On continued fraction expansion of potential counterexamples to p-adic Littlewood conjecture

Dzmitry Badziahin *

September 10, 2014

Abstract

The p-adic Littlewood conjecture (PLC) states that $\liminf_{q\to\infty} q\cdot|q|_p\cdot||qx|| = 0$ for every prime p and every real x. Let $w_{CF}(x)$ be an infinite word composed of the continued fraction expansion of x and let T be the standard left shift map. Assuming that x is a counterexample to PLC we get several quite restrictive conditions on limit elements of the sequence $\{\mathrm{T}^n w_{CF}(x)\}_{n\in\mathbb{N}}$. As a consequence we show (Theorem 5) that for any such limit element w we must have $\lim_{n\to\infty} P(w,n) - n = \infty$ where $P(w,n)$ is a word complexity of w. We also show that w can not be among a certain collection of recursively constructed words.

1 Introduction

In 2004 de Mathan and Teulie [6] proposed the following problem which now is called p-adic Littlewood conjecture (PLC).

Conjecture (PLC)**.** *Let p be a prime number. Then every real x satisfies*

$$\liminf_{q\to\infty} q\cdot|q|_p\cdot||qx|| = 0 \qquad (1)$$

where $||\cdot||$ denotes the distance to the nearest integer.

It is widely believed to be easier than the famous Littlewood conjecture where the expression above is replaced by

$$\liminf_{q\to\infty} q\cdot||qx||\cdot||qy|| = 0.$$

Despite of the essential efforts from the mathematical communities both conjectures still remain open.

Assume that there is a counterexample x to PLC. Then it must satisfy

$$\inf_{q\in\mathbb{N}}\{q\cdot|q|_p\cdot||qx||\} \geqslant \epsilon \qquad (2)$$

for some $\epsilon > 0$. We denote the set of $x\in\mathbb{R}$ which satisfy the condition (2) by $\mathbf{Mad}_\epsilon$. So PLC is equivalent to saying that for all $\epsilon > 0$ the set $\mathbf{Mad}_\epsilon$ is empty.

It is already known that $\mathbf{Mad}_\epsilon$ is very "small". The condition (2) straightforwardly implies that x is badly approximable hence it belongs to the set of zero Lebesgue measure.

*Research supported by EPSRC Grant EP/L005204/1

Moreover $\mathbf{Mad}_\epsilon$ is included in the subset $\mathbf{Bad}_\epsilon$ of the set $\mathbf{Bad}$ of badly approximable numbers which is defined as follows

$$\mathbf{Bad}_\epsilon := \{x \in \mathbb{R} \ : \ \inf_{q\in\mathbb{N}} q \cdot ||qx|| \geqslant \epsilon\}.$$

In [6] it was shown that quadratic irrational x, the classical examples of badly approximable numbers, satisfy PLC. Later Bugeaud, Drmota and de Mathan [2] generalized that result to numbers which continued fraction expansion contain arbitrarily long periodic parts. In 2007 Einsiedler and Kleinbock [4] proved that $\mathbf{Mad}_\epsilon$ is of zero box dimension for every $\epsilon > 0$.

Numbers from $\mathbf{Bad}$ can easily be described in terms of their continued fraction expansion. We'll state this classical fact in terms of infinite words (the details can be found in [3], for example).

Fact 1. *Let $w_{CF}(x)$ be an infinite word composed of the partial quotients of the continued fraction expansion of $x = [0; a_1, a_2, \ldots] \in \mathbb{R}$. If $x \in \mathbf{Mad}_\epsilon$ then $w_{CF}(x) \in \mathbb{A}_N^{\mathbb{N}}$ where $N = \epsilon^{-1} + 1$ and $\mathbb{A}_N := \{1, 2, \ldots, N\}$. In the other words the word $w_{CF}(x)$ belongs to the finite alphabet $\mathbb{A}_N$.*

We call a word $w \in \mathbb{N}^{\mathbb{N}}$ recurrent if every finite block occurring in w occurs infinitely often. Then w is eventually recurrent if $\mathrm{T}^m w$ is recurrent for some positive integer m where T is a standard left shift transformation in $\mathbb{N}^{\mathbb{N}}$.

Recently Badziahin, Bugeaud, Einsiedler and Kleinbock [1] imposed restrictions on $w_{CF}(x)$ for potential counterexamples x to PLC.

Theorem (BBEK1)**.** *If $w_{CF}(x)$ is eventually recurrent then x satisfies PLC.*

Almost all well known classical infinite words such as Sturmian words or the Thue-Morse word, are recurrent so Theorem BBEK1 states that none of them can be a continued fraction expansion of the counterexample to PLC. Another corollary from this theorem is that for $x \in \mathbf{Mad}$ the complexity $P(w_{CF(x)}, n)$ as a function on n does not grow too slow. By the complexity $P(w, n)$ of the word w we mean the number of distinct blocks of length n which occur in w.

Corollary (BBEK2)**.** *If $x \in \mathbf{Mad}$ then $P(w_{CF}(x), n) - n \to \infty$ as $n \to \infty$.*

On the other hand another result from [1] states that the complexity of $x \in \mathbf{Mad}$ can not grow too fast as well.

Theorem (BBEK3)**.** *If $x \in \mathbf{Mad}$ then*

$$\lim_{n\to\infty} \frac{\log P(w_{CF}(x), n)}{n} = 0.$$

In other words Theorem BBEK3 says that the complexity $w_{CF}(x)$ of a counterexample to PLC can not grow exponentially.

The condition of Theorem BBEK1 can be easily reformulated to the following equivalent condition: *For every $n \in \mathbb{N}$ the word $\mathrm{T}^n w_{CF}(x)$ is not a limit point of the sequence* $\{\mathrm{T}^n w_{CF}(x)\}_{n\in\mathbb{N}}$. However it says nothing about the limit points of that sequence themselves. In this paper we will put rather restrictive conditions on them. The author does not know if they rule out every possible infinite word w (this would actually imply PLC) however they believe that there still exist numbers x which survive after imposing all discovered conditions for the potential counterexamples to PLC and therefore PLC still remains open.

After making necessary preparations in Sections 2 and 3 we state the core results of this paper in Section 4 which are pretty technical. Then Section 5 discusses various applications of that results to certain infinite words. In particular it covers Sturmian words and a big collection of words achieved by a certain recursive concatenation procedure. Finally all necessary proofs are provided.

2 Preliminaries

By $\mathrm{SL}_2^{\pm}(R)$ we denote the set of 2×2 matrices over the ring R with denominator ± 1. We will extensively use the homomorphism ψ from the set of finite words over the alphabet $\mathbb{N}$ to $\mathrm{SL}_2^{\pm}(\mathbb{Z})$ defined in the following way:

$$\text{for } a\in\mathbb{N},\ \psi(a) := A_a := \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}; \quad \text{for } w = a_1\dots a_n,\ \psi(w) := A_w = A_{a_1}\cdot\ldots\cdot A_{a_n}.$$

Let T be the left shift transform in $\mathbb{N}^{\mathbb{N}}$, w_n be the n-letter prefix of an infinite word w. For the prefixes of the particular word $w_{CF}(x)$ we will use the notation $w_n(x)$. Denote by $\tilde{\mathrm{T}}\ :\ [0,1)\to[0,1)$ a Gauss map defined as follows $\tilde{\mathrm{T}}(x) := \{1/x\}$. The classical results from the theory of continued fractions relate the notions defined above in the following way:

Fact 2. *For every irrational $x\in[0,1)$ we have*

$$\begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} = A_{w_n(x)};\quad \tilde{\mathrm{T}}^n(x) = \frac{||q_nx||}{||q_{n-1}x||};\quad w_{CF}(\tilde{\mathrm{T}}^nx) = T^nw_{CF}(x) \quad \textit{and}$$

$$\frac{q_n}{q_{n-1}} = [a_n; a_{n-1},\dots,a_1].$$

where p_n/q_n is the n'th convergent to x.

We extend the Gauss map $\tilde{\mathrm{T}}$ defined over $[0,1)$ to $[0,1)\times\mathbf{P}^1_{\mathbb{Q}_p}$ in the following way: $\tilde{\mathrm{T}}(x,\mathbf{x}_p) := (\tilde{\mathrm{T}}x, A_{a_1}\mathbf{x}_p)$ where $\tilde{\mathrm{T}}x$ is the standard Gauss map which can be written as $\tilde{\mathrm{T}}x = 1/x - a_1,\ a_1 = [1/x]$. In the same way we extend the shift map T to the pairs $(w,\mathbf{x}_p)\in\mathbb{N}^{\mathbb{N}}\times\mathbf{P}^1_{\mathbb{Q}_p}$: $\mathrm{T}(w,\mathbf{x}_p) := (\mathrm{T}w, A_{a_1}\mathbf{x}_p)$. One can check that $\mathrm{T}^n(w,\mathbf{x}_p)$ is calculated as follows

$$\mathrm{T}^n(w,x_p) = \left(\mathrm{T}^nw, (A_{w_n})^T\mathbf{x}_p\right).$$

This together with Fact 2 implies the remarkable property of the map T:

Fact 3. *For every $x\in[0,1)$,*

$$\mathrm{T}^n\left(w_{CF}(x), \begin{pmatrix}0\\1\end{pmatrix}\right) = \left(\mathrm{T}^nw_{CF}(x), \begin{pmatrix}q_{n-1}\\q_n\end{pmatrix}\right)$$

where q_n is the denominator of nth convergent to x.

We say that $\mathbf{w} = (\omega_1,\omega_2)\in\mathbf{P}^1_{\mathbb{Q}_p}$ is p-adically badly approximable if there exists $\epsilon>0$ such that $\forall(a,b)\in\mathbb{Z}\backslash\{(0,0)\}$ one has

$$|a\omega_1 + b\omega_2|_p\cdot\min\{|\omega_1^{-1}|_p, |\omega_2^{-1}|_p\} \geqslant \min\{|a|^{-2}, |b|^{-2}\}\cdot\epsilon.$$

Sometimes instead of projective coordinates we will use affine ones. In that case we say that $\omega\in\mathbb{Q}_p$ is p-adically badly approximable if $(\omega,1)$ is. We call the set of all p-adically badly approximable points by **PBad**. Then by analogy with the definition of $\mathbf{Bad}_\epsilon$ we define the set $\mathbf{PBad}_\epsilon$ as the subset of **PBad** containing those points $\mathbf{w}$ for which ϵ in the definition is fixed.

We equip the space $\mathbf{P}^1_{\mathbb{Q}_p}$ with the metrics defined as follows. Given $\mathbf{w} = (\omega_1, \omega_2), \mathbf{v} = (\upsilon_1, \upsilon_2) \in \mathbf{P}^1_{\mathbb{Q}_p}$ let

$$d(\mathbf{w}, \mathbf{v}) := |\omega_1\upsilon_2 - \omega_2\upsilon_1|_p \cdot \min\{|\omega_1|_p^{-1}, |\omega_2|_p^{-1}\} \cdot \min\{|\upsilon_1|_p^{-1}, |\upsilon_2|_p^{-1}\}.$$

Wherever possible we will take the coordinates (ω_1, ω_2) of $\mathbf{w}$ such that $\max\{|\omega_1|_p, |\omega_2|_p\} = 1$. If this happens we emphasize it by using slightly different notation: $\mathbf{w} \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$. One can see that for $\mathbf{w}, \mathbf{v} \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$ the definition of distance $d(\mathbf{w}, \mathbf{v})$ as well as the definition of $\mathbf{w}$ being p-adically badly approximable point becomes simpler. We will use the following property of $d(\cdot, \cdot)$.

Lemma 1. *Let $\mathbb{Z}_p$ be the set of p-adic integers and $A, B \in \mathrm{SL}_2^{\pm}(\mathbb{Z}_p)$ be two matrices such that $A \equiv B \pmod{p^k}$ for some $k \in \mathbb{N}$, i.e. the p-adic norm of each entry of the matrix $A - B$ is at most p^{-k}. Then for every two points $\mathbf{w}, \mathbf{v} \in \mathbf{P}^1_{\mathbb{Q}_p}$ one has*

$$d(A\mathbf{w}, \mathbf{v}) \leqslant \max\{d(B\mathbf{w}, \mathbf{v}), p^{-k}\}.$$

Proof. Denote $\mathbf{u} = (u_1, u_2) = A\mathbf{w}$ and $\mathbf{u}' = (u_1', u_2') = B\mathbf{w}$. For simplicity we will choose $\mathbf{w}, \mathbf{v} \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$. One can check that since p-adic norms of all entries of A are at most 1 then $\max\{|u_1|_p, |u_2|_p\} \leqslant \max\{|\omega_1|_p, |\omega_2|_p\}$. On the other hand since A is invertible then the inverse inequality is also true. This implies that $\mathbf{u} \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$ and by the same arguments $\mathbf{u}' \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$.

Now we calculate

$$d(\mathbf{u}, \mathbf{v}) = |u_1\upsilon_2 - u_2\upsilon_1|_p = |u_1'\upsilon_2 - u_2'\upsilon_1 + d_1\upsilon_2 - d_2\upsilon_1|_p.$$

where $\mathbf{d} = (d_1, d_2) = (A - B)\mathbf{w}$. Next,

$$d(\mathbf{u}, \mathbf{v}) \leqslant \max\{d(\mathbf{u}', \mathbf{v}), |d_1\upsilon_2 - d_2\upsilon_1|_p\}.$$

Since $A \equiv B \pmod{p^k}$ an upper bound for the second term of the maximum is p^{-k} which finishes the proof of the lemma. □

Consider the set $\mathrm{SL}_2^{\pm}(\mathbb{Z}_p)$. In accordance to the Jordan normal form of the matrices one can split it into two subsets:

- $\mathrm{SL}_{2,1}^{\pm}(\mathbb{Z}_p)$ which consists of all matrices having two different eigenvectors in $\mathbf{P}^1_{\mathbb{Q}_p}$.
- $\mathrm{SL}_{2,2}^{\pm}(\mathbb{Z}_p)$ which consists of matrices which are similar to one of the matrices

$$\begin{pmatrix} v & 0 \\ 1 & v \end{pmatrix}; \quad v \in \overline{\mathbb{Q}_p}.$$

Lemma 2. *Let $A \in \mathrm{SL}_{2,1}^{\pm}(\mathbb{Z}_p)$. Then there exists a positive integer $\kappa(A) \leqslant p^2$ such that for each eigenvalue λ of A one has $|\lambda^{\kappa(A)} - 1|_p \leqslant p^{-1}$.*

Proof. Both eigenvalues λ and λ' of A are the roots of the quadratic equation

$$\lambda^2 - \mathrm{tr}(A)\lambda + \det(A) = 0.$$

Since $\det(A) = \pm 1$, λ is a unit, so $|\lambda|_p = 1$. Further arguments follow the standard proof of Fermat Little theorem. We compose a complete list of representatives of residue classes in $\mathbb{Z}_p[\lambda]$ modulo p such that their p-adic norm equals one. Since all that residue classes are contained in the set $\{a + b\lambda \ : \ 0 \leqslant a, b < p\}$ there are at most p^2 elements on the list. We denote its size by $\kappa(A)$, then the list looks as follows: $x_1, x_2, \ldots, x_{\kappa(A)}$. If we multiply each element from the list by λ the resulting numbers will again represent each residue class $\mathbb{Z}_p[\lambda]$ modulo p with p-adic norm equals one. Then by looking at products we get

$$\prod_{i=1}^{\kappa(A)} x_i \equiv \prod_{i=1}^{\kappa(A)} \lambda x_i \pmod p \quad \Rightarrow \quad |\lambda^{\kappa(A)} - 1|_p \leqslant p^{-1}.$$

□

One can define the p-adic logarithm as the following series

$$\log x = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(x-1)^n}{n}.$$

It is well-defined on disc $|x-1|_p < 1$. Therefore by Lemma 2 the value $\log \lambda^{\kappa(A)}$ is well defined for every eigenvalue of $A \in \mathrm{SL}^{\pm}_{2,1}(\mathbb{Z}_p)$. Notice also that for $|x|_p \leqslant p^{-1}$ one has $|\log x|_p = |x-1|_p$. Moreover one can check that for $x, y \in \mathbb{Q}_p$ such that $|x-1|_p < 1$ and $|y-1|_p < 1$ the following formula is satisfied

$$|\log x - \log y|_p = \left|\log \frac{x}{y}\right|_p = \left|\frac{x}{y} - 1\right|_p = |x-y|_p. \tag{3}$$

Now we want to remove (for the reason which will become clear later) all matrices A from $\mathrm{SL}^{\pm}_{2,1}(\mathbb{Z}_p)$ such that one of their eigenvalues λ satisfies $\log \lambda^{\kappa(A)} = 0$. So we introduce another set

$$\widetilde{\mathrm{SL}}_2(\mathbb{Z}_p) := \left\{ A \in \mathrm{SL}^{\pm}_{2,1}(\mathbb{Z}_p) : \text{ for two eigenvectors } \lambda_1, \lambda_2 \text{ of } A \text{ one has } \log \lambda_{1,2}^{\kappa(A)} \neq 0 \right\}.$$

Lemma 3. *For every finite nonempty word $w \in \mathbb{N}^n$ one has $A_w \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$.*

Proof. Firstly we show that A_w has two distinct eigenvalues, so it is in $Sl^{\pm}_{2,1}(\mathbb{Z}_p)$. The eigenvalues of A are the roots of the equation $\lambda^2 - \mathrm{tr}(A)\lambda + \det(A) = 0$. Since $\det(A) = \pm 1$ there is only one possibility for $\lambda_1 = \lambda_2$, namely there should be $\mathrm{tr}(A) = 2$ and $\det(A) = 1$ but one can easily check that there are no words w with this property.

For algebraic λ the condition $\log \lambda^{\kappa(A)} = 0$ is only possible when λ is a root of unity. The only quadratic roots of unity are either roots of the equation $x^6 = 1$ or $x^4 = 1$. Therefore they must be roots of one of the following quadratic equations:

$$\begin{array}{rrr} x^2 - 1 = 0; & x^2 + 1 = 0; & x^2 - 2x + 1 = 0; \\ x^2 + 2x + 1 = 0; & x^2 - x + 1 = 0; & x^2 + x + 1 = 0. \end{array}$$

There are only two words $w_1 = 1$ and $w_2 = 2$ for which $|\mathrm{tr}(A_w)| \leqslant 2$. However an easy check shows that the eigenvalues of both A_1 and A_2 are not roots of unity. □

3 Sets LMad and $\mathbf{LMad}_\epsilon$

In attempt to make an expression from (1) small one can try to take q a linear combination of the denominators q_0 and q_0' of two consecutive convergents to x. Then we get the following

Lemma 4. *Let $q_0 < q_0'$ be the denominators of two consecutive convergents to $x \in \mathbf{Bad}_\epsilon$. Then for every $a, b \in \mathbb{Z}$ and $r = r_{a,b} = |aq_0 + bq_0'|$ we have*

$$r \cdot |r|_p \cdot ||rx|| \leqslant 4\max\{a^2, b^2\}(N+1) \cdot |r|_p \tag{4}$$

where $N = [\epsilon^{-1}] + 1$.

Proof. We just use two standard facts: $(N+1)q_0 > q_0'$ (by Fact 1) and $q_0||q_0x|| < 1$, $q_0'||q_0'x|| < 1$. Then we get

$$r \cdot |r|_p \cdot ||rx|| \leqslant (2\max|a|, |b|)^2 \cdot q_0' \cdot \frac{1}{q_0} \cdot |r|_p \leqslant 4\max\{a^2, b^2\}(N+1)|r|_p.$$

□

As the consequence of the lemma, if one can find $\mathbf{q}_0 = (q_0, q_0')$ and $a, b \in \mathbb{Z}$ such that $r_{a,b} \neq 0$ and $|r_{a,b}|_p < \frac{\epsilon}{4(N+1)} \cdot \min\{a^{-2}, b^{-2}\}$ then x is not in $\mathbf{Mad}_\epsilon$. With help of Fact 3 one can then show another key property of the extended shift map T.

Corollary. *If x is a counterexample to PLC then every limit point $(w, \mathbf{x}_p)$ of $\{T^n(w_{CF}(x), \binom{0}{1})\}_{n\in\mathbb{N}}$ satisfies the following property: there exists $\epsilon > 0$ such that for every $n \in \mathbb{N}$ one has $T^n(w, \mathbf{x}_p) \in \mathbb{A}_N^{\mathbb{N}} \times \mathbf{PBad}_\epsilon$ where $N = [\epsilon^{-1}] + 1$ as before.*

We define the set of pairs $(w, \mathbf{x}_p)$ which satisfy the conditions of this corollary by **LMad**. By $\mathbf{LMad}_\epsilon$ we define the subset of **LMad** containing those pairs for which the parameter ϵ is fixed.

By Fact 1 and the compactness of the set $\mathbb{A}_N^{\mathbb{N}}$ elements $\mathrm{T}^n(w_{CF}(x))$ belong to the compact set. It is also well known that $\mathbf{P}^1_{\mathbb{Q}_p}$ is compact. Therefore the sequence $\{T^n(w_{CF}(x), \binom{0}{1})\}_{n\in\mathbb{N}}$ must have at least one limit point. Moreover there always exist a minimal subset of $\overline{\{\mathrm{T}^n(w_{CF}(x), \binom{0}{1})\}}_{n\in\mathbb{N}}$ which is invariant under T, i.e. the subset which does not contain any other non-empty invariant closed subsets. It is of the form $\overline{\{\mathrm{T}^n(w, \mathbf{x}_p)\}}_{n\in\mathbb{N}}$ for some pair $\mathbf{x} = (w, \mathbf{x}_p)$. It is well known ([5][Theorem 1.5.9]) that in that case w is uniformly recurrent or in other words it is recurrent and for any factor u of w the distance between any two consecutive appearances of u in w is bounded above by some constant $d = d(u)$. For convenience by $\mathcal{W}_{CF}(x)$ we denote the set of limit points of the sequence $\{\mathrm{T}^n w_{CF}(x)\}_{n\in\mathbb{N}}$.

In this paper we investigate the set **LMad**. The ideal situation would be if one could show that $\mathbf{LMad} = \emptyset$. Then it would immediately follow that the set **Mad** of counterexamples to PLC is also empty. Unfortunately this is not the case. We'll show (Theorem 3) that **LMad** contains infinitely many elements $\mathbf{x}$. On the other hand all elements of **LMad** which we are able to construct in this paper have periodic part w. Bugeaud, Drmota and de Mathan [2] showed that periodic w can not be in $\mathcal{W}_{CF}(x)$ for $x \in \mathbf{Mad}$, therefore the constructed pairs $(w, \mathbf{x}_p) \in \mathbf{LMad}$ can not produce counterexamples to PLC. Hopefully **LMad** does not contain any more elements. So it will be very interesting to solve the following problem:

Problem A. *Is it true that for every $(w, \mathbf{x}_p) \in \mathbf{LMad}$ the word w is periodic?*

The positive answer to this problem will imply PLC. In this paper we discover various conditions on **LMad** which are quite restrictive but not restrictive enough to give a complete answer to Problem A.

It follows straightforwardly from the definition that the set **LMad** is invariant under T and so is the set $\mathbf{LMad}_\epsilon$ for every $\epsilon > 0$. Moreover it can be verified that $\mathbf{LMad}_\epsilon$ is also closed and therefore it is compact. In order to investigate compact invariant subsets of $\mathbf{LMad}_\epsilon$ it is sufficient to consider the minimal invariant subsets for which the word w is always uniformly recurrent. One can check that every minimal invariant subset of **LMad** described in Theorem 3 is finite. Therefore Problem A can be reformulated as follows:

Problem A' *Are there infinite minimal invariant subsets of* $\mathbf{LMad}_\epsilon$*?*

Remark. In [4] Einsiedler and Kleinbock posed a generalization of PLC in the following way: every pair $(x,y) \in \mathbb{R}_{>0} \times \mathbb{Q}_p$ satisfies

$$\inf_{a\in\mathbb{N}, b\in\mathbb{N}\cup\{0\}} \max\{|a|,|b|\} \cdot |ax-b| \cdot |ay-b|_p = 0. \qquad (EK)$$

We do not cover this conjecture here however it has close connection with Problem A. In particular by a similar construction to that used in the proof of Theorem 3 one can show that if $x \in \mathbb{R}_{>0}$ and $y \in \mathbb{Q}_p$ are irrational roots of the same quadratic polynomial then the condition (EK) fails which in turn means that the generalization of PLC is false.

4 Core results

Given $\mathbf{x} = (w, \mathbf{x}_p) \in \mathbb{A}_N^{\mathbb{N}} \times \mathbf{P}^1_{\mathbb{Q}_p}$ and $n \in \mathbb{N}$ we write $T^n\mathbf{x}$ as $(T^n w, \mathbf{x}_{p,n})$. Define

$$B_k(\mathbf{x}) := \left\{ \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbf{P}^1_{\mathbb{Q}_p} \;:\; \exists\, n \in \mathbb{N},\ \text{s.t. } d\left(\begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \mathbf{x}_{p,n}\right) \leqslant p^{-k} \right\}.$$

Roughly speaking the set $B_k(\mathbf{x})$ contains p^{-k}-neighborhoods of the elements $\mathbf{x}_{p,n}$. The following theorem lies at the heart of this paper.

Theorem 1. *Let* $A \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$*. Let* $\mathbf{w}_1 = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$ *and* $\mathbf{w}_2 = \begin{pmatrix}\omega_3\\ \omega_4\end{pmatrix}$ *be two eigenvectors of* A^T *with* $\omega_{1,2,3,4} \in \overline{\mathbb{Q}_p}$ *and* $\max\{|\omega_1|_p, |\omega_2|_p\} = \max\{|\omega_3|_p, |\omega_4|_p\} = 1$*. Consider* $\mathbf{x} = (w, \mathbf{x}_p) \in \mathbb{A}_N^{\mathbb{N}} \times \mathbf{P}^1_{\mathbb{Q}_p}$ *and define*

$$\epsilon_1 := d(\mathbf{x}_p, \mathbf{w}_1), \quad \epsilon_2 := d(\mathbf{x}_p, \mathbf{w}_2), \quad \epsilon_3 := |\log(\lambda_1^{4\kappa(A)})|_p, \quad \delta := \min\{\epsilon_1, \epsilon_2, p^{-1}\}$$

where λ_1 *is one of the eigenvalues of* A*. Assume that* $\delta \neq 0$*. Finally let* $m \in \mathbb{N}$ *and* $k \in \mathbb{N}$ *satisfy the inequality*

$$p^k \geqslant \frac{\sqrt{d(\mathbf{w}_1, \mathbf{w}_2)\cdot m}}{\epsilon_3 \cdot \delta \cdot \sqrt{2\epsilon_1\epsilon_2 \cdot p \cdot \kappa(A)}}. \qquad (5)$$

If

$$\{\mathbf{x}_p, A^T\mathbf{x}_p, \ldots, (A^T)^m\mathbf{x}_p\} \subset B_k(\mathbf{x}) \qquad (6)$$

then $\mathbf{x} \notin \mathbf{LMad}_\epsilon$ *for*

$$\epsilon = \sqrt{\frac{2\epsilon_1\epsilon_2 \cdot p \cdot \kappa(A)}{\epsilon_3^2\delta^2 \cdot d(\mathbf{w}_1, \mathbf{w}_2)\cdot m}}. \qquad (7)$$

Note that the values $\kappa(A)$, $d(\mathbf{w}_1, \mathbf{w}_2)$ and ϵ_3 are solely defined by the matrix A and since $A \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ the last two of them are always strictly positive. The value δ measures how "close" is $\mathbf{x}_p$ to one of the eigenvectors of A^T. If the parameters A and m are fixed then as δ tends to zero, the estimate (7) on ϵ tends to infinity. In other words smaller the value of δ, weaker the estimate for ϵ.

We will also need to work with matrices A of the form

$$A = D_a := \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

It is easily verified that $D_a \not\in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ so Theorem 1 is not applicable to it. However very similar (and even simpler) result is true for such matrices too.

Theorem 2. *Let $A = D_a$ for some $a \in \mathbb{Z}_p \backslash \{0\}$. Consider $\mathbf{x} = (w, \mathbf{x}_p) \in \mathbb{A}_N^{\mathbb{N}} \times \mathbf{P}^1_{\mathbb{Q}_p}$ and define $\delta := d((\begin{smallmatrix} a \\ 0 \end{smallmatrix}), \mathbf{x}_p) \cdot |a|_p$. Assume that $\delta \neq 0$. Let $m \in \mathbb{N}$ and $k \in \mathbb{N}$ satisfy the inequality $p^k \geqslant m \cdot (p\delta)^{-1}$. If* (6) *is satisfied:*

$$\{\mathbf{x}_p, A^T\mathbf{x}_p, \ldots, (A^T)^m\mathbf{x}_p\} \subset B_k(\mathbf{x})$$

then $\mathbf{x} \not\in \mathbf{LMad}_\epsilon$ for $\epsilon = p\delta^{-1}m^{-1}$.

On the other hand if $\delta = 0$ then $\mathbf{x} \not\in \mathbf{LMad}$.

5 Applications of Theorem 1

Theorem 1 itself is quite technical and imposes a lot of conditions on pairs $(w, \mathbf{x}_p)$. However it can be used to check that $\mathbf{x} \not\in \mathbf{LMad}$ for many classes of pairs $(w, \mathbf{x}_p)$. The most straightforward application of Theorem 1 is the case of periodic w.

Theorem 3. *Let $w \in \mathbb{A}_N^{\mathbb{N}}$ be a periodic infinite word and $l \in \mathbb{N}$ be the length of its minimal period. Then $(w, \mathbf{x}_p)$ is in **LMad** if and only if $\mathbf{x}_p$ coincides with one of the eigenvectors of $A^T_{w_l}$.*

The “only if” part of this theorem is a straightforward corollary of Theorem 1. We just take $A = A_{w_l}$ which by Lemma 3 is in $\widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$, take k arbitrarily large and take the biggest $m \in \mathbb{N}$ which satisfies (5). The proof of “if” part is postponed to Section 9.

Theorem 3 shows that the set **LMad** is infinite (at least countable). Also note that for $\mathbf{x} \in \mathbf{LMad}$ described in this theorem we have $\mathrm{T}^l\mathbf{x} = \mathbf{x}$ which in turn implies that the set $\{\mathrm{T}^n\mathbf{x}\}_{n\in\mathbb{N}}$ is finite. We believe that Theorem 3 describes all elements of **LMad** and therefore Problem A and Problem A’ have positive and negative answers respectively.

Next, we can show that for a big collection of words w which can be recurrently constructed by concatenations the pair $(w, \mathbf{x}_p)$ is never in **LMad**. We call $\mathcal{W}(\sigma_1, \sigma_2, \ldots, \sigma_n)$ a concatenation map if it is some composition of concatenations of words $\sigma_1, \ldots, \sigma_n$.

Theorem 4. *Let sequence of finite words over the alphabet $\mathbb{A}_N$ be constructed recursively as follows: $\sigma_1, \ldots, \sigma_m$ are given words of length 1 such that not all of them equal to each other. Then for every $n \in \mathbb{N}$,*

$$\sigma_{n+m} := \sigma_{n+m-1}\mathcal{W}(\sigma_n, \sigma_{n+1}, \ldots, \sigma_{n+m-1})$$

where $\mathcal{W}$ is a concatenation map. Assume that for every m-tuple of words $\eta_1, \ldots, \eta_m$ the equation

$$A_{\eta_m} = \widetilde{\mathcal{W}}(X, A_{\eta_1}, \ldots, A_{\eta_{m-1}})$$

has at most one solution $X \in \mathrm{SL}_2^{\pm}(\mathbb{Z}_p)$. Here $\widetilde{\mathcal{W}}$ is made of $\mathcal{W}$ where each concatenation is replaced by a product of matrices. Then for every limit word w of the sequence σ_n and every $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$, $(w, \mathbf{x}_p) \not\in \mathbf{LMad}$.

In fact the condition on $\sigma_1, \ldots, \sigma_m$ in the theorem can be weakened. We just need that not all of these words are the powers of the same finite word. However for the sake of simplicity we do not put this condition to the theorem.

One can easily check that the Fibonacci word w_{fib} satisfies the conditions of Theorem 4. Indeed it is the limit point of the sequence $\{\sigma_n\}_{n\in\mathbb{N}}$ constructed as follows:

$$\sigma_1, \sigma_2 \text{ are distinct one-digit words;} \quad \sigma_{n+1} = \sigma_n\sigma_{n-1}.$$

Therefore $(w_{fib}, \mathbf{x}_p)$ is never in **LMad**.

In view of **LMad** being invariant under T, the fact that there are infinite words w such that $(w, \mathbf{x}_p)$ is never in **LMad** for every $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$ implies the following

Corollary. *If $\{\mathrm{T}^n w\}_{n\in\mathbb{N}}$ is dense everywhere on $\mathbb{A}_N^{\mathbb{N}}$ then for every $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$, $(w, \mathbf{x}_p) \notin$* **LMad**.

The next application shows that if $(w, \mathbf{x}_p) \in$ **LMad** then the complexity of the word w can not grow too slow.

Theorem 5. *Let non-periodic $w \in \mathbb{A}_N^{\mathbb{N}}$ be such that $\forall n \in \mathbb{N}$, $P(w, n) \leqslant n + C$ for some positive absolute constant C. Then $\mathbf{x} = (w, \mathbf{x}_p) \notin$* **LMad** *for every $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$.*

In particular this theorem covers all Sturmian words and therefore for every counterexample x to PLC, $\mathcal{W}_{CF}(x)$ must not be Sturmian.

We finish this section with nice combinatorial condition on a word w which guarantees that $(w, \mathbf{x}_p)$ does never belong to **LMad**. Before we do that we define a sequence of bipartite graphs $G_n(S_n, T_n, E_n)$ related to w. Their definition distantly resembles more classical Rauzy graphs for infinite words. Both S_n and T_n are the sets of all factors of w of length n. Then Vertices $s \in S_n$ and $t \in T_n$ are linked with an edge iff the word st is a factor of w.

Theorem 6. *Let $w \in \mathbb{A}_N^{\mathbb{N}}$ be a non-periodic uniformly recurrent word. If a number of connected components in G_n is bounded by an absolute constant independent of n then $(w, \mathbf{x}_p) \notin$* **LMad** *for every $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$.*

Remark. None of the results in this section cover the Thue-Morse word w_{tm}. However the author believes that Theorem 1 itself can be applied to it in order to show that $(w_{tm}, \mathbf{x}_p)$ is never in **LMad**. Anyway it would be interesting to check if there is any prime p and point $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$ such that $(w_{tm}, \mathbf{x}_p) \in$ **LMad**.

6 Proof of Theorems 1 and 2

Lemma 5. *Let $\mathbf{q} = (q, q') \in B_k(\mathbf{x})$ and $\mathbf{u} = (u, v) \in \mathbb{Z}^2$. Then if*

$$|(\mathbf{u}, \mathbf{q})|_p \cdot \min\{|q^{-1}|_p, |(q')^{-1}|_p\} \leqslant \delta$$

for some positive δ then there exists $l \in \mathbb{N}$ such that

$$|(\mathbf{u}, \mathbf{x}_{p,l})|_p \cdot \min\{|x_{p,l}^{-1}|_p, |(x'_{p,l})^{-1}|_p\} \leqslant \max\{\delta, p^{-k}\} \quad \textit{where} \quad \mathbf{x}_{p,l} = (x_{p,l}, x'_{p,l}).$$

Proof. Since $\mathbf{q} \in B_k(\mathbf{x})$ then there exists $\mathbf{x}_{p,l}$ such that $d(\mathbf{q}, \mathbf{x}_{p,l}) \leqslant p^{-k}$. Without loss of generality assume that $|q'|_p \geqslant |q|_p$. Now we calculate

$$|(\mathbf{u}, \mathbf{x}_{p,l})|_p = |ux_{p,l} + vx'_{p,l}|_p = |(q')^{-1}(uq'x_{p,l} - uqx'_{p,l} + uqx'_{p,l} + vq'x'_{p,l})|_p$$

$$\leqslant \max\{\max\{|x_{p,l}|_p, |x'_{p,l}|_p\} \cdot u \cdot d(\mathbf{q}, \mathbf{x}_{p,l}), |x'_{p,l}|_p \cdot |(q')^{-1}|_p \cdot |(\mathbf{u}, \mathbf{q})|_p\}$$
$$\leqslant \max\{|x_{p,l}|_p, |x'_{p,l}|_p\} \cdot \max\{p^{-k}, \delta\}.$$

By dividing both sides of the inequality by $\max\{|x_{p,l}|_p, |x'_{p,l}|_p\}$ we get the statement of the lemma. □

Proof of Theorem 1. The idea is to construct a sequence of points $\mathbf{q}_n \in B_k(\mathbf{x})$ and to show that one of them do not lie in $\mathbf{PBad}_\epsilon$. Define $\mathbf{q}_0 = (q_0, q'_0)$ such that $\max\{|q_0|_p, |q'_0|_p\} = 1$ and $\mathbf{q}_0 = \mathbf{x}_p$. Represent the vector $\mathbf{q}_0$ in the basis $\mathbf{w}_1$ and $\mathbf{w}_2$: $\mathbf{q}_0 = \alpha\mathbf{w}_1 + \beta\mathbf{w}_2$ where by Cramer's rule

$$\alpha = \frac{\det(\mathbf{q}_0, \mathbf{w}_2)}{\det(\mathbf{w}_1, \mathbf{w}_2)}, \quad \beta = \frac{\det(\mathbf{w}_1, \mathbf{q}_0)}{\det(\mathbf{w}_1, \mathbf{w}_2)}.$$

Since $\mathbf{q}_0, \mathbf{x}_1, \mathbf{w}_2 \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$ one can check that

$$|\alpha|_p = \frac{d(\mathbf{q}_0, \mathbf{w}_2)}{d(\mathbf{w}_1, \mathbf{w}_2)} = \frac{\epsilon_2}{d(\mathbf{w}_1, \mathbf{w}_2)} \quad \text{and} \quad |\beta|_p = \frac{d(\mathbf{q}_0, \mathbf{w}_1)}{d(\mathbf{w}_1, \mathbf{w}_2)} = \frac{\epsilon_1}{d(\mathbf{w}_1, \mathbf{w}_2)}. \tag{8}$$

Define $\mathbf{q}_n = (q_n, q'_n)$ as follows: $\mathbf{q}_n = (A^T)^n \mathbf{q}_0$. Vectors $\mathbf{w}_1$ and $\mathbf{w}_2$ are eigenvectors of A^T therefore

$$\mathbf{q}_n = \lambda_1^n \cdot \alpha\mathbf{w}_1 + \lambda_2^n \cdot \beta\mathbf{w}_2.$$

All entries of $(A^T)^n$ have p-adic norm at most 1, and moreover $(A^T)^n$ is invertible. Therefore one can repeat the same arguments as in the proof of Lemma 1 to show that $\max\{|q_n|_p, |q'_n|_p\} = \max\{|q_0|_p, |q'_0|_p\} = 1$ or $\mathbf{q}_n \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$.

For an arbitrary integer vector $\mathbf{u} = (u, v)$ one has $(\mathbf{u}, \mathbf{q}_n) = A\lambda_1^n + B\lambda_2^n$ where $A = A(u, v) = \alpha \cdot (\mathbf{u}, \mathbf{w}_1), B = B(u, v) = \beta \cdot (\mathbf{u}, \mathbf{w}_2)$.

From the equation for eigenvalues $\lambda_{1,2}$ one has $\lambda_1 \cdot \lambda_2 = \pm 1$ and $|\lambda_{1,2}|_p = 1$. Therefore $\lambda_1^2 = \lambda_2^{-2}$. This gives us the following

$$|\tilde{Q}_n|_p := |(\mathbf{u}, \mathbf{q}_{2\kappa(A)\cdot n})|_p = |A|_p \cdot \left|\frac{B}{A} + \lambda^n\right|_p. \tag{9}$$

where $\lambda = \lambda_1^{4\kappa(A)}$. Note that by Lemma 2, $|\lambda - 1|_p \leqslant p^{-1}$ and therefore $|\log\lambda|_p = |\log(\lambda_1^{4\kappa(A)})|_p = \epsilon_3 \leqslant p^{-1}$.

In the rest of the proof we will construct integers u and v such that for some $n \in \mathbb{N}$ the value of $|\tilde{Q}_n|_p$ becomes so small that $\mathbf{q}_{2\kappa(A)\cdot n}$ is surely out of $\mathbf{PBad}_\epsilon$. Then, using the fact that $\mathbf{q}_{2\kappa(A)\cdot n}$ is in $B_k(\mathbf{x})$ one concludes that $\mathbf{x}$ is not in $\mathbf{LMad}_\epsilon$.

We want to construct u and v such that $p\epsilon_3|A|_p > |A + B|_p$. Then it will imply that $|1 + B/A|_p < 1$ and this will enable us to use the idea from [2]. By Dirichlet pigeonhole principle one can choose $(u, v) \in \mathbb{Z}^2\backslash\{0\}$ such that

$$|A + B|_p = |uq_0 + vq'_0|_p \leqslant p(\epsilon_3\delta)^2;$$
$$|u|, |v| < (\epsilon_3\delta)^{-1}.$$

Note that since $v \in \mathbb{Z}$ then $|v|_p > \epsilon_3\delta$. Rewrite the value $|(\mathbf{u}, \mathbf{w}_1)|_p$ in the following way

$$|(\mathbf{u}, \mathbf{w}_1)|_p = |q_0|_p^{-1} \cdot |\omega_1(uq_o + vq'_0) + (\omega_2 q_0 - \omega_1 q'_0)v|_p.$$

Since $|\omega_1|_p \leqslant 1$, an upper bound for the first summand is

$$|\omega_1(uq_o + vq'_0)|_p \leqslant p(\epsilon_3\delta)^2$$

and for the second summand it is

$$|(\omega_2 q_0 - \omega_1 q_0')v|_p = \epsilon_1 \cdot |v|_p > \epsilon_3\delta^2 \geqslant p(\epsilon_3\delta)^2.$$

Therefore

$$|(\mathbf{u}, \mathbf{w}_1)|_p = \frac{\epsilon_1 \cdot |v|_p}{|q_0|_p}.$$

By the construction we have $|A+B|_p \leqslant p(\epsilon_3\delta)^2$ and we just showed that

$$|A|_p = |\alpha \cdot (\mathbf{u}, \mathbf{w}_1)|_p \overset{(8)}{=} \frac{\epsilon_1\epsilon_2 \cdot |v|_p}{|q_0|_p \cdot d(\mathbf{w}_1, \mathbf{w}_2)}.$$

Notice that $|q_0|_p \cdot d(\mathbf{w}_1, \mathbf{w}_2) = |\omega_4(q_0\omega_1 - q_0'\omega_2) - \omega_2(q_0\omega_3 - q_0'\omega_4)|_p \leqslant \max\{\epsilon_1, \epsilon_2\}$. This finally gives the following lower estimate for $|A|_p$:

$$\epsilon_3|A|_p \geqslant \epsilon_3 \cdot \min\{\epsilon_1, \epsilon_2\} \cdot |v|_p > (\epsilon_3\delta)^2 \geqslant p^{-1} \cdot |A+B|_p.$$

So the aim is proved. Now we shall give an upper bound for $|A|_p$. If $|q_0|_p < \epsilon$ where ϵ is given by (7) then we consider $\mathbf{u} = (1,0)$ and $|(\mathbf{u}, \mathbf{q}_0)|_p < \epsilon$ and by Lemma 5 with $\epsilon \geqslant p^{-k}$ we get

$$|(\mathbf{u}, \mathbf{x}_{p,l})|_p \cdot \min\{|\mathbf{x}_{p,l}^{-1}|_p, |(\mathbf{x}_{p,l}')^{-1}|_p\} \leqslant \epsilon$$

for some $l \in \mathbb{N}$. This implies that $\mathbf{x}_{p,l} \notin \mathbf{PBad}_\epsilon$ and $(w, \mathbf{x}_p)$ is not in $\mathbf{LMad}_\epsilon$ anyway. Hence we can assume that $|q_0|_p \geqslant \epsilon$ and then

$$|A|_p \leqslant \epsilon_1\epsilon_2 \cdot \epsilon^{-1} \cdot (d(\mathbf{w}_1, \mathbf{w}_2))^{-1}. \tag{10}$$

Next, estimate the value $|\frac{B}{A} + \lambda^n|_p$. Since by Lemma 2, $|\lambda - 1|_p \leqslant p^{-1}$ and $|\frac{B}{A} + 1|_p < 1$ we can use the property (3) of p-adic logarithm:

$$\left|\frac{B}{A} + \lambda^n\right|_p = \left|\log\left(\frac{-B}{A}\right) - n\log\lambda\right|_p < \left|\frac{\log(-B/A)}{\log\lambda} - n\right|_p.$$

Now we show that $\log(-B/A)/\log\lambda$ lies in $\mathbb{Q}_p$. This fact is proved in [2] but for the sake of completeness we repeat it here. It is trivial if $\lambda \in \mathbb{Q}_p$. Otherwise there exists a unique $\mathbb{Q}_p$-automorphism σ of $\mathbb{Q}_p(\lambda)$ different from the identity. We have $\sigma(\lambda) = 1/\lambda$ and therefore $\sigma\log(\lambda) = \log(\sigma(\lambda)) = -\log\lambda$. Next,

$$A\lambda^n + B\lambda^{-n} = (\mathbf{u}, \mathbf{q}_{4\kappa(A)\cdot n}) = \sigma((\mathbf{u}, \mathbf{q}_{4\kappa(A)\cdot n})) = \sigma(A)\lambda^{-n} + \sigma(B)\lambda^n.$$

Since it is true for every natural n then we have $\sigma(A) = B$ and $\sigma(B) = A$. Combining these equations for σ together we get

$$\sigma\left(\frac{\log(-B/A)}{\log\lambda}\right) = \frac{\log(-B/A)}{\log\lambda}.$$

Further,

$$\left|\log\left(-\frac{B}{A}\right)\right|_p = \left|\frac{B}{A} + 1\right|_p < p\epsilon_3 = p \cdot |\log\lambda|_p.$$

therefore $|\log(-B/A)/\log\lambda|_p < p$. This together with the fact that $\log(-B/A)/\log\lambda \in \mathbb{Q}_p$ implies that this number is also in $\mathbb{Z}_p$. Whence there exists integer n within the range $0 \leqslant n < p^d$ such that

$$\left|\frac{\log(-B/A)}{\log\lambda} - n\right|_p \leqslant p^{-d}.$$

In other words there exists $n \in \mathbb{Z}$ within the range $0 \leqslant n < N$ such that

$$\left|\frac{B}{A} + \lambda^n\right| \leqslant \frac{p}{N}.$$

One can choose $1 \leqslant n \leqslant \frac{m}{2\kappa(A)}$ such that

$$|\tilde{Q}_n|_p \leqslant |A|_p \cdot \frac{2p \cdot \kappa(A)}{m} \overset{(10)}{\leqslant} \frac{2\epsilon_1\epsilon_2 \cdot p \cdot \kappa(A)}{\epsilon \cdot d(\mathbf{w}_1, \mathbf{w}_2) \cdot m}.$$

Then by substituting the formula (7) for ϵ and using that $|u|, |v| < (\epsilon_3\delta)^{-1}$ we get $\max\{u^2, v^2\} \cdot |\tilde{Q}_n|_p < \epsilon$. Since $2\kappa(A) \cdot n \leqslant m$, vector $\mathbf{q}_{2\kappa(A)\cdot n}$ lies in the set $B_k(\mathbf{x})$. Therefore Lemma 5 is applicable here which in turn means that there exists $l \in \mathbb{N}$ such that

$$|(\mathbf{u}, \mathbf{x}_{p,l})|_p \cdot \min\{|x_{p,l}|_p^{-1}, |x'_{p,l}|_p^{-1}\} \leqslant \max\{|\tilde{Q}_n|_p, p^{-k}\}.$$

By (5) we estimate the value p^{-k} to finally get the bound

$$|(\mathbf{u}, \mathbf{x}_{p,l})|_p \cdot \min\{|x_{p,l}|_p^{-1}, |x'_{p,l}|_p^{-1}\} < \epsilon \cdot \min\{u^{-2}, v^{-2}\}.$$

Hence $\mathbf{x}_{p,l} \notin \mathbf{PBad}_\epsilon$ and $\mathbf{x} \notin \mathbf{LMad}_\epsilon$.

Proof of Theorem 2. As before represent $\mathbf{x}_p$ as (q_0, q'_0) where $\max\{|q_0|_p, |q'_0|_p\} = 1$ and denote it by $\mathbf{q}_0$. In this case one can easily check that $\delta = |aq'_0|_p$. By $\mathbf{q}_n$ we denote the point $(A^T)^n\mathbf{q}_0$ and as in the proof of the previous theorem we have $\max\{|q_n|_p, |q'_n|_p\} = 1$. Note that $(D_a^T)^n = D_{na}^T$ so one can easily get an explicit formula for $\mathbf{q}_n$:

$$\mathbf{q}_n = (q_0 + na \cdot q'_0, q'_0).$$

Firstly consider the situation when $\delta = 0$. In that case we should have $q'_0 = 0$ which straightforwardly implies that $\mathbf{x}_p \notin \mathbf{PBad}_\epsilon$ for an arbitrarily small ϵ. One just need to consider $\mathbf{u} = (1, 0)$ and then $(\mathbf{u}, \mathbf{q}_0) = 0$.

Now we can assume that $\delta > 0$. By Dirichlet pigeonhole principle one can choose $\mathbf{u} = (u, v) \in \mathbb{Z}^2/\{0\}$ such that

$$|(\mathbf{u}, \mathbf{q}_0)|_p \leqslant p\delta^2;$$
$$|u|, |v| < \delta^{-1}.$$

Since $|v|_p > \delta$ and $|aq'_0|_p = \delta$ we get

$$|(\mathbf{u}, \mathbf{q}_0)|_p \leqslant p\delta^2 < p \cdot |v|_p \cdot |aq'_0|_p = p \cdot |vaq'_0|_p.$$

This implies that $|(\mathbf{u}, \mathbf{q}_0)|_p \leqslant |vaq'_0|_p$ and therefore

$$\frac{(\mathbf{u}, \mathbf{q}_0)}{vaq'_0} \in \mathbb{Z}_p$$

One can write $(\mathbf{u}, \mathbf{q}_n)$ as

$$(\mathbf{u}, \mathbf{q}_n) = (\mathbf{u}, \mathbf{q}_0) + nvaq'_0,$$

hence there always exists an integer n within the range $0 \leqslant n < p^d$ such that

$$|(\mathbf{u}, \mathbf{q}_n)|_p = |vaq'_0|_p \cdot \left|\frac{(\mathbf{u}, \mathbf{q}_0)}{vaq'_0} - n\right|_p \leqslant \delta p^{-d}.$$

We choose $0 \leqslant n < m$ such that $|(\mathbf{u}, \mathbf{q}_n)|_p \leqslant p\delta m^{-1}$ and

$$\max\{u^2, v^2\}|(\mathbf{u}, \mathbf{q}_n)|_p < p\delta^{-1}m^{-1} = \epsilon.$$

then since $n \leqslant m$ we have $\mathbf{q}_n \in B_k(\mathbf{x})$ and therefore by Lemma 5 there exists $l \in \mathbb{N}$ such that

$$\max\{u^2, v^2\} \cdot |(\mathbf{u}, \mathbf{x}_{p,l})|_p \cdot \min\{|x_{p,l}|_p^{-1}, |x'_{p,l}|_p^{-1}\} < \max\{u^2, v^2\} \cdot \max\{|(\mathbf{u}, \mathbf{q}_n)|_p, p^{-k}\} \leqslant \epsilon.$$

Hence $\mathbf{x}_{p,l} \notin \mathbf{PBad}_\epsilon$ and $\mathbf{x} \notin \mathbf{LMad}_\epsilon$.

7 Some relations within words

In this section we consider several corollaries from Theorem 1 which will be more suitable for applications to various particular words $w \in \mathbb{A}_N^{\mathbb{N}}$. They will also provide some evidence that the conditions in this theorem together with Theorem 2 impose quite restrictive conditions on $\mathbf{x} \in \mathbf{LMad}$.

Given $k \in \mathbb{N}$ and an infinite or finite word w over alphabet $\mathbb{A}_N$ we define the set

$$U_k(w) := \{\phi_k(A_{w_n})) \in \mathrm{SL}_2^{\pm}(\mathbb{Z}/p^k\mathbb{Z}) \ : \ n \in \mathbb{Z}_{\geqslant 0}\}$$

where $\phi_k \ : \mathrm{SL}_2^{\pm}(\mathbb{Z}) \mapsto \mathrm{SL}_2^{\pm}(\mathbb{Z}/p^k\mathbb{Z})$ is the canonical homomorphism. In other words it is the set of all matrixes correspondent to the prefixes w_n modulo p^k. Roughly speaking Theorem 1 says that if $U_k(w)$ contains a chain $A, A^2, \ldots, A^m$ with $A \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ then either $\mathbf{x}_p$ coincides with one of the eigenvectors of A or $(w, \mathbf{x}_p)$ is not in $\mathbf{LMad}_\epsilon$ for some ϵ which can be explicitly calculated. Formally we have the following

Corollary 1. *Let $\mathbf{x} = (w, \mathbf{x}_p) \in \mathbb{A}_N^{\mathbb{N}} \times \mathbf{P}^1_{\mathbb{Q}_p}$. Suppose that there exists a matrix $A \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ such that*

$$\phi_k(A), \phi_k(A^2), \ldots \phi_k(A^m) \in U_k(w) \tag{11}$$

where the parameters $m, k \in \mathbb{N}$ satisfy the condition (5). Assume also that the parameter δ defined in Theorem 1 for the matrix A^T is not zero. Then $\mathbf{x} \notin \mathbf{LMad}_\epsilon$ for ϵ given by (7).

To check it we basically use Lemma 1 which shows that (6) follows from (11). Then all the conditions of Theorem 1 are satisfied.

In particular we can guarantee the condition (11) if $\phi_k(A) \cdot U_k(w) = U_k(w)$. Since $\mathrm{Id} \in U_k(w)$ then in this case every integer power $\phi_k(A^m)$ will belong to $U_k(w)$. In other words the condition (6) will be always satisfied and the value m from Corollary 1 will be only restricted by (5). As soon as $\mathbf{x}_p$ does not coincide with an eigenvector of A one can make m arbitrarily large and ϵ arbitrarily small as k tends to infinity. We will show in a minute that the situation when $\phi_k(A) \cdot U_k(w) = U_k(w)$ happens quite often.

One can easily check that $U_k(w)$ is always finite because the space it lies in is finite. It is also easy to check that $\#U_k(w) \to \infty$ as $k \to \infty$. The next proposition gives information about the structure of sets $U_k(w)$.

Proposition 1. *Let w be a recurrent word. Then for each $m \in \mathbb{N}$ and $k \in \mathbb{N}$ one has*

$$\phi_k(A_{w_m}) \cdot U_k(\mathrm{T}^m w) = U_k(w). \tag{12}$$

Proof. We first prove the following auxiliary statement: there exists $m \in \mathbb{N}$ such that $\phi_k(A_{w_m}) = \mathrm{Id}$. To show it we construct the sequence u_n of prefixes of w by the following rule.

- $u_1 := w_1$.
- Given u_n we take the prefix u_{n+1} such that it ends with u_n. In other words $u_{n+1} = v_{n+1}u_n$ for some word v_{n+1}. We can always do that because w is recurrent.

Because the set $\mathrm{SL}_2^{\pm}(\mathbb{Z}/p^k\mathbb{Z})$ is finite we can find $s, t \in \mathbb{N}$ such that $\phi_k(A_{u_s}) = \phi_k(A_{u_{s+t}})$. Then notice that

$$u_{s+t} = v_{s+t}v_{s+t-1} \ldots v_{s+1}u_s.$$

By substituting this to the matrix equality we get that $\phi_k(A_{v_{s+t}\ldots v_{s+1}}) = \mathrm{Id}$. Finally the observation that $v_{s+t} \ldots v_{s+1} = w_m$ is the prefix of w finishes the proof of the auxiliary statement.

Now we can prove the proposition. We will prove (12) for $m = 1$. The rest can easily be done by induction. The inclusion $\phi_k(A_{w_1}) \cdot U_k(\mathrm{T}w) \subseteq U_k(w)$ is straightforward. Indeed for every prefix u of $\mathrm{T}w$ the word w_1u is the prefix of w and therefore $\phi_k(A_{w_1}A_u) = \phi_k(A_{w_1u}) \in U_k(w)$. For inverse inclusion we only need to check that Id belongs to $\phi_k(A_{w_1}) \cdot U_k(\mathrm{T}w)$. Other elements of $U_k(w)$ correspond to prefixes w_n which start with the letter w_1 and this fact straightforwardly implies that they also belong to $\phi_k(A_{w_1}) \cdot U_k(\mathrm{T}w)$. On the other hand by the auxiliary statement one can represent Id as $\phi_k(A_{w_m})$ where the word w_m starts with w_1 as well. The proof is finished. □

Since there are only $\#U_k(w)$ different elements $\phi_k(A_{w_m})$ then Proposition 1 shows that the collection $\mathbf{U}_k := \{U_k(\mathrm{T}^m w) \ : \ m \in \mathbb{Z}_{\geqslant 0}\}$ consists of at most $\#U_k(w)$ elements. On the other hand if $\#\mathbf{U}_k < \#U_k(w)$ then one can find two prefixes w_m, w_n with $\phi_k(A_{w_m}) \neq \phi_k(A_{w_n})$ such that

$$\phi_k(A_{w_m}^{-1}) \cdot U_k(w) = \phi_k(A_{w_n}^{-1}) \cdot U_k(w).$$

Without loss of generality assume that $m > n$. Then this leads us to $\phi_k(A_u) \cdot U_k(\mathrm{T}^n w) = U_k(\mathrm{T}^n w)$ where $w_n u = w_m$. By Lemma 3, $A_u \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ and we also have $\phi_k(A_u) \neq \mathrm{Id}$ so the condition (11) is satisfied for $A = A_u$. Then the application of Corollary 1 will give us that either $\mathbf{x}_p$ is an eigenvalue of A_u or $\mathrm{T}^n\mathbf{x} \notin \mathbf{LMad}_\epsilon$ for ϵ defined by (7). However with help of only this basic observation we do not have a big control on ϵ. To use Corollary 1 in full we need some quantitative result of this kind which will be true for an arbitrarily large k.

Another useful corollary of Proposition 1 is that for every $m \in \mathbb{N}$ the sets $U_k(\mathrm{T}^m w)$ have the same size.

For every $n \in \mathbb{N}$ and every infinite word $w \in \mathbb{A}_N^{\mathbb{N}}$ we define the sets

$$V(n, w) := \{A_{w_m} \ : \ w_n \text{ is the prefix of } \mathrm{T}^m w\}$$

and $V_k(n, w) := \phi_k(V(n, w))$. One can easily check that the sets $V(n, w)$ are nested as n grows: $V(n_1, w) \subset V(n_2, w)$ for $n_1 \geqslant n_2$. The same is surely true for their projections $V_k(n, w)$. If w is recurrent then $V(n, w)$ is always infinite for all $n \in \mathbb{N}$, however $V_k(n, w)$ is obviously finite. We also define the set $Vp(n, w)$ which coincides with $V(n, w)$ but every element in $V_p(n, w)$ is considered as a matrix over $\mathbb{Z}_p$. Finally let

$$Vp(w) := \bigcap_{n=1}^{\infty} \overline{Vp(n, w)}.$$

We can not say anything about whether it is finite or not. However it is always non-empty since obviously $\mathrm{Id} \in Vp(w)$.

Proposition 2. *Let $w \in \mathbb{A}_N^{\mathbb{N}}$ be recurrent word. For each $k \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that for every $A \in V_k(n, w)$ we have $A \cdot U_k(w) = U_k(w)$.*

Proof. For each matrix $B \in U_k(w)$ associate the value $n(B)$, the length of the shortest word $w_{n(B)}$ such that $B = \phi_k(A_{w_{n(B)}})$. Since there are finitely many elements in $U_k(w)$ we can define $n := \max_{B \in U_k(w)}\{n(B)\}$. By the construction of n for every infinite word w^* which starts with w_n one has $U_k(w^*) \supset U_k(w)$.

Now for each $m \in \mathbb{N}$ such that $A_{w_m} \in V(n, w)$ by definition we have that the word $\mathrm{T}^m w$ starts with w_n. Therefore an application of Proposition 1 gives us $U_k(w) \subset U_k(\mathrm{T}^m w) = \phi_k(A_{w_m}) \cdot U_k(w)$. Or in other words, $\forall A \in V_k(n, w)$ one has $A \cdot U_k(w) \supset U_k(w)$. Finally since two sets $U_k(w)$ and $U_k(\mathrm{T}^m w)$ have the same cardinality we have the equality $A \cdot U_k(w) = U_k(w)$. □

8 Relation between $Vp(w)$ and LMad. Proof of Theorem 4

Proposition 2 shows that the condition (11) is satisfied for each $A \in V_k(n,w)$ where n is large enough. This observation gives rise to the following

Theorem 7. *Let $A_1, A_2 \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ be such that their eigenvectors $\mathbf{w}_{1,2,3,4} \in \mathbf{P}^1_{\mathbb{Q}_p}$ are all distinct. Let $w \in \mathbb{A}_N^{\mathbb{N}}$. Assume that for some $k \in \mathbb{N}$ and for all $n \in \mathbb{N}$, $\phi_k(A_1), \phi_k(A_2) \in V_k(n,w)$. Then for each $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$, $(w, \mathbf{x}_p) \notin \mathbf{LMad}_\epsilon$ where $\epsilon \gg_{A_1,A_2,p} p^{-k}$.*

Here we used the Vinogradov symbol: $x \gg_{A_1,A_2,p} y$ means that $x \geqslant c \cdot y$ where c is a positive constant dependent on A_1, A_2 and p only.

Proof. Consider the point $\mathbf{x} = (w, \mathbf{x}_p)$. Since all the values $\mathbf{w}_1, \ldots, \mathbf{w}_4$ are distinct then

$$\max\{\min\{d(\mathbf{x}_p, \mathbf{w}_1), d(\mathbf{x}_p, \mathbf{w}_2)\}, \min\{d(\mathbf{x}_p, \mathbf{w}_3), d(\mathbf{x}_p, \mathbf{w}_4)\}\} \gg_{A_1,A_2,p} 1.$$

Without loss of generality assume that the maximum above is reached for $\mathbf{w}_1$ and $\mathbf{w}_2$. Choose the matrix $A = A_1$. Then the estimate on the parameter δ from Theorem 1 is $\delta \gg_{A_1,A_2,p} 1$.

We have that $\phi_k(A)$ is in $V_k(n,w)$ for all $n \in \mathbb{N}$. Therefore by Proposition 2 we have $\phi_k(A) \cdot U_k(w) = U_k(w)$ and therefore (11) is true for an arbitrary $m \in \mathbb{N}$. Choose the biggest possible m such that the condition (5) is satisfied, then $m \asymp p^{2k}$. Now Corollary 1 implies that

$$\mathbf{x} \notin \mathbf{LMad}_\epsilon \ \text{ for } \ \epsilon \overset{(7)}{\gg}_{A_1,A_2,p} m^{-1/2} \gg_{A_1,A_2,p} p^{-k}.$$

□

Note that in Theorem 7 the estimate for ϵ depends only on A_1, A_2 and p but it does not depend on k. This simple observation makes the following corollary true.

Corollary 2. *If in terms of Theorem 7 one additionally has that $A_1, A_2 \in Vp(w)$ then $\mathbf{x} \notin \mathbf{LMad}$.*

Corollary shows that for $(w, \mathbf{x}_p) \in \mathbf{LMad}$ the set $Vp(w)$ must be very small in a sense that it should not contain two "independent" matrices, i.e. the matrices from $\widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ which eigenvectors do not intersect. This observation is sufficient to prove Theorem 4.

Proof of Theorem 4. Firstly note that for $n > m$ the word σ_{n-1} is the prefix of σ_n and therefore it is the prefix of σ_l for any $l \geqslant n$. This in turn implies that σ_{n-1} is a prefix of w. Let $L(n)$ be the length of σ_n. Then for $n > 2m$, σ_{n-m} is the prefix of $\mathrm{T}^{L(n-1)}\sigma_n$. These two facts together imply that $A_{\sigma_{n-1}} \in V(L(n-m), w)$.

Now fix $k \in \mathbb{N}$ and consider the sequence $s_n := \{\phi_k(A_{\sigma_n})\}_{n\in\mathbb{N}}$. Since s_{n+m} depends only on m-tuple $s_n, \ldots, s_{n+m-1}$ and there are only finitely many of such m-tuples over $\mathrm{SL}_2^{\pm}(\mathbb{Z}/p^k\mathbb{Z})$ then the sequence s_n is eventually periodic. Moreover by the condition of the theorem s_n is also uniquely determined by $s_{n+1}, \ldots, s_{n+m}$ therefore s_n is purely periodic.

$L(n)$ tends to infinity as $n \to \infty$ therefore $s_1, \ldots, s_m$ are in $V_k(l, w)$ for an arbitrary large l. Then since the inclusion is true for all $k \in \mathbb{N}$ we have that $s_1, \ldots, s_m \in Wp(l, w)$ for all $l \in \mathbb{N}$ and finally $A_{\sigma_1}, \ldots, A_{\sigma_k} \in Wp(w)$. Choose two of these matrices which are different (by the condition of the theorem we can do so). Without loss of generality let them be A_{σ_1} and A_{σ_2}. Since σ_1 and σ_2 are one letter words we use Lemma 3 to show that $\psi(\sigma_{1,2}) \in \widetilde{\mathrm{SL}}_2(\mathbb{Q}_p)$ and that the eigenvectors $\mathbf{w}_{1,2,3,4}$ of $\psi(\sigma_1)$ and $\psi(\sigma_2)$ are all distinct. Therefore Corollary 2 can be applied to $\mathbf{x} = (w, \mathbf{x}_p)$ which finishes the proof of the theorem.

We finish this section by showing that even weaker condition than in Corollary 2 on $Vp(w)$ tells quite a lot about possible elements $(w, \mathbf{x}_p) \in \mathbf{LMad}$.

Theorem 8. *Assume that $A \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ is an element of $Vp(w)$ and $\mathbf{w}_1, \mathbf{w}_2$ are two eigenvectors of A. Then there are at most two different values $\mathbf{x}_p$ such that $\mathbf{x} = (w, \mathbf{x}_p) \in \mathbf{LMad}$: $\mathbf{x}_p = \mathbf{w}_1$ or $\mathbf{x}_p = \mathbf{w}_2$.*

Note that both $\mathbf{w}_1$ and $\mathbf{w}_2$ are quadratic algebraic numbers therefore if w satisfies the conditions of Theorem 8 and $(w, \mathbf{x}_p) \in \mathbf{LMad}$ then $\mathbf{x}_p$ must be quadratic irrational.

Proof. there are two possible values $\mathbf{x}_p$ for which δ defined in Theorem 1 is zero: $\mathbf{x}_p = \mathbf{w}_1$ and $\mathbf{x}_p = \mathbf{w}_2$ where $\mathbf{w}_1$ and $\mathbf{w}_2$ are eigenvectors of A. If $\mathbf{x}_p$ is not one of that two values then δ becomes strictly positive and we can repeat the proof of Theorem 7 with A in place of A_1 to show that $(w, \mathbf{x}_p) \notin \mathbf{LMad}$. □

In view of Corollary 2 and Theorem 8 it would be interesting to investigate sets $Vp(w)$ for various words $w \in \mathbb{A}_n^{\mathbb{N}}$. In particular it would be good to describe the collection of words for which $Vp(w)$ does not contain any matrices $A \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$.

9 Periodic words w

According to Theorem 8 if $Vp(w) \cap \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p) \neq \emptyset$ then there are at most two possible values $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$ for which $(w, \mathbf{x}_p) \in \mathbf{LMad}$. Moreover both of them are quadratic algebraic. We'll show that in fact for at least some w with this property the set

$$\mathbf{LMad} \cap \{(w, \mathbf{x}_p) \ : \ \mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}\}$$

is nonempty. Consider an arbitrary purely periodic word w. Let u be the finite factor of w which comprises the minimal period of w. Then one can check that $Vp(w) = \{A_u^k\}_{k \in \mathbb{N}}$. By periodicity $\mathrm{T}^l w = w$ where l is the length of u. Consider the equation

$$\mathrm{T}^l(w, \mathbf{x}_p) = (w, \mathbf{x}_p) \tag{13}$$

in $\mathbf{x}_p$. If we represent $\mathbf{x}_p$ in affine form $\mathbf{x}_p = \left(\begin{smallmatrix} x_p \\ 1 \end{smallmatrix}\right)$ then it becomes a quadratic equation $a + cx_p = (b + dx_p)x_p$ where $A_u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. It has two different roots $x_{1,2} \in \overline{\mathbb{Q}_p}$. For some of the matrices A_u both of these roots are in $\mathbb{Q}_p$. Below we will show that for any such a root x_p we have $(w, \mathbf{x}_p) \in \mathbf{LMad}$.

Lemma 6. *Let $v \in \mathbb{Q}_p \backslash \mathbb{Q}$ be the solution of quadratic equation with integer coefficients. Then $\left(\begin{smallmatrix} v \\ 1 \end{smallmatrix}\right) \in \mathbf{PBad}_\epsilon$ for some $\epsilon = \epsilon(v) > 0$.*

The proof of the lemma uses similar ideas as Liouville's proof that every real quadratic irrational is badly approximable.

Proof. Let $\bar{v}$ be a conjugate of v. Consider $a, b \in \mathbb{Z}$ such that $|av - b|_p < 1$, for other pairs a, b the conditions of $\mathbf{PBad}_\epsilon$ are held automatically. Since $|a(v - \bar{v})|_p \ll_v 1$ we have that $|a\bar{v} - b|_p \ll_v 1$.

Consider the value $(av - b)(a\bar{v} - b)$. It is integer, therefore

$$|(av - b)(a\bar{v} - b)|_p \geqslant (a^2 v\bar{v} - ab(v + \bar{v}) + b^2)^{-1} \gg_v (\max\{a^2, b^2\})^{-1}.$$

Hence we get

$$|av-b|_p \cdot \min\{1, |v^{-1}|_p\} = \frac{|(av-b)(a\bar{v}-b)|_p \cdot \min\{1,|v^{-1}|_p\}}{|a\bar{v}-b|_p} \gg_v (\max\{a^2,b^2\})^{-1}.$$

□

Lemma 7. *Let $\mathbf{x} \in \mathbf{PBad}$. Then for any matrix $A \in \mathrm{GL}_2(\mathbb{Z})$ the point $A\mathbf{x}$ is in $\mathbf{PBad}$.*

Proof. Choose $\mathbf{x} \in \tilde{\mathbf{P}}^1_{\mathbb{Q}_p}$, i.e. $\mathbf{x} = (x,y)$ with $\max\{|x|_p,|y|_p\} = 1$. Then since $\mathbf{x} \in \mathbf{PBad}$ we have $|ux+vy|_p \gg \min\{|u|^{-2},|v|^{-2}\}$.

Write A in coordinate form: $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Consider $|u(ax+by)+v(cx+dy)|_p$. Then

$$|u\cdot(ax+by)+v\cdot(cx+dy)|_p = |(ua+vc)x+(ub+vd)y|_p$$

$$\gg \min\{|ua+vc|^{-2},|ub+vd|^{-2}\} \gg \min\{|u|^{-2},|v|^{-2}\}.$$

□

Now we are ready to show that for any solution of (13) we have $(w,\mathbf{x}_p) \in \mathbf{LMad}$. From the theory of continued fractions we know that $x_p \notin \mathbb{Q}$ (the solution of the equation $a+cx_p = (b+dx_p)x_p$ over $\mathbb{R}$ gives a solution which continued fraction expansion is periodic with period u). Therefore by Lemma 6, $\mathbf{x}_p$ is in $\mathbf{PBad}_{\epsilon_0}$ for some positive ϵ_0. Then by the construction of w and $\mathbf{x}_p$ we have that $\mathrm{T}^l(w,\mathbf{x}_p) = (w,\mathbf{x}_p)$ therefore to ensure that $(w,\mathbf{x}_p) \in \mathbf{LMad}$ it is sufficient to check that $\mathbf{x}_{p,i} \in \mathbf{PBad}_{\epsilon_i}$ where $1 \leqslant i < l$, $\mathrm{T}^i(w,\mathbf{x}_p) = (\mathrm{T}^i w, \mathbf{x}_{p,i})$ and ϵ_i are some positive constants. However this is in fact true by Lemma 7 and the fact that by the construction of T, $\mathbf{x}_{p,i} = (A_{w_i})^T\mathbf{x}_p$. So, $(w,\mathbf{x}_p) \in \mathbf{LMad}_\epsilon$ where $\epsilon = \min_{0\leqslant i<l}\{\epsilon_i\}$. Now note that if $\mathrm{T}^l(w,\mathbf{x}_p) = (w,\mathbf{x}_p)$ then $\mathbf{x}_p$ coincides with one of the eigenvectors of $A^T_{w_l}$. This finishes "if" part of the proof of Theorem 3.

10 Collections U_k and low complexity words w

In this section we show how can Theorems 1 and 2 can be applied to words with low complexity. We start with the following auxiliary lemma.

Lemma 8. *Let u,v be two finite words over the alphabet $\mathbb{N}$. If $A_u, A_v \in \widetilde{\mathrm{SL}}_2(\mathbb{Z}_p)$ share the same eigenvector $\mathbf{v}$ then there exists a finite word w and positive integer values m_1,m_2 such that $u = w^{m_1}, v = w^{m_2}$. Moreover A_w shares the same eigenvector $\mathbf{v}$.*

Proof. We consider $\mathbf{v}$ in affine form, so we can look at it as a number from $\overline{\mathbb{Q}}_p$. Note that $\mathbf{v}$ is algebraic and, since there is a field isomorphism between algebraic numbers in $\overline{\mathbb{Q}}_p$ and in $\mathbb{C}$, two matrices A_u and A_v should also share the same eigenvector $\mathbf{v}^* \in \mathbf{P}^1_{\mathbb{C}}$.

From the theory of continued fractions we know that A_u always has two different real eigenvectors. Considered as real numbers they satisfy the conditions $\mathbf{v}^*_1 < 0 < \mathbf{v}^*_2$ and $w_{CF}(\mathbf{v}^*_2) = u^\infty (= uuuuuu....)$. Since A_u and A_v share the same eigenvector in $\mathbf{P}^1_{\mathbb{Q}_p}$ they must also share the same positive eigenvector in $\mathbf{P}^1_{\mathbb{C}}$ which in turn implies that two infinite words u^∞ and v^∞ coincide. The conclusion of the lemma can be easily derived from this fact. □

Now we are ready to prove

Proposition 3. *Let $w \in \mathbb{A}_N^{\mathbb{N}}$ be recurrent and $\mathbf{U}_k$ be constructed from w. If for every $k \in \mathbb{N}$, $\#\mathbf{U}_k$ is bounded above by some absolute constant then there are at most two points $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$ such that $\mathbf{x} = (w, \mathbf{x}_p) \in \mathbf{LMad}$. Moreover if w is not periodic then $(w, \mathbf{x}_p) \notin \mathbf{LMad}$ for all points $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$.*

Proof. Assume that the sequence $\#\mathbf{U}_k$ is bounded. Since $\#\mathbf{U}_k$ is non decreasing then there exists k_0 such that for $k \geqslant k_0$, $\#\mathbf{U}_k$ is a constant. Consider the minimal number $n \in \mathbb{N}$ such that $\phi_{k_0}(A_{w_n}) = \mathrm{Id}$, from the proof of Proposition 1 we know that such n always exists. Then by Proposition 1, $\forall k \in \mathbb{N}$, $U_k(w) = \phi_k(A_{w_n}) \cdot U_k(\mathrm{T}^n w)$ and in particular $U_{k_0}(w) = U_{k_0}(\mathrm{T}^n w)$. Remind that

$$\mathbf{U}_k := \{U_k(\mathrm{T}^n w) \ : \ n \in \mathbb{N}\}.$$

Since for every $k \geqslant k_0$ the number of elements in $\mathbf{U}_k$ stays the same we should have $U_k(w) = U_k(\mathrm{T}^n w)$ for every $k \in \mathbb{N}$. In particular it means that $\forall k \in \mathbb{N}$,

$$\phi_k(A_{w_n}) \cdot U_k(w) = U_k(w)$$

and the conditions of Corollary 1 are satisfied for $A = A_{w_n}$. As k tends to infinity one can choose an arbitrary large m satisfying (5). If $\mathbf{x}_p$ does not coincide with any of the eigenvectors of A^T then we have $\delta > 0$, so Corollary 1 can be applied to get $\mathbf{x} \notin \mathbf{LMad}$. This shows the first statement of the proposition.

For the second statement we consider an infinite sequence $n_1 < n_2 < \ldots < n_t < \ldots$ of positive integers such that $\phi_{k_0}(A_{w_{n_t}}) = \mathrm{Id}$. By slightly modifying the arguments of Proposition 1 one can show that such a sequence also exists. We showed that if $(w, \mathbf{x}_p) \in \mathbf{LMad}$ then $\mathbf{x}_p$ must coincide with one of the eigenvalues of all matrices $A_{w_{n_t}}$, in other words all of them must share the same eigenvalue. By Lemma 8 it means that there exists a finite word $\tilde{w}$ such that $w_{n_t} = \tilde{w}^{m_t}$ which straightforwardly implies that w is periodic. □

We will associate each word $w \in \mathbb{A}_N^{\mathbb{N}}$ with another word $u = u(k) \in \mathbf{U}_k^{\mathbb{N}}$ by the following rule: $u = b_1 b_2 \ldots$ where

$$b_n = U_k(\mathrm{T}^{n-1} w).$$

Lemma 9. *Let $\mathbf{x} = (w, \mathbf{x}_p) \in \mathbf{LMad}$. Then there exists $k_0 \in \mathbb{N}$ such that for every $k > k_0$ and every two-letter factor $c_1 c_2$ of $u(k)$ there is the unique value $a \in \mathbb{A}_N$ with the following property:*

- *if $b_n b_{n+1} = c_1 c_2$ then $a_n = a$ where a_n is the nth letter of w.*

In other words Lemma 9 states that for k large enough any two-letter factor of u uniquely determines a one-letter factor of w.

Proof. Assume the contrary: one can find an arbitrarily large $k \in \mathbb{N}$ such that there exist positive integer n and l such that $b_n b_{n+1} = b_l b_{l+1} = c_1 c_2$ but the corresponding letters $a_n = a$ and $a_l = a'$ are different. From Proposition 1 we have

$$c_1 = \phi_k(A_a) \cdot c_2; \quad \text{and} \quad c_1 = \phi_k(A_{a'}) \cdot c_2.$$

which immediately implies that

$$c_1 = \phi_k(A_{a'}^{-1} A_a) \cdot c_1 = \phi_k(D_{a-a'}) c_1.$$

In other words it means that $U_k(\mathrm{T}^n w)$ contains matrices

$$\phi_k(D_{a'-a}), \phi_k(D_{a'-a}^2), \ldots, \phi_k(D_{a'-a}^m), \ldots$$

Lemma 1 shows that this property implies that

$$\{\mathbf{x}_{p,n}, D_{a-a'}^T \mathbf{x}_{p,n}, \ldots, (D_{a-a'}^T)^m \mathbf{x}_{p,n}\} \subset B_k(\mathrm{T}^n \mathbf{x})$$

where m can be made arbitrarily large. In other words (6) is satisfied for $\mathrm{T}^n\mathbf{x}$. Take $m = p^{k+1}\delta$. Then all the conditions of Theorem 2 are satisfied for the point $\mathrm{T}^n\mathbf{x}$. If $\mathbf{x}_{p,n}$ is such that $\delta = 0$ then Theorem 2 states that $\mathrm{T}^n\mathbf{x} \notin \mathbf{LMad}$ which by the invariance of $\mathbf{LMad}$ implies that $\mathbf{x} \notin \mathbf{LMad}$. This contradicts the conditions of the lemma. Otherwise it implies that $\mathrm{T}^n\mathbf{x} \notin \mathbf{LMad}_\epsilon$ where ϵ can be made an arbitrarily small positive number as k grows to infinity. Again this leads to a contradiction. □

In particular Lemma 9 shows that if $\mathbf{x} \in \mathbf{LMad}$ and the word u is periodic then the word w must be periodic too. Theorem 3 gives a complete description of elements $(w, \mathbf{x}_p) \in \mathbf{LMad}$ in this case.

Now we will check that for l large enough l-letter factor of w uniquely determines $(l+1)$-letter factor of u.

Lemma 10. *Let w be uniformly recurrent word. There exists $l \in \mathbb{N}$ such that for every l-letter factor v of w there exists unique $l+1$-letter factor v' of u such that*

- *if $v = (\mathrm{T}^n w)_l$ then $v' = (\mathrm{T}^n u)_{l+1}$.*

Proof. From the proof of Proposition 2 we know that there exists $m \in \mathbb{N}$ such that for every infinite word w^* starting with w_m we have $U_k(w) \subset U_k(w^*)$. Since w is uniformly recurrent there exists an absolute constant m_1 such that the distance between two consecutive factors w_m in w is at most m_1. Then one can easily check that every factor of w of length $l = m+m_1$ contains w_m as a factor. We will show that this value l works for the lemma.

Consider an arbitrary factor v of w of length l. We showed that it can be written as $v = u_1 w_m u_2$. Denote the length of u_1 by n_1. Consider an arbitrary $n \in \mathbb{N}$ such that $(\mathrm{T}^n w)_l = v$. Then $(\mathrm{T}^{n+n_1} w)_m = w_m$ and $U_k(\mathrm{T}^{n+n_1} w) \supset U_k(w)$. However every set in the collection $\mathbf{U}_k$ has the same cardinality therefore $U_k(\mathrm{T}^{n+n_1} w) = U_k(w)$. Finally by Proposition 1, $U_k(\mathrm{T}^n w) = \phi_k(A_{v_1}) \cdot U_k(w)$. The right hand side of the last equality does not depend on the position n of the factor v so the lemma is proved. □

Proof of Theorem 5. Firstly without loss of generality we can assume that w is uniformly recurrent. Otherwise $\overline{\{\mathrm{T}^n\mathbf{x}\}}_{n\in\mathbb{N}}$ is not minimal set invariant under T. Then we can consider its minimal subset which will be of the form $\overline{\{\mathrm{T}^n(w', \mathbf{x}'_p)\}}_{n\in\mathbb{N}}$ where w' is uniformly recurrent. Since $P(w', n) \leqslant P(w, n)$ all the conditions of Theorem 5 will be satisfied for w' as well and the statement of the theorem for w will easily be followed from the same statement for w'.

Suppose that a value $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$ such that $(w, \mathbf{x}_p) \in \mathbf{LMad}$ exists. If for some $n \in \mathbb{N}$ we have that $P(w, n+1) = P(w, n)$ then w is periodic (see [5] for details). But this contradicts to the conditions of the theorem. So we should have $P(w, n+1) - P(w, n) \geqslant 1$ for every $n \in \mathbb{N}$. Also Proposition 3 shows that the sequence $\{\#\mathbf{U}_k\}_{k\in\mathbb{N}}$ is unbounded.

Since $P(w, n) \leqslant n + C$, there exists a value $n_0 \in \mathbb{N}$ such that for every $n \geqslant n_0$, $P(w, n+1) - P(w, n) = 1$. Choose k_0 such that $\#\mathbf{U}_{k_0} > P(w, n_0)$. This will ensure that for each $k > k_0$, $P(w, n_0) < P(u(k), n_0 + 1)$. If for some $n \in \mathbb{N}$, $P(u, n) = P(u, n+1)$ then u is periodic which by Lemma 9 implies that w is periodic too — a contradiction. Hence we have $P(w, n+1) - P(u, n) \geqslant 1$ and this immediately implies that $\forall n \geqslant n_0$, $P(w, n) < P(u, n+1)$. On the other hand Lemmata 9 and 10 together imply that there exists $l_0 \in \mathbb{N}$ such that $\forall l \geqslant l_0$, $P(u, l) = p(w, l-1)$. So we get a contradiction with assumption that the value $\mathbf{x}_p$ exists.

Remark. The complexity condition in Theorem 5 does not seem to be sharp. One can possibly use more delicate arguments to improve them.

11 Proof of Theorem 6

Since w is uniformly recurrent, Lemma 10 can be applied to find the value $l = l(k) \in \mathbb{N}$ such that every factor v of w of length l uniquely determines an element $u \in \mathbf{U}_k$. In other words as soon as $\mathrm{T}^n w$ starts with v the set $U_k(\mathrm{T}^n w)$ remains the same. Moreover the proof of Lemma 10 tells that $U_k(\mathrm{T}^n w) = U_k(v)$.

Now consider the graph G_l and take two vertices $t_1, t_2 \in T_l$ such that they are connected with the same vertex $s \in S_l$. then $U_k(s) = U_k(st_1) = U_k(st_2)$. We apply Proposition 1 to get

$$U_k(s) = \phi_k(A_s)U_k(t_1) = \phi_k(A_s)U_k(t_2) \quad \text{or} \quad U_k(t_1) = U_k(t_2).$$

By repeating this argument for every triple t_1, t_2, s in the graph G_l one can show that for any two words $t_1^*, t_2^* \in T_l$ from the same connected component of G_l we must have $U_k(t_1^*) = U_k(t_2^*)$. The number of different elements $U_k(s)$ where s runs through all vertices in S_l coincides with $\#\mathbf{U}_k$. Therefore if the number of connected components in G_l is bounded by absolute constant independent on l then $\#\mathbf{U}_k$ is bounded by the same constant. However Proposition 3 states that in this case $(w, \mathbf{x}_p) \notin \mathbf{LMad}$ for every $\mathbf{x}_p \in \mathbf{P}^1_{\mathbb{Q}_p}$.

It would be interesting to investigate the graphs G_l for various infinite words w. They are surely connected for infinite words w such that $\{\mathrm{T}^n w\}_{n\in\mathbb{N}}$ is dense everywhere on $\mathbb{A}_N^{\mathbb{N}}$. On the other hand numerical evidence suggests that the number of connected components of G_l for Thue-Morse word w_{tm} tends to infinity as $l \to \infty$. Even though the author does not know the proof of this fact it seems that Thue-Morse word is not covered by the last theorem.

References

[1] D. Badziahin, Y. Bugeaud, M. Einsiedler, D. Kleinbock, On the complexity of a putative counterexample to the p-adic Littlewood conjecture. Preprint, 2014.

[2] Y. Bugeaud, M. Drmota, and B. de Mathan, On a mixed Littlewood conjecture in Diophantine approximation. *Acta Arith.* V. 128 pp. 107–124, 2007.

[3] J. W. S. Cassels, An introduction to Diophantine Approximation. Cambridge University Press, Cambridge, 1955.

[4] M. Einsiedler and D. Kleinbock, Measure rigidity and p-adic Littlewood-type problems. *Compositio Math.* V. 143 pp. 689–702, 2007.

[5] M. Lothaire, Algebraic combinatorics on words. Cambridge University Press, Cambridge, 2002.

[6] B. de Mathan et O. Teulié, Problèmes diophantiens simultanés. *Monatsh. Math.* V. 143 pp. 229–245, 2004.

Dzmitry A. Badziahin: Department of Mathematics, Durham University,
Durham, DH1 3LE, England.
e-mail: dzmitry.badziahin@durham.ac.uk