p$,

$$\Phi \circ f(x) = g \circ \Phi(x). \tag{1}$$

The maps are measurably isomorphic if there exists an invertible, measure-preserving map Φ such that (1) holds for almost all $x \in \mathbb{Z}_p$.

Dynamical properies of p^α-Bernoulli functions

Theorem (Kingsbery et al.)

If f is a p^α-Bernoulli function on $\mathbb{Z}_p$, then f is topologically and measurably isomorphic to $S^{(\alpha)}$, where $S^{(\alpha)}$ is the αth iterate of the shift map S on $\mathbb{Z}_p$ defined by $S(x) = \frac{x-x_0}{p}$, where $x = x_0 + x_1 p + \cdots$,

Definition

Two functions $f : \mathbb{Z}_p \to \mathbb{Z}_p$ and $g : \mathbb{Z}_p \to \mathbb{Z}_p$ are said to be topologically isomorphic if there exists a homeomorphism $\Phi : \mathbb{Z}_p \to \mathbb{Z}_p$ such that, for all $x \in \mathbb{Z}_p$,

$$\Phi \circ f(x) = g \circ \Phi(x). \tag{1}$$

The maps are measurably isomorphic if there exists an invertible, measure-preserving map Φ such that (1) holds for almost all $x \in \mathbb{Z}_p$.

Applications from relations with other areas

• Non-Archimedean dynamical system(NADS) has many applications to mathematical physics, computer science, cryptography, and so on. In particular, it can be applied to cryptography in order to generate pseudo-random numbers(PRNG).

• Reference: **"Applied Algebraic Dynamics"** by Vladimir Anashin and Andrei Khrennikov

• **One-to-one correspondence** between NADS and other area(in a broad sense)

NADS	Automata Theory	Cryptography	Quantum M.
1-Lipschitz fun.	Autonomous fun.	T-fun.	Causality law
MP fun.	Reversible transd.	Bijective fun.	Reversible law
Ergodic fun.	?	Transitive fun.	?

Problems in non-Archimedean dynamics

Problems to be tackled:

For $(R, \pi, |?|_\pi) = (\mathbb{Z}_p, p, |?|_p)$ or $(\mathbb{F}_q[[T]], T, |?|_T)$,
we want to characterize dynamical properties of two types of functions $f : R \to R$;
(1) Measure-preservation/Ergodicity of a 1-Lipschitz function f
(2) Bernoullicity/Measure-preservation/Ergodicity of an expansive function f
in terms of expansion coefficients $\{a_n\}_{n\geq 0}$ of f expressed as

$$f(x) = \sum_{n=0}^{\infty} a_n e_n(x)$$

where $\{e_n\}_{n\geq 0}$ is an orthonormal basis of the space $C(R, K)$ of continuous functions on R to K.

Bases for the space $C(R, K)$

• R: the integer ring of a local field K :
Here we are interested in two cases $(R, \pi, |?|_\pi) = (\mathbb{Z}_p, p, |?|_p)$ or $(\mathbb{F}_q[[T]], T, |?|_T)$

• $C(R, K)$: the space of all continuous functions from R to K

It is a K-Banach space under $||f||_{\sup} = \max\{|f(x)| : x \in R\}$

• We say that a sequence of functions $\{e_n\}_{n\geq 0}$ in $C(R, K)$ is an orthonormal basis for $C(R, K)$ if and only if the following two conditions are satisfied:
(1) Every $f \in C(R, K)$ can be expanded uniquely as $f = \sum_{n=0}^{\infty} a_n e_n$, with $a_n \in K \to 0$ as $n \to \infty$.
(2) The sup-norm of f is given by $\|f\| = \max\{|a_n|\}$.

Well-known bases for $C(R, K)$

- The table below is a list of bases for $C(R, K)$ which are being used in non-Archimedean dynamical systems.

Rings	Classical case $\mathbb{Z}_p$	Function fields $\mathbb{F}_q[[T]]]$
Bases	Mahler polynomials	Carlitz-Wagner polynomials
	van der Put	Analogue of van der Put
	q-Mahler	No analogue
	No analogue	Digit derivatives
	Digit shifts (NA)	Digit shifts

- Mahlar baisis on $\mathbb{Z}_p$ = binomial coefficient polynomials

$$\binom{x}{m} = \frac{x(x-1)\cdots(x-m+1)}{m!} \in \mathbb{Q}[x] \ (m \geq 1) \ \text{ and } \ \binom{x}{0} = 1.$$

Mahler's theorem

Theorem

(1) $\{\binom{x}{m}\}_{m\geq 0}$ *is an orthonormal basis of* $C(\mathbb{Z}_p, \mathbb{Q}_p)$. *Every* $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$ *can be expanded uniquely as* $f(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m}$ *with* $a_m \in \mathbb{Q}_p \to 0$ *as* $m \to \infty$, *with the sup-norm given by* $\|f\|_{\sup} = \max_{m\geq 0}\{|a_m|_p\}$.
(2) The coefficients $\{a_m\}_{m\geq 0}$ *can be recovered by the formula:*

$$a_m = \triangle^m f(0) = \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} f(k).$$

- Difference operator: $\triangle f(x) := f(x+1) - f(x)$.

- $\triangle^n f(x) = \sum_{m=0}^{\infty} a_{m+n} \binom{x}{m}; \quad \triangle^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k).$

Van der Put's Theorem

- Van der Put functions $\{\chi(m,x)\}_{m\geq 0}$ are defined as the characteristic functions of certain balls $B_{p^{-\lfloor \log_p m\rfloor -1}}(m)$ in $\mathbb{Z}_p$:

$$\chi(m,x) = \begin{cases} 1 & \text{if } |x-m| \leq p^{-\lfloor \log_p m\rfloor -1}; \\ 0 & \text{otherwise.} \end{cases}$$

Theorem

(1) $\{\chi(m,x)\}_{m\geq 0}$ *is an orthonormal basis for* $C(\mathbb{Z}_p, \mathbb{Q}_p)$. *That is, every* $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$ *can be expanded uniquely as* $f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x)$, *with* $B_m \in \mathbb{Q}_p \to 0$ *as* $m \to \infty$, *whose sup-norm is given by* $||f||_{\sup} = \max_{m\geq 0}\{|B_m|\}$.
(2) *The coefficients* B_m *are determined by*

$$B_m = \begin{cases} f(m) - f(m_-) & \textit{if } \ m \geq p; \\ f(m) & \textit{otherwise.} \end{cases}$$

Ergodicity of f on $\mathbb{Z}_2$ in Mahler's expansion

Theorem 1.(Anashin 1994, J 2013)

Let $f(x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} c_m \binom{x}{m} : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function.
(1) f is measure-preserving if $c_1 \not\equiv 0 \pmod{p}$ and

$$c_m \equiv 0 \pmod{p} \quad \textit{for all} \quad m \geq 2.$$

(2) f is ergodic whenever the following conditions are satisfied:
(i) $c_0 \not\equiv 0 \pmod{p}$.
(ii)

$$c_1 \equiv \begin{cases} 1 \pmod{p} & \textit{if } p > 2; \\ 1 \pmod{4} & \textit{if } p = 2. \end{cases}$$

(iii) $c_m \equiv 0 \pmod{p^{\lfloor \log_p(m+1) \rfloor + 1 - \lfloor \log_p(m) \rfloor}}$ for all $m \geq 2$.
Moreover, in the case $p = 2$ these conditions are necessary.

- This result also works for the q-Mahler basis.

Ergodicity of f on $\mathbb{Z}_2$ in van der Put's expansion

Theorem 2.(Anashin, Khrennikov and Yurova 2011, J 2013)

A 1- Lipschitz function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ represented as

$$f(x) = \sum_{m=0}^{\infty} 2^{\lfloor \log_2 m \rfloor} b_m \chi(n, x) \ (b_m \in \mathbb{Z}_2)$$

is ergodic if and only if the following conditions are satisfied:
(1) $b_0 \equiv 1 \pmod 2$; $b_0 + b_1 \equiv 3 \pmod 4$; $b_2 + b_3 \equiv 2 \pmod 4$;
(2) $b_m \equiv 1 \pmod 2$ for all $m \geq 2$;
(3) $\sum_{i=2^{m-1}}^{2^m - 1} b_i \equiv 0 \pmod 4$ for all $m \geq 3$.

From now on, we assume that p is an odd prime.

Measure-preservation criterion in van der Put's expansion

Theorem 3.(Khrennikov and Yurova 2013) *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function in van der Put's expansion represented as*

$$f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} b_m \chi(m, x).$$

Then, f is measure-preserving if and only if the following conditions are satisfied:

(MP1) $\{b_0 = f(0), \cdots, b_{p-1} = f(p-1)\}$ *is a complete set of all distinct residues modulo p;*

(MP2) *For any integer $s \geq 1,\ 0 \leq k < p^s$, $\{b_{k+\ell p^s}\}_{1 \leq \ell \leq p-1}$ is a complete set of all distinct nonzero residues modulo p.*

Remark: We give an alternative proof of this result using the arguments in the function field analog of the criterion of Khrennikov and Yurova.

Bernoullicity criterion in van der Put's expansion

Theorem 4. *Let f be a p^α-Lipschitz function represented in van der Put's expansion as*

$$f(x) = \sum_{m=0}^{p^\alpha - 1} B_m(f)\chi(m,x) + \sum_{m \geq p^\alpha}^{\infty} p^{\lfloor \log_p m \rfloor - \alpha} b_m(f)\chi(m,x),$$

where $b_m(f) \in \mathbb{Z}_p$. Then, f is p^α-Bernoulli if and only if the following conditions are satisfied:

(B1) *For all $0 \leq i < p^\alpha$, $\{f(i + \ell p^\alpha)\}_{0 \leq \ell \leq p-1}$ is a complete set of all distinct residues modulo p;*

(B2) *For all $s \geq 1$, and all $0 \leq i < p^{\alpha+s}$, $\{b_{i+\ell p^{\alpha+s}}(f)\}_{1 \leq \ell \leq p-1}$ is a complete set of distinct nonzero residues modulo p.*

Sketch of Proof of Theorem 4.

Lemma 1.

A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is p^α-Lipschitz(expansive) if and only if, for every integer $0 \le i < p^\alpha$, $f_i : \mathbb{Z}_p \to \mathbb{Z}_p$ is a 1-Lipschitz function, where f_i is defined by $f_i(x) = f(i + p^\alpha x)$.

Lemma 2.

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a p^α-Lipschitz function. Then, the following are equivalent:
(1) f is a p^α-Bernoulli function.
(2) For every integer $0 \le i < p^\alpha$, $|f_i(x) - f_i(y)| = |x - y|$ for all $x, y \in \mathbb{Z}_p$.
(3) For every integer $0 \le i < p^\alpha$, f_i is a measure-preserving 1-Lipschitz function on $\mathbb{Z}_p$.

- Use Theorem 3 and Lemma 2.(2) to prove Theorem 4.

Sketch of Proof of Theorem 4.

Lemma 1.

A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is p^α-Lipschitz(expansive) if and only if, for every integer $0 \leq i < p^\alpha$, $f_i : \mathbb{Z}_p \to \mathbb{Z}_p$ is a 1-Lipschitz function, where f_i is defined by $f_i(x) = f(i + p^\alpha x)$.

Lemma 2.

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a p^α-Lipschitz function. Then, the following are equivalent:
(1) f is a p^α-Bernoulli function.
(2) For every integer $0 \leq i < p^\alpha$, $|f_i(x) - f_i(y)| = |x - y|$ for all $x, y \in \mathbb{Z}_p$.
(3) For every integer $0 \leq i < p^\alpha$, f_i is a measure-preserving 1-Lipschitz function on $\mathbb{Z}_p$.

- Use Theorem 3 and Lemma 2.(2) to prove Theorem 4.

Conjecture for measure-preservation of 1-Lipschitz functions in Mahler's expansion

Conjecture A. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function represented in Mahler's expansion as

$$f(x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} c_m \binom{x}{m} \quad (c_m \in \mathbb{Z}_p).$$

Then, f is measure-preserving if and only if the following conditions are satisfied:

(i) $\{f(0), f(1), \cdots, f(p-1)\}$ is a complete set of all distinct residues modulo p;

(ii) For all $s \geq 1$ and all $m = m_- + m_s p^s$ with $0 \leq m_- < p^s$ and $2 \leq m_s \leq p-1$, $c_m \equiv 0 \pmod{p}$.

(iii) For all $s \geq 1$ and all $0 \leq k < p^s$,

$$\sum_{r=0}^{s} \sum_{i=0}^{p^r - 1} \binom{k}{i} c_{i+p^r} \not\equiv 0 \pmod{p}.$$

Known Results for Conjecture A

- What we proved for Conjecture A;

1. Conjecture A holds for $p = 3$.
2. The sufficiency of Conjecture A holds.
3. Conjecture A holds for functions in $\mathbf{B}(\mathbb{Z}_p)$.

- Subclasses of 1-Lischitz dynamical systems:

$$\mathbb{Z}_p[x] \subset \mathbf{B}(\mathbb{Z}_p) \subset Udm^{(1)}(\mathbb{Z}_p) \subset \mathrm{Lip}_1(\mathbb{Z}_p),$$

where $\mathbf{B}(\mathbb{Z}_p) :=$ the set of **B**-functions or locally analytic functions of order 1 on $\mathbb{Z}_p$:

$$\mathbf{B}(\mathbb{Z}_p) := \{f(x) = \sum_{m=0}^{\infty} \lambda_m \binom{x}{m} : \frac{\lambda_m}{m!} \in \mathbb{Z}_p, \quad m = 0, 1, \cdots\}.$$

$Udm^{(1)}(\mathbb{Z}_p) :=$ the set of 1-Lipschitz, uniformly differentiable modulo p functions on $\mathbb{Z}_p$ of $N_1(f) = 1$.

- Try to prove that Conjecture A holds for functions in $Udm^{(1)}(\mathbb{Z}_p)$.

Definition of $Udm^{(1)}(\mathbb{Z}_p)$-functions

Definition.(Due to Anashin) *A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is uniformly differentiable modulo p^k if there exists a positive integer N and $\partial_k f(u) \in \mathbb{Q}_p$ such that for any $u \in \mathbb{Z}_p$, the congruence*

$$f(u + p^r h) \equiv f(u) + p^r h \partial_k f(u) \pmod{p^{k+r}}$$

holds for any integer $r \geq N$ and any $h \in \mathbb{Z}_p$, where $\partial_k f(u)$ does not depend on r and h. The smallest of these N is denoted by $N_k(f)$.

- $Udm^{(1)}(\mathbb{Z}_p) :=$ the set of a 1-Lipschitz, uniformly differentiable modulo p function on $\mathbb{Z}_p$ of $N_1(f) = 1$.
- $f \in Udm^{(1)}(\mathbb{Z}_p)$ if and only if for any $u \in \mathbb{Z}_p$, any integer $r \geq 1$ and any $h \in \mathbb{Z}_p$, the congruence holds:

$$f(u + p^r h) \equiv f(u) + p^r h \partial_1 f(u) \pmod{p^{1+r}},$$

with $\partial_1 f(u) \in \mathbb{Z}_p$. Note that $\mathbf{B}(\mathbb{Z}_p) \subset Udm^{(1)}(\mathbb{Z}_p)$.

Conjecture A holds for $Udm^{(1)}(\mathbb{Z}_p)$-functions

Theorem 5. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a $Udm^{(1)}(\mathbb{Z}_p)$-function represented in Mahler's expansion*

$$f(x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} c_m \binom{x}{m} \quad (c_m \in \mathbb{Z}_p).$$

Then, f is measure-preserving if and only if

(a) $\{f(0), f(1), \cdots, f(p-1)\}$ *is a complete set of all distinct residues modulo p;*

(b) *For all $0 \le k < p$,*

$$c_1 + \sum_{i=0}^{p-1} \binom{k}{i} c_{i+p} \not\equiv 0 \pmod{p}.$$

Remarks: 1. Condition (ii) of Conjecture A is redundant for functions in $Udm^{(1)}(\mathbb{Z}_p)$.
2. Any integer $s \geq 1$ in Condition (iii) equivalently reduces $s = 1$.

Key idea: interplay between coefficients of van der Put and Mahler

• What we need to do is to compute the following congruence sums: for all $s \geq 1$ and all $0 \leq k < p^s$,
(1) For all $0 \leq i \leq p-3$,

$$\sum_{\ell=1}^{p-1} \ell^i \sigma(\ell) := \sum_{\ell=1}^{p-1} \ell^i b_{k+\ell p^s} \equiv 0 \pmod{p};$$

(2)

$$\sum_{\ell=1}^{p-1} \ell^{p-2} \sigma(\ell) := \sum_{\ell=1}^{p-1} \ell^{p-2} b_{k+\ell p^s} \not\equiv 0 \pmod{p}.$$

where $\sigma : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $\ell \mapsto b_{k+\ell p^s} := p^{-s} B_{k+\ell p^s} \pmod{p}$.
• From K-Y criterion and Lagrange interpolation,
f is MP if and only if σ is a permutation on $\mathbb{F}_p^*$, together with condition (i) of Conjecture A.

Properties of 1-Lipschitz functions

- Gregory-Newton formula: For all integers $n \geq 0$ and all functions f with coefficients in an extension field of $\mathbb{Q}$,

$$f(x+n) = \sum_{i=0}^{\infty} \triangle^i f(x) \binom{n}{i}$$

Proposition.(V. Anashin) (1) A continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is 1-Lipschitz if and only if, for every integer $n \geq 1$, $\frac{\triangle^n f(x)}{n}$ is an integer-valued function.
(2) Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function, let $k \in \mathbb{Z}_p$, and let a base-p expansion of n contain more than one nonzero digits (i.e., $n \neq tp^r$ for $r \in \{0, 1, 2, \ldots\}, t \in \{1, 2, \ldots p-1\}$). Then,

$$\frac{\triangle^n f(k)}{n} \equiv 0 \pmod{p}.$$

More properties of 1-Lipschitz functions

- What is $\frac{\triangle^{tp^s} f(k)}{p^s}$ if $n = tp^s$, where $1 \le t \le p-1$?

Lemma 3. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function in van der Put's expansion represented as*

$$f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} b_m \chi(m,x).$$

Let $s \ge 1$ be an integer and k be an integer such that $0 \le k < p^s$. Then the following hold: (1) For all $2 \le t \le p-1$,

$$\frac{\triangle^{tp^s} f(k)}{p^s} \equiv \sum_{\ell=1}^{t} (-1)^{t+\ell} \binom{t}{\ell} b_{k+\ell p^s} \pmod{p}.$$

(2) $\frac{\triangle^{p^s} f(k)}{p^s} \equiv b_{k+p^s} + \sum_{\ell=1}^{p-1} \frac{f(k+\ell p^{s-1}) - f(k)}{\ell p^{s-1}} \pmod{p}.$

More properties of 1-Lipschitz functions

• In light of Lemma 3, we have the following inversion formula between $\frac{\triangle^{tp^s} f(k)}{p^s}$ and b_{k+tp^s}.

Lemma 4. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function in van der Put's expansion represented as before. Let $s \geq 1$ be an integer and k be an integer such that $0 \leq k < p^s$. For all $1 \leq t \leq p-1$,*

$$b_{k+tp^s} \equiv tA_0 + \sum_{\ell=1}^{t} \binom{t}{\ell} \frac{\triangle^{\ell p^s} f(k)}{p^s} \pmod{p},$$

where

$$A_0 \equiv \sum_{r=0}^{s-1} \sum_{\ell=1}^{p-1} (-1)^{\ell-1} \frac{\triangle^{\ell p^r} f(k)}{\ell p^r} \pmod{p}.$$

More properties of 1-Lipschitz functions

- We are now ready to compute the sums in question: for $0 \le i \le p-3$ or $i = p-2$, $\sum_{\ell=1}^{p-1} \ell^i b_{k+\ell p^s}$.

Lemma 5. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function represented in van der Put's expansion as before.*
(1) For all $0 \le i \le p-3$, all $s \ge 1$ and all $0 \le k < p^s$,

$$\sum_{\ell=1}^{p-1} \ell^i b_{k+\ell p^s} \equiv \sum_{t=2}^{p-1} \sum_{\ell=t}^{p-1} \ell^i \binom{\ell}{t} \frac{\triangle^{tp^s} f(k)}{p^s} \pmod{p}.$$

(2)

$$\begin{aligned} \sum_{\ell=1}^{p-1} \ell^{p-2} b_{k+\ell p^s} &\equiv \sum_{r=0}^{s} \sum_{\ell=1}^{p-1} (-1)^\ell \frac{\triangle^{\ell p^r} f(k)}{\ell p^r} \pmod{p} \\ &\equiv \sum_{r=0}^{s} \sum_{\ell=1}^{p-1} \sum_{i=0}^{k} \frac{(-1)^\ell}{\ell} \binom{k}{i} c_{\ell p^r + i} \pmod{p} \end{aligned}$$

Equivalent properties for 1-Lipschitz functions

Lemma 6. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function represented in the expansions of van der Put and Mahler.*

$$\begin{aligned} f(x) &= \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} c_m \binom{x}{m} \quad (c_m \in \mathbb{Z}_p); \\ f(x) &= \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} b_m \chi(m, x) \quad (b_m \in \mathbb{Z}_p). \end{aligned}$$

The following are equivalent:
For all $s \geq 1$ and $0 \leq k < p^s$, and $2 \leq \ell \leq p-1$.
(1) $\sum_{\ell=1}^{p-1} \ell^i b_{k+\ell p^s} \equiv 0 \pmod{p}$ *for all* $i = 0, \cdots, p-3$.
(2) $\frac{\triangle^{\ell p^s} f(k)}{p^s} \equiv 0 \pmod{p}$.
(3) $c_{k+\ell p^s} \equiv 0 \pmod{p}$.
(4) $b_{k+\ell p^s} \equiv \ell b_{k+p^s} \pmod{p}$.
(5) $\sum_{j=1}^{\ell} (-1)^j \binom{\ell}{j} b_{k+jp^s} \equiv 0 \pmod{p}$.

Theorem 5. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a $Udm^{(1)}(\mathbb{Z}_p)$-function represented in Mahler's expansion*

$$f(x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} c_m \binom{x}{m} \quad (c_m \in \mathbb{Z}_p).$$

Then, f is measure-preserving if and only if

(a) $\{f(0), f(1), \cdots, f(p-1)\}$ *is a complete set of all distinct residues modulo p;*

(b) *For all $0 \leq k < p$,*

$$c_1 + \sum_{i=0}^{p-1} \binom{k}{i} c_{i+p} \not\equiv 0 \pmod{p}.$$

Sketch of Proof of Theorem 5.

Proof(of reduction of any $s \geq 1$ to 1) Let f be in $Udm^{(1)}(\mathbb{Z}_p)$. For all $s \geq 1$, $0 \leq k < p^s$, and $1 \leq \ell < p$,

$$b_{k+\ell p^s} \equiv \ell b_{k+p^s} \pmod{p} \tag{2}$$

$$b_{k+\ell p^s} \equiv \ell \partial_1 f(k) \pmod{p}. \tag{3}$$

$$\Rightarrow \; b_{k+p^s} \equiv \partial_1 f(k) \equiv \partial_1(\bar{k}) \equiv b_{\bar{k}+p} \pmod{p}$$

$(becasue\ \partial_1 f(u)\ is\ 1 - Lipschitz\ in\ the\ middle\ and\ (7)\ with\ s = 1.)$

$$\begin{aligned}\Rightarrow \sum_{\ell=1}^{p-1} \ell^{p-2} b_{k+\ell p^s} &\equiv \sum_{\ell=1}^{p-1} \ell^{p-2} b_{\bar{k}+\ell p} \equiv -b_{\bar{k}+p} \pmod{p} \;\; (by\ FLT) \\ &\equiv c_1 + \sum_{i=0}^{p-1} \binom{\bar{k}}{i} c_{i+p} \pmod{p} \;\; (by\ Lemma\ 5(2))\end{aligned}$$

(2) $\Rightarrow \sum_{\ell=1}^{p-1} \ell^i b_{k+\ell p^s} \equiv \sum_{\ell=1}^{p-1} \ell^{i+1} b_{\bar{k}+p} \equiv 0 \pmod{p}$, for $0 \leq i \leq p-3$.

Bernoullicity of 2^α-Lipschitz functions

• We turn to Bernoullicity of p^α-Lipschitz functions on $\mathbb{Z}_p$.

Theorem 6. *Let $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ be a 2^α-Lipschitz function represented in Mahler's expansion as*

$$f(x) = \sum_{m=0}^{2^\alpha - 1} a_m \binom{x}{m} + \sum_{m \geq 2^\alpha} 2^{\lfloor \log_2 m \rfloor - \alpha} c_m \binom{x}{m}.$$

The function f is 2^α -Bernoulli if and only if the following conditions are satisfied: For all $s \geq 0$ and $0 \leq i < 2^{\alpha+s}$,

$$\sum_{r=\alpha}^{\alpha+s} \sum_{j=0}^{2^r - 1} \binom{i}{j} c_{2^r + j} \equiv 1 \pmod{2}.$$

• Proof follows from the following corollary using Bernoullicity criteria (Theorem 4):

Corollary. *A function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is 2^k-Bernoulli if and only if, for all $s \geq 0$ and $0 \leq i < 2^{k+s}$,*

$$f(i + 2^{k+s}) \equiv f(i) + 2^s \pmod{2^{s+1}}.$$

Bernoullicity of p^α-Lipschitz functions where p is an odd prime

Theorem 7. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a p^α-Lipschitz function represented in Mahler's expansion as* $f(x) = \sum_{m=0}^{p^\alpha - 1} a_m \binom{x}{m} + \sum_{m \geq p^\alpha} p^{\lfloor \log_p m \rfloor - \alpha} c_m \binom{x}{m}$. *The function f is p^α-Bernoulli whenever the following conditions are satisfied:*

(1) *For all $0 \leq i < p^\alpha$, $\{f(i + \ell p^\alpha)\}_{0 \leq \ell \leq p-1}$ is a complete set of all distinct residues modulo p;*

(2) *For all $m = m_- + m_s p^s \geq p^{\alpha+1}$ with $1 < m_s < p$,* $c_m \equiv 0 \pmod{p}$;

(3) *For all $s \geq 1$ and $0 \leq i < p^{\alpha+s}$,*

$$\sum_{r=\alpha}^{\alpha+s} \sum_{m=0}^{p^r - 1} \binom{i}{m} c_{p^r + m} \not\equiv 0 \pmod{p}.$$

Conversely, if f is a p^α-Bernoulli function satisfying a certain hypothesis (H), these conditions are necessary.

Bernoullicity of p^α-Lipschitz functions where p is odd prime

Hypothesis (H) For all $s \geq 1$, $0 \leq i < p^{\alpha+s}$ and $1 \leq \ell < p$,

$$f(i + \ell p^{\alpha+s}) - f(i) \equiv \varepsilon \ell p^s \pmod{p^{s+1}}$$

for some integer ε with $p \nmid \varepsilon$ that does not depend on ℓ.
Such functions include
(i) beta-transformations T_β on $\mathbb{Z}_p$ with $|\beta| = p^\alpha (\alpha \geq 1)$, which are complete generalizations of the shift maps on $\mathbb{Z}_p$;
(ii) p^α-Bernoulli polynomial functions $f \in \mathbb{Q}_p[x]$ with additional assumptions that $|f^{(j)}(x)| \leq p^{j\alpha}$ for all $j \geq 1$, where $f^{(j)}$ denotes the jth derivative of f.

Root existence of 1-Lipschitz functions on $\mathbb{Z}_p$

Recall Hensel's Lemma: $\mathbb{Z}_p[x] \subset \mathrm{Lip}_1(\mathbb{Z}_p)$

Hensel's Lemma for polynomials

Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial. Suppose there exists $\bar{h} \in \{0, 1, \ldots, p-1\}$ such that

$$f(\bar{h}) \equiv 0 \pmod{p} \text{ and } f'(\bar{h}) \not\equiv 0 \pmod{p}.$$

Then there exists a unique $h \in \mathbb{Z}_p$ such that

$$f(h) = 0 \text{ and } h \equiv \bar{h} \pmod{p}.$$

Hensel's Lemma for analytic functions

Let $f(x) = \sum_{n\geq 0} c_n x^n \in \mathbb{Z}_p[[x]]$ be an analytic function on $\mathbb{Z}_p$. Suppose there exists $\bar{h} \in \{0, 1, \ldots, p-1\}$ such that $f(\bar{h}) \equiv 0 \pmod{p}$ and $f'(\bar{h}) \not\equiv 0 \pmod{p}$. Then there exists a unique $h \in \mathbb{Z}_p$ such that

$$f(h) = 0 \text{ and } h \equiv \bar{h} \pmod{p}.$$

Root existence of 1-Lipschitz functions on $\mathbb{Z}_p$

Recall Hensel's Lemma: $\mathbb{Z}_p[x] \subset \mathrm{Lip}_1(\mathbb{Z}_p)$

Hensel's Lemma for polynomials

Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial. Suppose there exists $\bar{h} \in \{0, 1, \ldots, p-1\}$ such that

$$f(\bar{h}) \equiv 0 \pmod{p} \text{ and } f'(\bar{h}) \not\equiv 0 \pmod{p}.$$

Then there exists a unique $h \in \mathbb{Z}_p$ such that

$$f(h) = 0 \text{ and } h \equiv \bar{h} \pmod{p}.$$

Hensel's Lemma for analytic functions

Let $f(x) = \sum_{n \geq 0} c_n x^n \in \mathbb{Z}_p[[x]]$ be an analytic function on $\mathbb{Z}_p$. Suppose there exists $\bar{h} \in \{0, 1, \ldots, p-1\}$ such that $f(\bar{h}) \equiv 0 \pmod{p}$ and $f'(\bar{h}) \not\equiv 0 \pmod{p}$. Then there exists a unique $h \in \mathbb{Z}_p$ such that

$$f(h) = 0 \text{ and } h \equiv \bar{h} \pmod{p}.$$

Root of 1-Lipschitz functions on $\mathbb{Z}_p$ in van der Put's expansion

• Generalization of Hensel's lemma for 1-Lipschitz(not necessarily differentiable) functions on $\mathbb{Z}_p$.(Because the Theorem implies HL.)

Theorem 8.(Yurova and Khrennikov 2016) *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function represented in van der Put's expansion as*

$$f(x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} b_m \chi(m, x) \quad (b_m \in \mathbb{Z}_p).$$

Suppose that f satisfies the following two assumptions:
(1) For some natural number R, there exists $\overline{h} \in \{0, 1, \cdots, p^R - 1\}$ such that $f(\overline{h}) \equiv 0 \pmod{p^R}$.
(2) For any $m \geq p^R$ such that $m \equiv \overline{h} \pmod{p^R}$, $\{b_{m+tp^{1+\lfloor \log_p m \rfloor}}\}_{1 \leq t \leq p-1}$ is a complete set of nonzero residues modulo p.
Then there exists a unique $h \in \mathbb{Z}_p$ such that $f(h) = 0$ and $h \equiv \overline{h} \pmod{p^R}$.

Theorem 9. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be 1-Lipschitz function represented in Mahler's expansion as*

$$f(x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} c_m \binom{x}{m} \quad (c_m \in \mathbb{Z}_p).$$

Suppose f satisfies the following conditions:

(1) *For some natural number R, there exists $\bar{h} \in \{0, 1, \cdots, p^R - 1\}$ such that $f(\bar{h}) \equiv 0 \pmod{p^R}$.*

(2) *For all $s \geq 1$ and all $m = m_- + m_s p^s$ with $0 \leq m_- < p^s$ and $2 \leq m_s \leq p - 1$,*

$$c_m \equiv 0 \pmod{p}.$$

(3) *For all $m \geq p^R$ such that $m \equiv \bar{h} \pmod{p^R}$,*

$$\sum_{r=0}^{1+\lfloor \log_p m \rfloor} \sum_{i=0}^{p^r-1} \binom{m}{i} c_{i+p^r} \not\equiv 0 \pmod{p}.$$

Then, there exists a unique $h \in \mathbb{Z}_p$ such that $f(h) = 0$ and $h \equiv \bar{h} \pmod{p^R}$.

Root of 1-Lipschitz functions on $\mathbb{Z}_p$ in Mahler's expansion

Corollary

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz, uniformly differentiable modulo p function of $N_1(f) = 1$, represented in Mahler's expansion as before. Suppose f satisfies the following conditions:

(1) *There exists $\bar{h} \in \{0, 1, \cdots, p-1\}$ such that $f(\bar{h}) \equiv 0 \pmod{p}$*

(2) *For only $\bar{h}$,*

$$c_1 + \sum_{i=0}^{p-1} \binom{\bar{h}}{i} c_{i+p} \not\equiv 0 \pmod{p}.$$

Then, there exists a unique $h \in \mathbb{Z}_p$ such that $f(h) = 0$ and $h \equiv \bar{h} \pmod{p}$.

Thank you for your attention !!!

Properties of B-functions

$$\mathbf{B}(\mathbb{Z}_p) := \{f(x) = \sum_{m=0}^{\infty} \lambda_m \binom{x}{m} : \frac{\lambda_m}{m!} \in \mathbb{Z}_p, \quad m = 0, 1, \cdots\}.$$

Proposition

(1) The class $\mathbf{B}(\mathbb{Z}_p)$ is the space of differentiable everywhere, 1-Lipschitz functions on $\mathbb{Z}_p$.
(2) This class is closed under addition, multiplication, differentiation, and composition.
(3) The countable set of all polynomials with non-negative rational integer coefficients is a dense subset of $\mathbf{B}(\mathbb{Z}_p)$.
(4) Every $f \in \mathbf{B}(\mathbb{Z}_p)$ has a Taylor expansion at all points $x = a \in \mathbb{Z}_p$: for $a, h \in \mathbb{Z}_p$ and $s = 1, \cdots$, we have

$$f(a + p^s h) = \sum_{m=0}^{\infty} \frac{f^{(m)}(a)}{m!} (p^s h)^m,$$

where $\frac{f^{(m)}(a)}{m!}$ are p-adic integers for all $m \geq 0$.