Toward the ergodicity of p-adic 1-Lipschitz functions represented by the van der Put series

Sangtae Jeong

Department of Mathematics

Inha University

stj@inha.ac.kr

International Workshop on p-adic Methods at Bielefeld Univ.

2013. 04. 15

Outline

1. Goal of the Talk
2. Brief introduction to non-Archimedean dynamical systems
3. Summary on known results for ergodicity of maps on R
4. Ergodicdity of 1- Lipschitz functions on $\mathbb{Z}_p$
5. Some equivalent statements
6. Alternative proofs of Anashin-Khrennikov-Yurova results

Goal of the Talk

In this talk,

• Provide the sufficient conditions for the ergodicity of a 1-Lipschitz fucntion $f : \mathbb{Z}_p \to \mathbb{Z}_p$ represented by the van der Put series.

• Provide alternative proofs of two criteria for an ergodic 1-Lipschitz function on $\mathbb{Z}_2$, represented by
(a) the Mahler basis (due to **Anashin**)
(b) the van der Put basis (due to **Anashin, Khrennikov and Yurova**)

• Give a characterization for the ergodicity of a polynomial over $\mathbb{Z}_2$ in term of its coefficients(if time permits).

Preliminaries to non-Archimedean dynamical systems

• Non-Archimedean dynamical system is made up of a triple (R, f, μ) where
R: a measurable space ($R = \mathbb{Z}_p$ or $\mathbb{F}_q[[T]]$)
f: a measurable function $f : R \to R$
μ: a normalized measure on R so that
$\mu(R) = 1; \mu(a + \pi^k R) = 1/q^k$, $q = \#R/(\pi)$.

• It has many applications to mathematical physics, computer science, cryptography, and so on. In particular, it can be applied to pseudo-random numbers in cryptography.

• Measure-preserving and ergodic functions on R :
(1) A mapping $f : R \to R$ is measure-preserving if $\mu(f^{-1}(M)) = \mu(M)$ for each measurable subset $M \subset R$.

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

Equivalent statements for 1-Lipschitz functions

$(R, \pi, |?|_\pi) = (\mathbb{Z}_p, p, |?|_p)$ or $(\mathbb{F}_q[[T]], T, |?|_T)$

• $f : R \to R$ is 1-Lipschitz (or compatible) if one of the equivalent statements is satisfied:
(1) $|f(x) - f(y)|_\pi \leq |x - y|_\pi$ for all $x, y \in R$;
(2) $|f(x + y) - f(x)|_\pi \leq |y|_\pi$ for all $x, y \in R$;
(3) $|\Phi_1 f(x, y) := \frac{1}{y}(f(x + y) - f(x))|_\pi \leq 1$ for all $x \in R$ and all $y \neq 0 \in R$;
(4) $||\Phi_1 f(x, y)||_{\sup} \leq 1$ for all $y \neq 0 \in R$;
(5) $f(x + \pi^n R) \subset f(x) + \pi^n R$ for all $x \in R$ and any integer $n \geq 1$;
(6) $f(x) \equiv f(y) \pmod{\pi^n}$ whenever $x \equiv y \pmod{\pi^n}$ for any integer $n \geq 1$.

• Then, a 1-Lipschitz function induces a (reduced) function $f_{/n} : R/\pi^n R \to R/\pi^n R$ for all integers $n \geq 1$.

Equivalent statements and Problems

Equivalent statements for measure-preserving and ergodic functions

(1) A 1-Lipschitz function $f : R \to R$ is measure-preserving
$\Leftrightarrow$ its reduced function $f_{/n} : R/\pi^n R \to R/\pi^n R$ is bijective for all integers $n \geq 1$.
$\Leftrightarrow$ f is an isometry; $|f(x) - f(y)|_\pi = |x - y|_\pi$ for all $x, y \in R$.
(2) A 1-Lipschitz function $f : R \to R$ is ergodic if and only if its reduced function $f_{/n} : R/\pi^n R \to R/\pi^n R$ is transitive for all integers $n \geq 1$. (• transitive = forming a cycle by repeating f)

Problems to be tackled:

To characterize 3 types of (1-Lipschitz, measure-preserving, ergodic) functions f on R, in terms of coefficients $\{a_n\}_{n\geq 0}$ of f written as

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

where e_n is a well behaved orthonormal basis for $C(R, K)$, the space of continuous functions on R.

Equivalent statements and Problems

Equivalent statements for measure-preserving and ergodic functions

(1) A 1-Lipschitz function $f : R \to R$ is measure-preserving
$\Leftrightarrow$ its reduced function $f_{/n} : R/\pi^n R \to R/\pi^n R$ is bijective for all integers $n \geq 1$.
$\Leftrightarrow$ f is an isometry; $|f(x) - f(y)|_\pi = |x - y|_\pi$ for all $x, y \in R$.
(2) A 1-Lipschitz function $f : R \to R$ is ergodic if and only if its reduced function $f_{/n} : R/\pi^n R \to R/\pi^n R$ is transitive for all integers $n \geq 1$. (• transitive = forming a cycle by repeating f)

Problems to be tackled:

To characterize 3 types of (1-Lipschitz, measure-preserving, ergodic) functions f on R, in terms of coefficients $\{a_n\}_{n\geq 0}$ of f written as

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

where e_n is a well behaved orthonormal basis for $C(R, K)$, the space of continuous functions on R.

Summary on known results for ergodicity of 1-Lipschitz maps on R

For a 1-Lipschitz map $f : R \to R$ written as

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

where e_n is an orthonormal basis of $C(R, K)$, we have characterization results for ergodicity on R in the following cases :

- Known results for ergodicity of 1-Lipschitz maps on R :

R	bases $e_n(x)$	discoverers
$\mathbb{Z}_2$	Mahler basis	Anashin
$\mathbb{Z}_2$	Van der Put basis	Ana., Khrennikov and Yurova
$\mathbb{F}_2[[T]]$	Analog of Van der Put	Lin, Shi and Yang
$\mathbb{F}_2[[T]]$	Carlitz-Wagner basis	Lin, Shi and Yang
$\mathbb{F}_2[[T]]$	digit derivatives basis	Jeong
$\mathbb{F}_2[[T]]$	digit shift operators basis	Jeong

Ergodicity of f on $\mathbb{Z}_2$ with respect to Mahler basis

Theorem(Anashin)

A 1-Lipschitz function

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n} : \mathbb{Z}_p \to \mathbb{Z}_p$$

is ergodic whenever the following conditions are satisfied:
(1) $a_0 \not\equiv 0 \pmod{p}$.
(2)

$$a_1 \equiv \begin{cases} 1 \pmod{p} & \textit{if} \quad p > 2; \\ 1 \pmod{4} & \textit{if} \quad p = 2. \end{cases}$$

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

Useful criteria for ergodicity and measure-preservation

Corollary(Anashin)

(a) Every 1-Lipschitz function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is ergodic if and only if it is of the form

$$f(x) = 1 + x + 2\Delta g(x)$$

for a suitable constant $d \in \mathbb{Z}_2$ and a suitable1-Lipschitz function $g : \mathbb{Z}_2 \to \mathbb{Z}_2$.
(b) Every 1-Lipschitz function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is measure-preserving if and only if it is of the form $f(x) = d + x + 2g(x)$ for a suitable constant $d \in \mathbb{Z}_2$ and a suitable1-Lipschitz function $g : \mathbb{Z}_2 \to \mathbb{Z}_2$.

For later use, we have the following.
Lemma(Anashin)

Given a 1-Lipschitz function $g : \mathbb{Z}_p \to \mathbb{Z}_p$ and a p-adic integer $d \not\equiv 0 \pmod{p}$, the function $f(x) = d + x + p\Delta g(x)$ is ergodic.

Van der Put basis

- The van der Put basis $\chi(m,x)$ on $\mathbb{Z}_p$. For an integer $m > 0$ and $x \in \mathbb{Z}_p$, we define

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

and

$$\chi(0,x) = \begin{cases} 1 & \textit{if} |x| \le p^{-1}; \\ 0 & \textit{otherwise}. \end{cases}$$

- For an positive integer $m = m_0 + m_1 p + \cdots + m_s p^s (m_s \neq 0)$,

$$q(m) = m_s p^s; \quad m\_ := m - q(m)$$

- **Theorem**(Van der Put)

Any continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is uniquely represented as $f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x)$.
The expansion coefficients $\{B_m\}_{m \ge 0}$ can be recovered by

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

Ergodicity of f on $\mathbb{Z}_2$ with respect to van der Put basis

Theorem(Anashin, Khrennikov and Yurova)

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

$$f(x) = b_0 \chi(0, x) + \sum_{n=1}^{\infty} 2^{\lfloor \log_2 n \rfloor} b_n \chi(n, x)$$

with $b_n \in \mathbb{Z}_2$, is ergodic if and only if the following conditions are satisfied:

(1) $b_0 \equiv 1 \pmod 2$;
(2) $b_0 + b_1 \equiv 3 \pmod 4$;
(3) $b_2 + b_3 \equiv 2 \pmod 4$;
(4) $|b_n| = 1$ for all $n \geq 2$;
(5) $\sum_{i=2^{n-1}}^{2^n - 1} b_i \equiv 0 \pmod 4$ for all $n \geq 3$.

Measure-preservation of f on $\mathbb{Z}_p$ with respect to van der Put basis

Theorem(Khrennikov and Yurova)

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1- Lipschitz function represented as

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

Then f is measure-preserving if and only if
(1) $\{b_0, b_1, \cdots, b_{p-1}\}$ is distinct modulo p;
(2) For any integer $k \geq 1$, $b_{m+p^k}, b_{m+2p^k}, \cdots, b_{m+(p-1)p^k}$ are nonzero residues modulo p for all $m = 0, \cdots p^k - 1$.

From now on, use the notation for $m \geq 0$,

$$B_m = p^{\lfloor \log_p m \rfloor} b_m.$$

Main Results: Ergodicdity of 1- Lipschitz functions on $\mathbb{Z}_p$

- Anashin's results using Mahler basis $\Rightarrow$ Anashin-Khrennikov-Yurova results using van der Put basis.

- Strategy for main results- Going backward:
Anashin- Khrennikov-Yurova results using van der Put basis $\Rightarrow$ Anashin's results using Mahler basis.
–Provide the sufficient conditions for ergodicity of 1- Lipschitz functions on $\mathbb{Z}_p$, thereby obtaining a generalization of AKY results.
–Give simple, alternate proofs of two results, especially Anashin's results for Mahler basis. Because his results rely on a criteria based on the algebraic normal form of Boolean functions which determines the measure-preservation and ergodicity of 1-Lipschitz functions.

Main Results: Ergodicdity of 1- Lipschitz functions on $\mathbb{Z}_p$

Theorem A (J)

Let $f(x)=\sum_{m=0}^{\infty} B_m \chi(m,x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a measure-preserving 1-Lipschitz function of the form $f(x) = d + \varepsilon x + p\Delta g(x)$ for a suitable 1-Lipschitz function $g(x)$, where $\varepsilon \equiv 1 \pmod p$ and $d \not\equiv 0 \pmod p$. Then (i) the function f is ergodic.

(ii) We have the following congruence relations:

(1) $B_0 \equiv s \pmod p$ for some $0 < s < p$;

(2) $\sum_{m=0}^{p-1} B_m \equiv ps + \frac{1}{2}(p-1)p \pmod{p^2}$;

(3)

$$\sum_{m=p}^{p^2-1} B_m \equiv \frac{1}{2}(p-1)p^3 \equiv \begin{cases} 4 & \pmod{2^3} \quad \text{if} \quad p=2; \\ 0 & \pmod{p^3} \quad \text{if} \quad p>2; \end{cases}$$

(4) $B_m \equiv q(m) \pmod{p^{\lfloor \log_p m \rfloor + 1}}$ for all $m \geq p$;

(5) $\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv 0 \pmod{p^{n+1}}$ for all $n \geq 3$.

Main Results: Ergodicdity of p-adic 1- Lipschitz functions on $\mathbb{Z}_p$

Theorem B(J)

Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function. Then f is ergodic if f satisfies the following conditions:

(0) $B_m \equiv B_0 + m \pmod p$ for $0 < m < p$; (additional condition)

(1) $B_0 \equiv s \pmod p$ for some $0 < s < p$;

(2) $\sum_{m=0}^{p-1} B_m \equiv ps + \frac{1}{2}(p-1)p \pmod{p^2}$;

(3)

$$\sum_{m=p}^{p^2-1} B_m \equiv \frac{1}{2}(p-1)p^3 \equiv \begin{cases} 4 \pmod{2^3} & \textit{if} \quad p = 2; \\ 0 \pmod{p^3} & \textit{if} \quad p > 2; \end{cases}$$

(4) $B_m \equiv q(m) \pmod{p^{\lfloor \log_p m \rfloor + 1}}$ for all $m \geq p$;

(5) $\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv 0 \pmod{p^{n+1}}$ for all $n \geq 3$.

Measure preservation of 1- Lipschitz functions on $\mathbb{Z}_p$

To sketch a proof, we need to go through several lemmas;

Lemma 1

The 1- Lipschitz function $f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x) : \mathbb{Z}_p \to \mathbb{Z}_p$ is measure-preserving whenever the following conditions are satisfied:
(1) $\{B_0, B_1, \cdots, B_{p-1}\}$ is distinct modulo p;
(2) $B_m \equiv q(m) \pmod{p^{\lfloor \log_p m \rfloor + 1}}$ for all $m \geq p$.

Lemma 2

Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a measure-preserving 1- Lipschitz function. Then we have the following:
(1) $\{B_0, B_1, \cdots, B_{p-1}\}$ is distinct modulo p.
(2) $|B_m| = |q(m)| = |p|^{\lfloor \log_p m \rfloor}$ for all $m \geq p$

Congruence formula of measure-preserving 1- Lipschitz functions on $\mathbb{Z}_p$

Lemma 3

Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a measure-preserving 1- Lipschitz function. For $p^{n-1} \leq m \leq p^n - 1$ $(n \geq 2)$, set

$$B_m = p^{n-1} b_m = p^{n-1}(b_{m0} + b_{m1} p + \cdots),$$

where

$$(b_{m0} \neq 0, 0 \leq b_{mi} \leq p-1, i = 0, 1 \cdots).$$

Then, for all $n \geq 2$, we have

$$\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv \frac{1}{2}(p-1)p^{2n-1} + T_n p^n \pmod{p^{n+1}},$$

where T_n is defined by $T_n = \sum_{m=p^{n-1}}^{p^n-1} b_{m1}$.

Lemma 4

If a 1-Lipschitz fun. $f = \sum_{m=0}^{\infty} B_m \chi(m,x) : \mathbb{Z}_p \to \mathbb{Z}_p$ is of the form $f(x) = \Delta g(x)$ for some 1-Lip. fun. $g = \sum_{m=0}^{\infty} \tilde{B}_m \chi(m,x)$,

$$\begin{aligned} B_m &= \tilde{B}_{m+1} - \tilde{B}_m \qquad\qquad \textit{if } 0 \le m \le p-2; \\ &= \tilde{B}_p + \tilde{B}_0 - \tilde{B}_{p-1} \qquad \textit{if } m = p-1; \\ &= \tilde{B}_{m+1} - \tilde{B}_m \textit{ if } m \ne p^{n-1} - 1 + m_{n-1}p^{n-1}, \\ &\qquad\qquad p^{n-1} \le m \le p^n - 1, n \ge 2; \\ &= \tilde{B}_{m+1} - \tilde{B}_m - \tilde{B}_{p^{n-1}} \textit{if } m = p^{n-1} - 1 + m_{n-1}p^{n-1}, \\ &\qquad\qquad 1 \le m_{n-1} \le p-1, n \ge 2. \end{aligned}$$

Lemma 5

Let $f = \sum_{m=0}^{\infty} B_m \chi(m,x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function satisfying (1) $\sum_{m=0}^{p-1} B_m \equiv 0 \pmod{p}$;
(2) $\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv 0 \pmod{p^n}$ for all $n \ge 2$. Then there exists a 1-Lipschitz function $g(x)$ such that $f(x) = \Delta g(x)$.

Proof of Main Results

Sketch of proof:

(i) Use Anashin's lemma: Every 1- Lipschitz function f of the form $f = B_0 + x + p\Delta g(x)$ with some 1-Lipschitz function $g(x)$ is ergodic.

(ii) Using conditions (0)-(1)-(4) and

$$B_0 = \sum_{m=0}^{p-1} B_0 \chi(m,x); \quad x = \sum_{m=1}^{p-1} m\chi(m,x) + \sum_{m \geq p} q(m)\chi(m,x),$$

Decompose f into a function of the form

$$f = B_0 + x + p\sum_{m \geq 0} B''_m \chi(m,x).$$

(iii) Condition (2) is equivalent to $\sum_{m=0}^{p-1} B''_m \equiv 0 \pmod p$ conditions (5) and (3) are equivalent to $\sum_{m=p^{n-1}}^{p^n-1} B''_m \equiv 0 \pmod{p^n}$ for all $n \geq 2$. By Lemma 5, we have the desired result.

Remark. When p is 2, it reduces to AKY results.

Some equivalent statements

Lemma 6

Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function represented by the van der Put series. Then, for all $n \geq 2$, we have

$$\sum_{m=p^{n-1}}^{p^n-1} B_m = \sum_{m=0}^{p^n-1} f(m) - p \sum_{m=0}^{p^{n-1}-1} f(m).$$

From this point onward, we assume that $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is a measure-preserving 1-Lipschitz function. For a nonnegative integer m, write

$$f(m) = \sum_{i=0}^{\infty} f_{mi} p^i \text{ with } 0 \leq f_{mi} \leq p-1 \ (i = 0, 1, \cdots)$$

For an integer $n \geq 1$, we define S_n to be

$$S_n = \sum_{m=0}^{p^n-1} f_{mn}.$$

Some equivalent statements

Lemma 6 gives

$$\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv 0 \pmod{p^{n+1}} \Leftrightarrow \sum_{m=0}^{p^n-1} f(m) \equiv p \sum_{m=0}^{p^{n-1}-1} f(m) \pmod{p^{n+1}}.$$

RHS gives the following congruence:

$$S_n \equiv \begin{cases} S_{n-1} \pmod{p} & (n \geq 2) \textit{ if } p \neq 2; \\ S_{n-1} \pmod{2} & (n \geq 3) \textit{ if } p = 2. \end{cases}$$

By Lemma 6 again for all $n \geq 2$, we have

$$T_n \equiv S_n - S_{n-1} \pmod{p}.$$

Lemma 3 gives

$$\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv \frac{1}{2}(p-1)p^{2n-1} + T_n p^n \pmod{p^{n+1}}.$$

Some equivalent statements

Theorem C

Let $f(x)=\sum_{m=0}^{\infty} B_m\chi(m,x):\mathbb{Z}_p\to\mathbb{Z}_p$ be a mp 1-Lipschitz function and let T_n and S_n be defined as before. Then

(1) $n=2$: (a) $p=2$: $\sum_{m=2}^{2^2-1} B_m\equiv 4 \pmod{2^3}$

$$\Leftrightarrow S_2\equiv S_1 \pmod 2 \Leftrightarrow T_2\equiv 0 \pmod 2;$$

or $\sum_{m=2}^{2^2-1} B_m\equiv 0 \pmod{2^3}$

$$\Leftrightarrow S_2\equiv S_1+1 \pmod 2 \Leftrightarrow T_2\equiv 1 \pmod 2.$$

(b) $p>2$: $\sum_{m=p}^{p^2-1} B_m\equiv rp^2 \pmod{p^3}$

$$\Leftrightarrow S_2\equiv S_1+r \pmod p \Leftrightarrow T_2\equiv r \pmod p.$$

(2) $n\geq 3$ and any prime p: $\sum_{m=p^{n-1}}^{p^n-1} B_m\equiv rp^n \pmod{p^{n+1}}$

$$\Leftrightarrow S_n\equiv S_{n-1}+r \pmod p \Leftrightarrow T_n\equiv r \pmod p.$$

Alternative proofs of Anashin-Khrennikov-Yurova results

The following lemma is very crucial, which is an analog in $\mathbb{Z}_2$ of the result(**Lin, Shi and Yang**) for the formal power series ring $\mathbb{F}_2[[T]]$ over the field $\mathbb{F}_2$ of two elements.

Lemma 7

Let $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ be a measure-preserving 1-Lipschitz function such that f is transitive modulo $2^n, n \geq 1$. Then f is transitive modulo 2^{n+1} if and only if S_n is odd, where S_n is defined by

$$S_n = \sum_{m=0}^{p^n-1} f_{mn}; \quad f(m) = \sum_{i=0}^{\infty} f_{mi} p^i.$$

By Lemma 7 and Theorem C we reprove the AKY result.

Corollary 1

Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_2 \to \mathbb{Z}_2$ be a 1-Lipschitz function. Then f is ergodic if and only if all conditions in AKY's Theorem are satisfied.

Alternative proofs of Anashin-Khrennikov-Yurova results

By Corollary 1 we reprove the Anashin's result.

Corollary 2

Let $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ be a 1-Lipschitz function. Then, (1) f is measure-preserving if and only if f is of the form $f(x) = d + x + 2g(x)$ for some 2-adic integer $d \in \mathbb{Z}_2$ and some 1-Lipschitz function $g(x)$.
(2) f is ergodic if and only if f is of the form $f(x) = 1 + x + 2\Delta g(x)$ for some 1-Lipschitz function $g(x)$.

By Corollary 2 we reprove the Anashin's result.

Corollary 3

Let $f(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m} : \mathbb{Z}_2 \to \mathbb{Z}_2$ be a 1-Lipschitz function. Then f is ergodic if and only if all conditions in Anashin's Theorem are satisfied.

An application: Ergodicity of polynomials over $\mathbb{Z}_2$

- To provide a characterization for the ergodicity of a polynomial over $\mathbb{Z}_2$ in term of its coefficients. For simplicity, we take a polynomial $f \in \mathbb{Z}_2[x]$ with $f(0) = 1$:

$$f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + 1.$$

Then we set

$$A_0 = \sum_{i \equiv 0 \pmod 2, i > 0} a_i, \quad A_1 = \sum_{i \equiv 1 \pmod 2} a_i.$$

Theorem(Larin, Durand and Paccaut)

The polynomial f is ergodic over $\mathbb{Z}_2$ if and only if the following conditions are simultaneously satisfied:

$$a_1 \equiv 1 \pmod 2;$$
$$A_1 \equiv 1 \pmod 2;$$
$$A_0 + A_1 \equiv 1 \pmod 4;$$
$$a_1 + 2a_2 + A_1 \equiv 2 \pmod 4.$$

Future Work

(1) For a general prime $p > 2$, try to provide characterization results for $f : \mathbb{Z}_p \to \mathbb{Z}_p$ to be ergodic.

(2) Problem (raised by Anashin): Try to develop the theory for $\mathbb{F}_q[[t]]$ analogous to Anashin's theory on derivatives modulo p^k on $\mathbb{Z}_p$

Thank you for your attention !!!

Future Work

(1) For a general prime $p > 2$, try to provide characterization results for $f : \mathbb{Z}_p \to \mathbb{Z}_p$ to be ergodic.

(2) Problem (raised by Anashin): Try to develop the theory for $\mathbb{F}_q[[t]]$ analogous to Anashin's theory on derivatives modulo p^k on $\mathbb{Z}_p$

Thank you for your attention !!!