On minimal decomposition of p-adic polynomial dynamical systems

Fan Ai-Hua, Lingmin Liao

ON MINIMAL DECOMPOSITION OF p-ADIC POLYNOMIAL DYNAMICAL SYSTEMS

AIHUA FAN AND LINGMIN LIAO

Abstract. A polynomial of degree ≥ 2 with coefficients in the ring of p-adic numbers $\mathbb{Z}_p$ is studied as a dynamical system on $\mathbb{Z}_p$. It is proved that the dynamical behavior of such a system is totally described by its minimal subsystems. For an arbitrary quadratic polynomial on $\mathbb{Z}_2$, we exhibit all its minimal subsystems.

1. Introduction

Let $\mathbb{Z}_p$ be the ring of p-adic integers (p being a prime number). Let $f \in \mathbb{Z}_p[x]$ be a polynomial of coefficients in $\mathbb{Z}_p$ and with degree $\deg f \geq 2$. It is simple fact that $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is a 1-Lipschitz map. In this paper we study the topological dynamical system $(\mathbb{Z}_p, f)$. We refer to [27] for dynamical terminology and [19, 22, 25, 26] for notions related to p-adic numbers.

Our first theorem is a general result which shows that a polynomial system admits at most countably many minimal subsystems. This describes to some extent the dynamical behavior of the system (see Theorem 4.2).

Theorem A. *Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. We have the following decomposition*

$$\mathbb{Z}_p = A \bigsqcup B \bigsqcup C$$

where A is the finite set consisting of all periodic points of f, $B = \bigsqcup_i B_i$ is the union of all (at most countably many) clopen invariant sets such that each B_i is a finite union of balls and each subsystem $f : B_i \to B_i$ is minimal, and each point in C lies in the attracting basin of a periodic orbit or of a minimal subsystem.

We will refer to the above decomposition as *the minimal decomposition* of the system $f : \mathbb{Z}_p \to \mathbb{Z}_p$. A finite periodic orbit of f is by definition a minimal set. But for the convenience of the present paper, only the sets B_i in the above decomposition are called *minimal components*.

There were few works done on the minimal decomposition. Multiplications on $\mathbb{Z}_p$ ($p \geq 3$) were studied by Coelho and Parry [9] and general affine maps were studied by Fan, Li, Yao and Zhou [12]. The minimal decomposition of a polynomial system has been known in these cases and only in these cases. Quadratic polynomials will be studied at the end of the present paper.

One of interesting problems well studied in the literature is the minimality of the system $f : \mathbb{Z}_p \to \mathbb{Z}_p$, which corresponds to the situation where $A = C = \emptyset$ and B consists of one minimal component ([2, 3, 4, 5, 8, 10, 14, 15, 16, 17, 18, 20]).

2000 *Mathematics Subject Classification.* Primary 37E99; Secondary 11S85, 37A99.

Key words and phrases. p-adic dynamical system, minimal component, quadratic polynomial.

The above theorem shows that there are only a finite number of periodic orbits. The possible periods are shown in the following theorem (see Theorem 4.1). The statements 1)-3) were known to Pezda [24], the statements 1) and 2) are also found by Desjardins and Zieve [10] in a different way. The statement 4) is new.

Theorem B. *Let $f \in \mathbb{Z}_p[x]$.*

1) *If $p \geq 5$, the periods of periodic orbits are of the form ab with $a|(p-1)$ and $1 \leq b \leq p$.*

2) *If $p = 3$, the periods of periodic orbits must be $1, 2, 3, 4, 6$ or 9.*

3) *If $p = 2$, the periods of periodic orbits must be $1, 2$ or 4.*

4) Let $p = 2$. If there is 4-periodic orbit, then $f(z \bmod 2) \bmod 2$ should be a permutation on $\mathbb{Z}/2\mathbb{Z}$. There is no 4-periodic orbit for quadratic polynomials.

What kind of set can be a minimal component of a polynomial system? In a recent work, Chabert, Fan and Fares [8] showed that each minimal component B_i must be a Legendre set and that in general, any Legendre set is a minimal component of some 1-Lipschtz system. We will show that for a polynomial system, the minimal components B_i are Legendre sets of special forms. Let $(p_s)_{s\geq 1}$ be a sequence of positive integers such that $p_s|p_{s+1}$ for every $s \geq 1$. We denote by $\mathbb{Z}_{(p_s)}$ the inverse limit of $\mathbb{Z}/p_s\mathbb{Z}$, which is called an odometer. The map $x \to x+1$ is called the adding machine on $\mathbb{Z}_{(p_s)}$. We will prove the following theorem (see Theorem 5.2).

Theorem C. *Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. If E is a minimal clopen invariant set of f, then $f : E \to E$ is conjugate to the adding machine on an odometer $\mathbb{Z}_{(p_s)}$, where*

$$(p_s) = (k, kd, kdp, kdp^2, \cdots)$$

with integers k and d such that $1 \leq k \leq p$ and $d|(p-1)$.

As we have already pointed out, the minimal decomposition is fully studied for affine maps. It seems much more difficult to study the minimal decomposition for higher order polynomials. In this paper, we try to attack the problem for quadratic polynomials. For an arbitrary 2-adic quadratic polynomial

$$f(x) = ax^2 + bx + c$$

on $\mathbb{Z}_2$, we find all its minimal components.

As we shall see, such a quadratic system $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ is conjugate to one of the following quadratic polynomials

$$x^2 - \lambda, \quad x^2 + bx, \quad x^2 + x - d$$

where $\lambda \in \mathbb{Z}_2$, $b \equiv 1 \pmod 2$ and $\sqrt{d} \notin \mathbb{Z}_2$. Our results are stated in Theorems 6.1-6.9. Let us state here some of these results.

Theorem D. *Consider the polynomial $x^2 - \lambda$ on $\mathbb{Z}_2$.*

1) *If $\lambda \equiv 0 \pmod 4$, then there are two attracting fixed points, one in $4\mathbb{Z}_2$ with basin $2\mathbb{Z}_2$, and the other one in $1 + 4\mathbb{Z}_2$ with basin $1 + 2\mathbb{Z}_2$.*

2) *If $\lambda \equiv 1 \pmod 4$, then the whole $\mathbb{Z}_2$ is attracted into a periodic orbit of period 2 with one orbit point in $4\mathbb{Z}_2$, and the other one in $3 + 4\mathbb{Z}_2$.*

3) *If $\lambda \equiv 2 \pmod 4$, then there are two attracting fixed points, one in $2 + 4\mathbb{Z}_2$ with basin $2\mathbb{Z}_2$, and the other one in $3 + 4\mathbb{Z}_2$ with basin $1 + 2\mathbb{Z}_2$.*

4) *If $\lambda \equiv 3 \pmod 4$, then the whole $\mathbb{Z}_2$ is attracted into a periodic orbit of period 2 with one orbit point in $1 + 4\mathbb{Z}_2$, and the other one in $2 + 4\mathbb{Z}_2$.*

Theorem E. *Consider the polynomial $f(x) = x^2 + x$ on $\mathbb{Z}_2[x]$. There is one fixed point 0. We have $f(1 + 2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$ and we can decompose $2\mathbb{Z}_2$ as*

$$2\mathbb{Z}_2 = \{0\} \bigsqcup \left(\bigsqcup_{n\geq 2} 2^{n-1} + 2^n\mathbb{Z}_2 \right).$$

Each $2^{n-1} + 2^n\mathbb{Z}_2$ $(n \geq 2)$ consists of 2^{n-2} pieces of minimal components:

$$2^{n-1} + t2^n + 2^{2n-2}\mathbb{Z}_2, \quad t = 0, \ldots, 2^{n-2} - 1.$$

Theorem F. *Consider the polynomial $f(x) = x^2 + x - d$ with $d \equiv 3 \pmod 4$. Then $f(2\mathbb{Z}_2) \subset 1 + 2\mathbb{Z}_2$ and $1 + 2\mathbb{Z}_2$ is the unique minimal component of f.*

The main idea used in the paper comes from Desjardins and Zieve's work [10] and the Ph.D thesis of Zieve [28]. Let E be an f-invariant compact set. It is now well known that the subsystem (E, f) is minimal if and only if the induced map $f_n : E/p^n\mathbb{Z} \to E/p^n\mathbb{Z}$ is minimal (transitive) for any $n \geq 1$ (see [5, 8]). The idea of Desjardins and Zieve is to establish relations between f_n's cycles and f_{n+1}'s cycles, by linearizing the k-th iteration f_{n+1}^k on a cycle of f_n of length k.

The paper is organized as follows. In Section 2, we give a full development of the idea in [10] by studying the induced dynamical systems f_n on $\mathbb{Z}/p^n\mathbb{Z}$ when $p \geq 3$. Section 3 is devoted to the case of $p = 2$ which was not treated in [10]. As we shall see, the situation in the case $p = 2$ is not exactly the same as in the case $p \geq 3$. In Sections 4 and 5, we investigate how a minimal component is formed by analyzing the reduced maps f_n $(n \geq 1)$ and we prove the decomposition theorem. In Section 5, we discuss the possible forms of minimal components. In Section 6, we give a detailed description of the minimal decomposition for an arbitrary quadratic polynomial system on $\mathbb{Z}_2$.

2. Induced dynamics on $\mathbb{Z}/p^n\mathbb{Z}$ $(p \geq 3)$

The main core of this section follows Desjardins and Zieve [10]. We shall give more details and rewrite some proofs for reader's convenience. The case $p = 2$, which is a little bit special, will be fully discussed in the next section.

Let $p \geq 3$ be a prime (we may replace 3 by 2 in many places). Let $n \geq 1$ be a positive integer. Denote by f_n the induced mapping of f on $\mathbb{Z}/p^n\mathbb{Z}$, i.e.,

$$f_n(x \bmod p^n) = f(x) \qquad \bmod p^n.$$

Many properties of the dynamics f are linked to those of f_n. One is the following.

Theorem 2.1 ([5], [8])**.** *Let $f \in \mathbb{Z}_p[x]$ and $E \subset \mathbb{Z}_p$ be a compact f-invariant set. Then $f : E \to E$ is minimal if and only if $f_n : E/p^n\mathbb{Z}_p \to E/p^n\mathbb{Z}_p$ is minimal for each $n \geq 1$.*

It is clear that if $f_n : E/p^n\mathbb{Z}_p \to E/p^n\mathbb{Z}_p$ is minimal, then $f_m : E/p^m\mathbb{Z}_p \to E/p^m\mathbb{Z}_p$ is also minimal for each $1 \leq m < n$. So, the above theorem shows that it is important to investigate under what condition, the minimality of f_n implies that of f_{n+1}.

Assume that $\sigma = (x_1, \cdots, x_k) \subset \mathbb{Z}/p^n\mathbb{Z}$ is a cycle of f_n of length k (also called k-cycle), i.e.,

$$f_n(x_1) = x_2, \cdots, f_n(x_i) = x_{i+1}, \cdots, f_n(x_k) = x_1.$$

In this case we also say σ is at level n. Let

$$X := \bigsqcup_{i=1}^{k} X_i \quad \text{where} \quad X_i := \{x_i + p^n t;\ t = 0, \cdots, p-1\} \subset \mathbb{Z}/p^{n+1}\mathbb{Z}.$$

Then

$$f_{n+1}(X_i) \subset X_{i+1}\ (1 \le i \le k-1) \quad \text{and} \quad f_{n+1}(X_k) \subset X_1.$$

In the following we shall study the behavior of the finite dynamics f_{n+1} on the f_{n+1}-invariant set X and determine all cycles in X of f_{n+1}, which will be called *lifts* of σ (from level n to level $n+1$). Remark that the length of any lift $\tilde{\sigma}$ of σ is a multiple of k.

Let $g := f^k$ be the k-th iterate of f. Then, any point in σ is fixed by g_n, the n-th induced map of g. For $x \in \sigma$, denote

$$a_n(x) := g'(x) = \prod_{j=0}^{k-1} f'(f^j(x)) \tag{2·1}$$

$$b_n(x) := \frac{g(x) - x}{p^n} = \frac{f^k(x) - x}{p^n}. \tag{2·2}$$

The values on the cycle $\sigma = (x_1, \ldots, x_k)$ of the functions a_n and b_n are important for our purpose. They define, for each x, an affine map

$$\Phi(x, t) = b_n(x) + a_n(x)t \qquad (x \in \sigma, t \in \mathbb{Z}/p\mathbb{Z}).$$

The 1-order Taylor expansion of g at x implies

$$g(x + p^n t) \equiv x + p^n b_n(x) + p^n a_n(x) t \equiv x + p^n \Phi(x, t) \pmod{p^{2n}}. \tag{2·3}$$

An important consequence of the last formula shows that $g_{n+1} : X_i \to X_i$ is conjugate to the linear map

$$\Phi(x_i, \cdot) : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

We could call it the *linearization* of $g_{n+1} : X_i \to X_i$.

For any $x \in X$ (and even for any $x \in \mathbb{Z}_p$), we can define the values of $a_n(x)$ and $b_n(x)$ by the formulas (2·1) and (2·2). As we shall see in the following lemma, the coefficient $a_n(x) \pmod p$ is always constant on X_i and the coefficient $b_n(x) \pmod p$ is also constant on X_i but under the condition $a_n(x) \equiv 1 \pmod p$.

Denote by $v_p(n)$ the p-valuation of n.

Lemma 2.2. *Let $n \ge 1$ and $\sigma = (x_1, \cdots, x_k)$ be a k-cycle of f_n.*

(i) *For $1 \le i, j \le k$, we have*

$$a_n(x_i) \equiv a_n(x_j) \pmod{p^n}.$$

(ii) *For for $1 \le i \le k$ and $0 \le t \le p-1$, we have*

$$a_n(x_i + p^n t) \equiv a_n(x_i) \pmod{p^n}.$$

(iii) *For $1 \le i \le k$ and $0 \le t \le p-1$, we have*

$$b_n(x_i + p^n t) \equiv b_n(x_i) \pmod{p^A},$$

where $A := \min\{v_p(a_n(x_i) - 1), n\} = \min\{v_p(a_n(x_j) - 1), n\}$ for $1 \le i, j \le k$.

(iv) *For all $1 \le i, j \le k$ we have*

$$\min\{v_p(b_n(x_i)), A\} = \min\{v_p(b_n(x_j)), A\}.$$

Consequently, if $a_n(x_i) \equiv 1 \pmod{p^n}$,

$$\min\{v_p(b_n(x_i)), n\} = \min\{v_p(b_n(x_j)), n\}.$$

Proof. Assertion (i) follows directly from the definition of $a_n(x_i)$ and the fact that $\sigma = (x_i, f_n(x_i), \cdots, f_n^{k-1}(x_i))$. The assertion (ii) is a direct consequence of

$$a_n(x_i + p^n t) \equiv \prod_{j=1}^{k} f'(f^j(x_i + p^n t)) \equiv \prod_{j=1}^{k} f'(f^j(x_i)) \pmod{p^n}.$$

The 1-order Taylor expansion of g at x_i gives

$$g(x_i + p^n t) - (x_i + p^n t) \equiv p^n \left(\frac{g(x_i) - x_i}{p^n}\right) + p^n t(g'(x_i) - 1) \pmod{p^{2n}}.$$

Hence

$$b_n(x_i + p^n t) \equiv b_n(x_i) + t(a_n(x_i) - 1) \pmod{p^n}.$$

Then (iii) follows.

Write

$$g(f(x_i)) - f(x_i) = f(f^k(x_i)) - f(x_i) = f(x_i + p^n b_n(x_i)) - f(x_i).$$

The 1-order Taylor expansion f at x_i leads to

$$g(f(x_i)) - f(x_i) \equiv p^n b_n(x_i) f'(x_i) \pmod{p^{2n}}.$$

Hence we have

$$b_n(f(x_i)) \equiv b_n(x_i) f'(x_i) \pmod{p^n}.$$

Since when $A = 0$, the result is obvious, we may suppose that $A \neq 0$. Then $a_n(x_i) \equiv 1 \pmod{p}$ (for $1 \leq i \leq k$) which implies $f'(x_i) \not\equiv 0 \pmod{p}$ for all $1 \leq i \leq k$. Notice that $f(x_i) \equiv x_{i+1} \pmod{p^n}$. Then by (iii), we obtain (iv). □

According to Lemma 2.2 (i) and (ii), the value of $a_n(x) \pmod{p^n}$ does not depend on $x \in X$. According to Lemma 2.2 (iii) and (iv), whether $b_n(x) \equiv 0 \pmod{p}$ does not depend on $x \in X$ if $a_n(x) \equiv 1 \pmod{p}$. For simplicity, sometimes we shall write a_n and b_n without mentioning x.

The above analysis allows us to distinguish the following four behaviors of f_{n+1} on X:

(a) If $a_n \equiv 1 \pmod{p}$ and $b_n \not\equiv 0 \pmod{p}$, then Φ preserves a single cycle of length p, so that f_{n+1} restricted to X preserves a single cycle of length pk. In this case we say σ *grows*.

(b) If $a_n \equiv 1 \pmod{p}$ and $b_n \equiv 0 \pmod{p}$, then Φ is the identity, so f_{n+1} restricted to X preserves p cycles of length k. In this case we say σ *splits*.

(c) If $a_n \equiv 0 \pmod{p}$, then Φ is constant, so f_{n+1} restricted to X preserves one cycle of length k and the remaining points of X are mapped into this cycle. In this case we say σ *grows tails*.

(d) If $a_n \not\equiv 0, 1 \pmod{p}$, then Φ is a permutation and the ℓ-th iterate of Φ reads

$$\Phi^\ell(x, t) = b_n(a_n^\ell - 1)/(a_n - 1) + a_n^\ell t$$

so that

$$\Phi^\ell(t) - t = (a_n^\ell - 1)\left(t + \frac{b_n}{a_n - 1}\right).$$

Thus, Φ admits a single fixed point $t = -b_n/(a_n - 1)$, and the remaining points lie on cycles of length d, where d is the order of a_n in $(\mathbb{Z}/p\mathbb{Z})^*$. So, f_{n+1} restricted to

X preserves one cycle of length k and $\frac{p-1}{d}$ cycles of length kd. In this case we say σ *partially splits*.

Now let us study the relation between (a_n, b_n) and (a_{n+1}, b_{n+1}). Our aim is to see the change of nature from a cycle to its lifts.

Lemma 2.3. *Let $\sigma = (x_1, \ldots, x_k)$ be a k-cycle of f_n and let $\tilde{\sigma}$ be a lift of σ of length kr, where $r \geq 1$ is an integer. We have*

$$a_{n+1}(x_i + p^n t) \equiv a_n^r(x_i) \pmod{p^n}, \qquad (1 \leq i \leq k, 0 \leq t \leq p-1) \tag{2·4}$$

$$\begin{aligned} &pb_{n+1}(x_i + p^n t) \\ \equiv &t(a_n(x_i)^r - 1) + b_n(x_i)\big(1 + a_n(x_i) + \cdots + a_n(x_i)^{r-1}\big) \pmod{p^n}. \end{aligned} \tag{2·5}$$

Proof. The formula (2·4) follows from

$$a_{n+1} \equiv (g^r)'(x_i + p^n t) \equiv (g^r)'(x_i) \equiv \prod_{j=0}^{r-1} g'(g^j(x_i)) \equiv a_n^r \pmod{p^n}.$$

By repeating r times of the linearization (2·3), we obtain

$$g^r(x_i + p^n t) \equiv x_i + \Phi^r(x_i, t)p^n \pmod{p^{2n}},$$

where Φ^r means the r-th composition of Φ as function of t, and

$$\Phi^r(x_i, t) = ta_n(x_i)^r + b_n(x_i)\big(1 + a_n(x_i) + \cdots + a_n(x_i)^{r-1}\big).$$

Thus (2·5) follows from the definition of b_{n+1} and the above two expressions. □

By Lemma 2.3, we obtain immediately the following proposition.

Proposition 2.4. *Let $n \geq 1$. Let σ be a k-cycle of f_n and $\tilde{\sigma}$ be a lift of σ. Then we have*

1) *if $a_n \equiv 1 \pmod{p}$, then $a_{n+1} \equiv 1 \pmod{p}$;*
2) *if $a_n \equiv 0 \pmod{p}$, then $a_{n+1} \equiv 0 \pmod{p}$;*
3) *if $a_n \not\equiv 0, 1 \pmod{p}$ and $\tilde{\sigma}$ is of length k, then $a_{n+1} \not\equiv 0, 1 \pmod{p}$;*
4) *if $a_n \not\equiv 0, 1 \pmod{p}$ and $\tilde{\sigma}$ is of length kd where $d \geq 2$ is the order of a_n in $(\mathbb{Z}/p\mathbb{Z})^*$, then $a_{n+1} \equiv 1 \pmod{p}$.*

This result is interpreted as follows in dynamical system language:
1) If σ grows or splits, then any lift $\tilde{\sigma}$ grows or splits.
2) If σ grows tails, then the single lift $\tilde{\sigma}$ also grows tails.
3) If σ partially splits, then the lift $\tilde{\sigma}$ of the same length as σ partially splits, and the other lifts of length kd grow or split.

If $\sigma = (x_1, \cdots, x_k)$ is a cycle of f_n which grows tails, then f admits a k-periodic point x_0 in the clopen set $\mathbb{X} = \bigsqcup_{i=1}^{k}(x_i + p^n\mathbb{Z}_p)$ and $\mathbb{X}$ is contained in the attracting basin of the periodic orbit $x_0, f(x_0), \cdots, f^{k-1}(x_0)$.

With the preceding preparations, we are ready to prove the following Propositions 2.5-2.7 which predict the behavior of the lifts of a cycle σ by the properties of σ. We refer the reader to [10] for their proofs. Otherwise we can follow the similar proofs of Propositions 3.1-3.3 in the case $p = 2$.

Proposition 2.5 ([10]). *Let σ be a growing cycle of f_n and $\tilde{\sigma}$ be the unique lift of σ.*

1) *If $p \geq 3$ and $n \geq 2$ then $\tilde{\sigma}$ grows.*
2) *If $p > 3$ and $n \geq 1$ then $\tilde{\sigma}$ grows.*
3) *If $p = 3$ and $n = 1$, then $\tilde{\sigma}$ grows if and only if $b_1(x) \not\equiv g''(x)/2 \pmod{p}$.*

According to 1) and 2) of Proposition 2.5, in the cases $p \geq 3, n \geq 2$ and $p > 3, n \geq 1$, if $\sigma = (x_1, \cdots, x_k)$ grows then its lift also grows, and the lift of the lift will grow and so on. So, the clopen set

$$\mathbb{X} = \bigsqcup_{i=1}^{k} (x_i + p^n \mathbb{Z}_p)$$

is a minimal set by Theorem 2.1.

Let

$$A_n(x) := v_p(a_n(x) - 1), \quad B_n(x) := v_p(b_n(x)).$$

By Lemma 2.2, for a cycle $\sigma = (x_1, \ldots, x_k)$, $\min\{A_n(x_i), n\}$ does not depend on the choice of $x_i, 1 \leq i \leq k$ and if $B_n(x_i) < \min\{A_n(x_i), n\}$ then $B_n(x_i)$ does not depend on the choice of $x_i, 1 \leq i \leq k$. Sometimes, there is no difference when we choose x_i or x_j in the cycle. So, without misunderstanding, we will not mention x_i in A_n and B_n (see the proof of Proposition 3.2 for the details corresponding to the case $p = 2$).

We say that a cycle σ at level n *splits ℓ times* if σ splits, and the lifts of σ at level $n + 1$ split and inductively all lifts at level $n + j$ $(2 \leq j < \ell)$ split. Similarly, one can imagine what we mean if we say a cycle *grows ℓ times*. That a cycle *grows forever* means that it grows infinite times.

Proposition 2.6 ([10]). *Let $p \geq 3$ and $n \geq 1$. Let σ be a splitting cycle of f_n.*

1) *If $\min\{A_n, n\} > B_n$, every lift splits $B_n - 1$ times then all lifts at level $n + B_n$ grow forever.*

2) *If $A_n \leq B_n$ and $A_n < n$, there is one lift which behaves the same as σ (i.e., this lift splits and $A_{n+1} \leq B_{n+1}$ and $A_{n+1} < n + 1$) and other lifts split $A_n - 1$ times then all lifts at level $n + A_n$ grow forever..*

3) *If $B_n \geq n$ and $A_n \geq n$, then all lifts split at least $n - 1$ times.*

Proposition 2.7 ([10]). *Let $p \geq 3$ and $n \geq 1$. Let σ be a partially splitting k-cycle of f_n and $\tilde{\sigma}$ be a lift of σ of length kd, where d is the order of a_n in $\mathbb{Z}/p\mathbb{Z}$.*

1) *If $A_{n+1} < nd$, then $\tilde{\sigma}$ splits $A_{n+1} - 1$ times then all lifts at level $n + A_{n+1}$ grow forever.*

2) *If $A_{n+1} \geq nd$, then $\tilde{\sigma}$ splits at least $nd - 1$ times.*

We remark that in the partially splitting case, $\min\{A_{n+1}(x), nd\}$ depends only on the lifting cycle of f_{n+1} of length kd but not on x (see [10], Corollary 3).

3. Induced dynamics on $\mathbb{Z}/p^n\mathbb{Z}_p$ $(p = 2)$

In this section we focus on the special case $p = 2$ which is not considered in [10]. The first part in the preceding section (where $p \geq 3$ is not explicitly assumed) remains true for $p = 2$. Notice that when $p = 2$, there is no partially splitting cycle.

We only need to study how a cycle grow or split. We distinguish four cases. Let σ be a cycle of f_n. We say σ *strongly grows* if $a_n \equiv 1 \pmod 4$ and $b_n \equiv 1 \pmod 2$, and σ *weakly grows* if $a_n \equiv 3 \pmod 4$ and $b_n \equiv 1 \pmod 2$. We say σ *strongly splits*

if $a_n \equiv 1 \pmod 4$ and $b_n \equiv 0 \pmod 2$, and σ *weakly splits* if $a_n \equiv 3 \pmod 4$ and $b_n \equiv 0 \pmod 2$.

The following results hold true when $p = 2$. Their proofs are postponed and got together at the end of this section.

Proposition 3.1. *Let σ be a cycle of f_n $(n \geq 2)$. If σ strongly grows then the lift of σ strongly grows. If σ weakly grows then the lift of σ strongly splits.*

The first assertion of Proposition 3.1 implies that if $\sigma = (x_1, \cdots, x_k)$ is a strongly growing cycle of f_n $(n \geq 2)$, then $\bigsqcup(x_i + p^n\mathbb{Z}_p)$ is a minimal set.

Recall that

$$A_n(x) = v_2(a_n(x) - 1), \quad B_n(x) = v_2(b_n(x)).$$

In the following proposition, the x in $A_n(x), B_n(x)$ can be chosen any x_i of the cycle $\sigma = (x_1, \cdots, x_k)$ (see its proof).

Proposition 3.2. *Let σ be a strongly splitting cycle of f_n $(n \geq 2)$.*

1) *If $\min\{A_n, n\} > B_n$, then all lifts strongly split $B_n - 1$ times, then all the lifts at level $n + B_n$ strongly grow.*

2) *If $A_n \leq B_n$ and $A_n < n$, then one lift behaves the same as σ (i.e., this lift strongly splits and $A_{n+1} \leq B_{n+1}$ and $A_{n+1} < n + 1$). The other one splits $A_n - 1$ times, then all the lifts lifts at level $n + A_n$ strongly grow forever.*

3) *If $B_n \geq n$ and $A_n \geq n$, then all lifts strongly split at least $n - 1$ times.*

Proposition 3.3. *Let σ be a weakly splitting cycle of f_n $(n \geq 2)$. Then one lift behaves the same as σ and the other one weakly grows and then strongly splits.*

To prove these propositions, we need the following lemmas.

Lemma 3.4. *Let σ be a growing cycle of f_n $(n \geq 2)$. Then*

$$a_{n+1}(x_i) \equiv 1 \pmod 4, \tag{3·1}$$

$$2b_{n+1}(x_i + p^n t) \equiv b_n(x_i)(1 + a_n(x_i)) \pmod 4. \tag{3·2}$$

Proof. Taking $p = 2$ and $r = 2$ in (2·4), we get

$$a_{n+1}(x_i) \equiv a_n^2(x_i) \pmod{2^n}.$$

Since $n \geq 2$ and $a_n \equiv 1 \pmod 2$, we obtain (3·1).

Taking $p = 2$ and $r = 2$ in (2·5), we get

$$2b_{n+1}(x_i + 2^n t) \equiv t(a_n(x_i)^2 - 1) + b_n(x_i)(1 + a_n(x_i)) \pmod{2^n}.$$

Since $n \geq 2$ and $a_n(x_i) \equiv 1 \pmod 2$, we obtain (3·2). □

Lemma 3.5. *Let σ be a splitting cycle of f_n. If $A_n < n$, then $A_{n+1} = A_n$ and if $A_n \geq n$, then $A_{n+1} \geq n$. Consequently,*

$$\min\{A_{n+1}, n\} = \min\{A_n, n\}. \tag{3·3}$$

Proof. We need only to notice that we have $a_{n+1} \equiv a_n \pmod{2^n}$ when σ splits. □

Lemma 3.6. *Let $\sigma = (x_1, \ldots, x_k)$ be a splitting cycle of f_n. Then for $1 \leq i \leq k$ and for $t = 0$ or 1, we have*

$$2b_{n+1}(x_i + 2^n t) \equiv b_n(x_i) + t(a_n(x_i) - 1) \pmod{2^n}. \tag{3·4}$$

Consequently, we have

$$B_{n+1}(x_i + 2^n t) = B_n(x_i) - 1 \qquad \text{if } B_n(x_i) < \min\{A_n(x_i),\ n\}, \tag{3·5}$$

Proof. Since σ splits, taking $p = 2$ and $r = 1$ in (2·5), we obtain the result. □

The following lemma concerns an elementary property of polynomials on $\mathbb{Z}_2$.

Lemma 3.7. *Let $h \in \mathbb{Z}_2[x]$. If $a \equiv b \pmod 2$, then $h'(a) \equiv h'(b) \pmod 4$. Furthermore, if $h'(a) \equiv 1 \pmod 2$, then $h'(a)h'(b) \equiv 1 \pmod 4$.*

Proof. It suffices to notice that the coefficient of x^{2k+1} in $h'(x)$ is equal to $0 \pmod 2$. □

Lemma 3.8. *Let σ be a growing k-cycle of f_n ($n \geq 1$). Then its lift strongly grows or strongly splits.*

Proof. Let x_1 be a point in σ. What we have to show is $a_{n+1}(x_1) \equiv 1 \pmod 4$. Since σ is a growing k-cycle, we have

$$f^k(x_1) \equiv x_1 \pmod{2^n}, \qquad a_n(x_1) = (f^k)'(x_1) \equiv 1 \pmod 2.$$

So, by Lemma 3.7, we have

$$a_{n+1}(x_1) = (f^{2k})'(x_1) = (f^k)'(x_1)(f^k)'(f^k(x_1)) \equiv 1 \pmod 4.$$

□

A direct consequence is the following result.

Corollary 3.9. *If a cycle grows twice (maybe between the two growths, there are several splittings), then all the lifts will grow forever.*

Proof. Let $\tilde{\sigma}$ be the lift of the growing cycle σ. Assume that after several times of splitting, one of lifts of $\tilde{\sigma}$ grows (then all the lifts at the same level grow). By Lemma 3.8, this growing lift at a level $n \geq 2$ must strongly grow. Thus by Proposition 3.1, the lifts will grow forever. □

We are now going to prove Propositions 3.1-3.3.

Proof of Proposition 3.1. If σ grows, then by (3·1), the lift of σ strongly grows or strongly splits. If σ strongly grows, then by (3·2), we have

$$2b_{n+1}(x_i + p^n t) \equiv 2b_n(x_i) \pmod 4.$$

Thus

$$b_{n+1}(x_i + p^n t) \equiv b_n(x_i) \not\equiv 0 \pmod 2.$$

Hence the lift of σ strongly grows.

If σ weakly grows, then by (3·2), we have

$$2b_{n+1}(x_i + p^n t) \equiv 0 \pmod 4.$$

Thus

$$b_{n+1}(x_i + p^n t) \equiv 0 \pmod 2.$$

Hence the lift of σ strongly splits. □

Proof of Proposition 3.2. First notice that if σ strongly splits then $a_n \equiv 1 \pmod 4$. Since $n \geq 2$, by Lemma 2.2 we have $a_\ell \equiv 1 \pmod 4$ for all $\ell > n$. So, all the lifts strongly grow or strongly split.

Proposition 3.2 contains three cases which are defined by some conditions on A_n and B_n. If such a condition is satisfied, we say σ or (A_n, B_n) belongs to the corresponding case.

Case 1: $\min\{A_n, n\} > B_n$. Recall that by Lemma 2.2, both $\min\{A_n(x_i), n\}$ and $\min\{A_n(x_i), B_n(x_i), n\}$ are independent of x_i. Thus in this case, we can simply write A_n and B_n. By (3·5), we have $B_{n+1} = B_n - 1$. Thus by (3·3)

$$\min\{A_{n+1}, n+1\} \geq \min\{A_{n+1}, n\} = \min\{A_n, n\} > B_n > B_{n+1}.$$

Hence the lifts of σ still belong to Case 1. By induction, we know that after $\ell := B_n$ times, $B_{n+\ell} = 0$ (i.e. $b_{n+\ell} \neq 0 \bmod p$). Since σ strongly splits, we have $a_{n+\ell} \equiv 1 \pmod 4$. Thus the lifts at level $n+\ell$ strongly grow. That is to say all lifts of σ split $B_n - 1$ times, then all the lifts lifts at level $n + B_n$ strongly grow forever.

Case 2: $A_n \leq B_n$ *and* $A_n < n$. Since $A_n(x_i) < n$ for some i, implies for all $1 \leq i \leq k$, $A_n(x_i) = A_n(x_j)$. We can also deduce that if $A_n(x_i) \leq B_n(x_i)$ for some i then for all i $A_n(x_i) \leq B_n(x_i)$. Otherwise, if $A_n(x_j) > B_n(x_j)$ for some j, then by Lemma 2.2, $B_n(x_i) = B_n(x_j) < A_n(x_j) = A_n(x_i)$ which leads to a contradiction. So in this case, we can choose any $1 \leq i \leq k$ and we simply write A_n and B_n. By Lemma 3.5, we have $A_{n+1} = A_n$. Since $B_n \geq A_n$, there exists one t such that

$$b_n + t(a_n - 1) \equiv 0 \pmod{2^{A_n+1}},$$

and the other one which we can write as $1 - t$ such that

$$b_n + t(a_n - 1) \not\equiv 0 \pmod{2^{A_n+1}}.$$

Hence by (3·4), for one lift of σ $B_{n+1} \geq A_n$ and for the other one $B_{n+1} = A_n - 1$. Thus for one lift, $A_{n+1} = A_n \leq B_{n+1}$, and $A_{n+1} = A_n < n+1$. Therefore, this lift belongs to Case 2. For the other one, $B_{n+1} = A_n - 1 = A_{n+1} - 1 < A_{n+1}$, and $B_{n+1} = A_n - 1 < n + 1$. Thus this lift belongs to Case 1. By induction, we know that one lift of σ behaves the same as σ (i.e., strongly splits and satisfies the condition of Case 2 at level $n+1$) and the other one splits $A_n - 1$ times, then the lifts strongly grow.

Case 3: $B_n \geq n$ *and* $A_n \geq n$. First we notice that by Lemma 2.2, if for some $1 \leq i \leq k$, we have $B_n(x_i) \geq n$ and $A_n(x_i) \geq n$, then for all $1 \leq i \leq k$, the same property established. The following statement will be the same if we choose another i. So we still simply write A_n and B_n. By the definition of b_n, if the cycle splits, the order of b_n deceases at most one when the level goes up one step. Since $B_n \geq n$, we have $B_{n+1} \geq n - 1$, and if $n \geq 2$, the lifts of σ still strongly split. Thus by induction, the lifts of σ split at least $n - 2$ times. But after that we can not give any more information. □

Proof of Proposition 3.3. Since σ weakly splits, $a_{n+1} \equiv a_n \equiv 3 \pmod 4$. Thus $A_{n+1} = A_n = 1 < n$ and $B_n \geq 1 = A_n$. Thus (A_n, B_n) belongs to Case 2 in Proposition 3.2. By the proof of Proposition 3.2, we know that for one lift of σ, $B_{n+1} \geq A_n$ and then $A_{n+1} = A_n \leq B_{n+1}$. Thus this lift behaves the same as σ. For the other lift, $B_{n+1} = A_n - 1 = 0$. Hence this second lift weakly grows, and then its lift strongly splits by Proposition 3.1. Therefore, we complete the proof. □

4. Minimal decomposition

If a cycle always grows (grows forever) then it will produce a minimal component of f. If a cycle always splits (splits infinite times) then it will produce a periodic orbit of f. If a cycle grows tails, it will produce an attracting periodic orbit with an attracting basin. We shall describe this more precisely.

Let $\sigma = (x_1, \ldots, x_k)$ be a cycle of f_n. Recall that in this case σ is called a k-cycle at level n. Let

$$\mathbb{X} := \bigsqcup_{i=1}^{k} (x_i + p^n \mathbb{Z}_p).$$

There are four special situations for the dynamical system $f : \mathbb{X} \to \mathbb{X}$.

(S1) Suppose σ grows tails. Then f admits a k-periodic orbit with one periodic point in each ball $x_i + p^n\mathbb{Z}_p$ $(1 \leq i \leq k)$, and all other points in $\mathbb{X}$ are attracted into this orbit. In this situation, if x is a point in the k-periodic orbit, then $|(f^k)'(x)|_p < 1$ since $(f^k)'(x) = a_m(x) \equiv 0 \pmod{p^m}$ for all $m \geq n$. The periodic orbit $(x, f(x), \cdots, f^{k-1}(x))$ is then attractive.

(S2) Suppose σ grows and its lifts always grow. Then f is transitive (minimal) on each $\mathbb{X}/p^m\mathbb{Z}_p$ $m \geq n$. Thus, by Theorem 2.1, f is minimal on $\mathbb{X}$. In this case, we say that σ is a starting growing cycle at level n.

(S3) Suppose σ splits and there is a splitting lift at each level larger than n. Then there is a k-periodic orbit with one periodic point in each $x_i + p^n\mathbb{Z}_p$ $(1 \leq i \leq k)$. We say that σ is a starting splitting cycle at level n. In this situation, if x is a point in the k-periodic orbit, then $(f^k)'(x) = 1$ since $(f^k)'(x) = a_m(x) \equiv 1 \pmod{p^m}$ for all $m \geq n$. Thus the periodic orbit $(x, f(x), \cdots, f^{k-1}(x))$ is indifferent.

(S4) Suppose $\sigma = (x_1, \ldots, x_k)$ partially splits $(p \geq 3)$. Then by Proposition 2.7, there is one lift of length k which still partially splits like σ. Thus there is a k-periodic orbit with one periodic point in each $x_i + p^n\mathbb{Z}_p$ $(1 \leq i \leq k)$. In this situation, if x is a point in the k-periodic orbit formed above, then $|(f^k)'(x)|_p = 1$ since $(f^k)'(x) = a_m(x) \not\equiv 0, 1 \pmod{p^m}$ for all $m \geq n$. Hence, the periodic orbit $(x, f(x), \cdots, f^{k-1}(x))$ is indifferent.

Now we can deduce all possible periods of the polynomial systems on $\mathbb{Z}_p$.

Theorem 4.1. *Let $f \in \mathbb{Z}_p$ with $\deg f \geq 2$.*

1) *If $p \geq 5$, the lengths of periodic orbits are of the form ab with $a|(p-1)$ and $1 \leq b \leq p$;*

2) *If $p = 3$, the lengths of periodic orbits must be $1, 2, 3, 4, 6$ or 9;*

3) *If $p = 2$, the lengths of periodic orbits must be $1, 2$ or 4.*

4) *Let $p = 2$. If there is 4-periodic orbit, then f_1 should be a permutation on $\mathbb{Z}/2\mathbb{Z}$. There is no 4-periodic orbit for quadratic polynomials.*

Remark 1. The statements 1)-3) were due to Pezda ([24]). By using the idea we explained in the preceding sections which is quite different from that of Pezda, Desjardins and Zieve ([10]) also gave 1) and 2). The statement 4) is new.

Proof. We only show 3) and 4), because the proofs of 1) and 2) are similar and can be found in [10] and [24].

Notice that any periodic orbit comes from an infinite sequence of splitting of some cycle, and that the length of the periodic orbit is the length of the starting splitting cycle. So, what we want to study are all possible lengths of starting splitting cycles.

The possible lengths of cycles at the first level (i.e. the cycles of f_1 on $\mathbb{Z}/2\mathbb{Z}$) are 1 and 2. Notice that the growth of length must be multiplied 2, according to

our discussion in the preceding sections. So, the possible lengths of cycles are 2^k ($k \geq 0$). However, by Corollary 3.9, if a cycle grows twice it will grow forever. There, any cycle of length 2^k ($k \geq 3$), which must have grown twice, can not be a starting splitting cycle. Hence the lengths of starting splitting cycles can only be $1, 2, 4$. This completes the proof of 3).

If there is a periodic orbit of length 4, there must be a starting splitting cycle of length 4. This is possible only in the following case: at the first level, f_1 admit a 2-cycle. Otherwise it needs to grow twice and then its lifts will grow forever. This will produce a clopen minimal set not a periodic orbit. This is the first part of 4). For the second part of 4), one can see from our study on the quadratic polynomials in Section 6 (Theorems 6.1-6.9). □

Theorem 4.2. *Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. We have the following decomposition*

$$\mathbb{Z}_p = A \bigsqcup B \bigsqcup C$$

where A is the finite set consisting of all periodic points of f, $B = \bigsqcup_i B_i$ is the union of all (at most countably many) clopen invariant sets such that each B_i is a finite union of balls and each subsystem $f : B_i \to B_i$ is minimal, and each point in C lies in the attracting basin of a periodic orbit or of a minimal subsystem.

Proof. We first explain that there are only finitely many periodic points. In fact, by Theorem 4.1, there are only finitely many possible lengths of periods. Periodic points are solutions of the equations $f^{q_i}(x) = x$ with $\{q_i\}$ being one of possible lengths of periods. Since $\deg f \geq 2$, each equation admits a finite number of solutions. So, there is only a finite number of periodic points.

We start from the second level. Decompose $\mathbb{Z}_p$ into p^2 balls with radius p^{-2}. Each ball is identified with a point in $\mathbb{Z}/p^2\mathbb{Z}$. The induced map f_2 admits some cycles. The points outside any cycle are mapped into the cycles. The ball corresponding to such a point will be put into the third part C. From now on, we really start our analysis with cycles at level $n \geq 2$. Let $\sigma = (x_1, \ldots, x_k)$ be a cycle at level $n \geq 2$. Let

$$\mathbb{X} = \bigsqcup_{i=1}^{k} (x_i + p^n \mathbb{Z}_p).$$

Suppose $p \geq 3$. We distinguish four cases.

(P1) *σ grows tails.* Then by (S1), the clopen set $\mathbb{X}$ consists of a k-periodic orbit and other points are attracted by this periodic orbit. So, $\mathbb{X}$ contributes to the first part A and the third part C.

(P2) *σ grows.* Then by Proposition 2.5, σ is in the situation (S2). Therefore $\mathbb{X}$ is a minimal component. So, $\mathbb{X} \subset B$.

(P3) *σ splits.* Then we shall apply Proposition 2.6.

- If σ belongs to Case 1 described by Proposition 2.6, then after finitely many times of splitting, the lifts will grow forever and so they are in the situation of (S2). Therefore we get a finite number of minimal components, all belonging to B.
- If σ belongs to Case 2, then there is one lift of σ sharing the property (S3), and other lifts different from the cycle containing the periodic orbit (at any level $m \geq n + 1$) find themselves in the situation (S2) after finitely many

times of lifting. Therefore, we get a periodic orbit and countable infinite minimal components.

- If σ belongs to Case 3, then σ splits into p^n cycles at level $2n$. These cycles at level $2n$ may continue this procedure of analysis of (P3). But this procedure can not continue infinitely, because there is only a finite number of periodic points. So, all these cycle may continue to split but they must end with their lifts belonging either to Case 1 or Case 2 in Proposition 2.6. So, $\mathbb{X}$ contributes to both A and B.

(P4) *σ partially splits.* Then σ is in the situation (S4). Thus there comes out a periodic orbit. Suppose σ_m is the lift of σ containing the periodic orbit at level $m \geq n+1$. If σ_m belongs to Case 1 in Proposition 2.7, then the other lifts different from σ_{m+1}, will be in the situation (S1) after finite times. If σ_m belongs to Case 2 in Proposition 2.7, then each of other lifts different from σ_{m+1}, split to be p^{nd-1} cycles at level nd. We then go to (P3) for these cycles at level nd.

SUPPOSE $p = 2$. We distinguish five cases.

(Q1) *σ grows tails.* Then σ is in the situation (S1). We have the same conclusion as (P1) above.

(Q2) *σ strongly grows.* Then by Proposition 3.1, σ is in the situation (S2). We have the same conclusion as (P2) above.

(Q3) *σ strongly splits.* By Proposition 3.2, the arguments are the same as (P3): The procedures will be ended if the condition 1) or 2) in Proposition 3.2 is satisfied. If the condition 3) in Proposition 3.2 is satisfied, we repeat the analysis of (Q3) for the lifts of σ. But the procedures will be eventually ended with the condition 1) or 2), because there is only a finite number of periodic points.

(Q4) *σ weakly grows.* Then by Proposition 3.1, the lift of σ strongly splits. We are then in the case (Q3).

(Q5) *σ weakly splits.* By Proposition 3.3, then one lift is in the situation (S3) which produces a periodic orbit, and the other lifts different from the cycle containing the periodic orbit, at any level $m \geq n+1$, will weakly grow. Then we are in the case (Q4).

All the above procedures will stop. So, we get the decomposition in finite steps. □

We have excluded the affine polynomials from the theorem. Exactly speaking, the conclusion is false for affine polynomials. For example, every points in $\mathbb{Z}_p$ are fixed by $f(x) := x$. Anyway, affine polynomials have been fully studied in [12].

Corollary 4.3. *Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. If f admits an indifferent fixed point or a periodic orbit, then there exists a sequence of minimal components with their diameters and their distances from the fixed point or the periodic orbit tending to zero.*

Proof. Suppose $(x_1, \ldots, x_k)$ is an indifferent periodic orbit. Let $x_j^{(n)} \in \mathbb{Z}/p^n\mathbb{Z}$ and $x_j^{(n)} \equiv x_j \pmod{p^n}$ for $1 \leq j \leq k$. Then $\sigma_n = (x_1^{(n)}, \ldots, x_k^{(n)})$ is a splitting or partially splitting cycle at level n. By the procedures of the decomposition, the cycle σ_n should be in the situation (S3) or (S4). That is to say σ_n splits for all n or σ_n partially splits for all n.

Since there are only finite number of periodic orbits, for any $\epsilon > 0$ small enough, there is no other periodic orbits in the ϵ neighborhood of the orbit $(x_1, \ldots, x_k)$.

Take n such that $p^{-n} < \epsilon$. Then the lifts of σ_n which are different to σ_{n+1} will never split infinitely. Hence they will grow after finite times. Then all the lifts of σ_n which are different to σ_{n+1}, considered as union of balls, consist of finite number of minimal components. Since these balls are contained in $x_j + p^n\mathbb{Z}_p$ for each j respectively. Thus there is a minimal component such that the diameter and the distance to the orbit $(x_1, \ldots, x_k)$ are all less than p^{-n}. The result is obtained if we consider infinitely n and find one minimal component for each n. □

5. Conjugacy classes of Minimal subsystems

Recently, Chabert, Fan and Fares [8] proved that minimal sets of a 1-Lipschitz map are Legendre sets. We shall prove that minimal sets of a polynomial are some special Legendre sets. A set $E \subset \mathbb{Z}_p$ is a *Legendre set* if for any $s \geq 1$ and any $x \in E/p^s\mathbb{Z}_p$, the number

$$q_s := \text{Card } \left\{y \in E/p^{s+1}\mathbb{Z}_p : \ y \equiv x \mod p^s\right\}$$

is independent of $x \in E/p^s\mathbb{Z}_p$. Let

$$p_s := q_1 q_2 \cdots q_s \qquad (\forall s \geq 1).$$

It is clear that $p_s = \text{Card } E/p^s\mathbb{Z}_p$. We call $(p_s)_{s\geq 1}$ the *structure sequence* of E. Consider the inverse limit

$$\mathbb{Z}_{(p_s)} := \lim_{\leftarrow} \mathbb{Z}/p_s\mathbb{Z}.$$

This is a profinite group, usually called an *odometer*, and the map $\tau : x \mapsto x + 1$ is called the *adding machine* on $\mathbb{Z}_{(p_s)}$.

Theorem 5.1 ([8]). *Let E be a clopen set in $\mathbb{Z}_p$ and $f : E \to E$ be a 1-Lipschitz map. If the dynamical system (E, f) is minimal, then f is an isometry, E is a Legendre set and the system (E, f) is conjugate to the adding machine $(\mathbb{Z}_{(p_s)}, \tau)$ where (p_s) is the structure sequence of E. On the other hand, on any Legendre set there exists at least one minimal map.*

We improve the above result in the case of polynomials by giving more information on the structure sequence.

Theorem 5.2. *Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. If E is a minimal clopen invariant set of f, then $f : E \to E$ is conjugate to the adding machine on an odometer $\mathbb{Z}_{(p_s)}$, where*

$$(p_s) = (k, kd, kdp, kdp^2, \cdots)$$

with some $1 \leq k \in \mathbb{N}, k \leq p$ and $d|(p-1)$.

Proof. By our previous discussion on the cycles of f_n on $\mathbb{Z}/p^n\mathbb{Z}$, a clopen minimal set E is formed when a cycle grows forever. If n is the starting level for the cycle to grow, then E is a union of some balls with radius p^{-n}. Therefore, for $s \geq n$, every nonempty intersection of E with a ball of radius p^{-s} contains p balls of radius $p^{-(s+1)}$. That is to say $q_s = p$. From the cycle at the first level to the starting growing cycle at level n, the growth of cycle length is multiplied by 1, p or some d satisfying $d|(p-1)$. That is to say for $1 \leq s < n$, every nonempty intersection of E with a ball of radius p^{-s} contains the same number ($1, p$ or d) of balls of radius $p^{-(s+1)}$. Thus E is a Legendre set. To determine p_s for $1 \leq s < n$, we distinguish three cases: $p \geq 5$, $p = 3$, $p = 2$.

Case $p \geq 5$. In this case, when a cycle grows, its lift grows forever. A cycle at level 1 may start with growing, several times of splitting or several times of partially splitting and then the lifts grow forever. Therefore, there are three ways to form a minimal set. We show the three ways by the growth of cycle length as follows (k being the length of the cycle σ at the level 1).

Case 1. σ grows:

$$(k, kp, kp^2, \dots),$$

Case 2. σ splits:

$$(k, k, \dots, k, kp, kp^2, \dots),$$

Case 3. σ partially splits:

$$(k, kd, \dots, kd, kdp, kdp^2, \dots), \quad d|(p-1), d \geq 2.$$

The above three cases correspond to three kinds of adding machines. However, by the result of Buescu and Stewart [7], the adding machines in both Case 1 and Case 2 are conjugate to $(\mathbb{Z}_{(p_s)}, \tau)$ where $p_s = (k, kp, kp^2, \dots)$. In Case 3, the adding machines are all conjugate to $(\mathbb{Z}_{(p_s)}, \tau)$ where $p_s = (k, kd, kdp, kdp^2, \dots)$ and $d|(p-1), d \geq 2$.

Case $p = 3$. We distinguish four cases.

Case 1. σ grows and its lift also grows:

$$(k, kp, kp^2, \dots),$$

Case 2. σ grows but its lift splits:

$$(k, kp, \dots, kp, kp^2, \dots),$$

Case 3. σ splits:

$$(k, k, \dots, k, kp, kp^2, \dots),$$

Case 4. σ partial splits:

$$(k, kd, \dots, kd, kdp, kdp^2, \dots), \quad d|(p-1), d \geq 2.$$

Then (E, f) is conjugate to $(\mathbb{Z}_{(p_s)}, \tau)$ where $p_s = (k, kd, kdp, kdp^2, \dots)$ with $1 \leq k \leq p$, and $d|(p-1)$.

Case $p = 2$. We distinguish twelve cases.

$$(1, \underbrace{1, 1, \dots 1}_{\text{strongly split}}, 2, 2^2, 2^3, \dots),$$

$$(1, \underbrace{1}_{\text{strongly grows}}, 2, 2^2, 2^3, \dots),$$

$$(1, \underbrace{1}_{\text{weakly splits}}, \underbrace{1}_{\text{weakly grows}}, \underbrace{2, \dots 2}_{\text{strongly split}}, 2^2, 2^3, \dots),$$

$$(1, \underbrace{1}_{\text{weakly grows}}, \underbrace{2, \dots 2}_{\text{strongly split}}, 2^2, 2^3, \dots),$$

$$(1, \underbrace{2, \dots, 2}_{\text{strongly split}}, 2^2, 2^3, \dots),$$

$$(1, \underbrace{2}_{\text{strongly grows}}, 2^2, 2^3, \dots),$$

$$(2,\ \underbrace{2,\dots,2}_{\text{strongly split}}\ ,2^2,2^3,\dots),$$

$$(2,\ \underbrace{2}_{\text{strongly grows}}\ ,2^2,2^3,\dots),$$

$$(2,\ \underbrace{2}_{\text{weakly splits}}\ ,\ \underbrace{2}_{\text{weakly grows}}\ ,\ \underbrace{2^2,\dots,2^2}_{\text{strongly split}},2^3,\dots),$$

$$(2,\ \underbrace{2}_{\text{weakly grows}}\ ,\ \underbrace{2^2,\dots,2^2}_{\text{strongly split}},2^3,\dots),$$

$$(2,\ \underbrace{2^2,\dots,2^2}_{\text{strongly split}},2^3,\dots),$$

$$(2,\ \underbrace{2^2}_{\text{strongly grows}}\ ,2^3,\dots).$$

In any of these cases, the system (E,f) is conjugate to $(\mathbb{Z}_2,x+1)$. □

6. 2-adic Quadratic Polynomials

In this section, we undertake a full investigation on the minimal decomposition of 2-adic quadratic polynomial systems on $\mathbb{Z}_2$ of the form:

$$f(x):=ax^2+bx+c\ (a,b,c\in\mathbb{Z}_2,a\neq 0).$$

As we shall see, the system $f(x)=ax^2+bx+c$ is conjugate to one of the following quadratic polynomials

$$x^2-\lambda,\quad x^2+bx,\quad x^2+x-d$$

where $\lambda\in\mathbb{Z}_2$, $b\equiv 1\pmod 2$ and $\sqrt{d}\notin\mathbb{Z}_2$.

Let us state our results on the minimal decomposition of $(\mathbb{Z}_p,f)$. The proofs are postponed at the end of this section. By the way, we shall discuss the behavior of f on the field $\mathbb{Q}_p$.

If $a\equiv 1\pmod 2$, then $\lim_{n\to\infty}|f^n(x)|=\infty$ for any $x\notin\mathbb{Z}_2$. An elementary calculation shows that ax^2+bx+c on $\mathbb{Z}_2$ is conjugate to x^2+bx+c on $\mathbb{Z}_2$ through the conjugacy $x\mapsto ax$. If $a\equiv 0\pmod 2$, then $\lim_{n\to\infty}|f^n(x)|=\infty$ for any $x\notin\frac{1}{a}\mathbb{Z}_2$ and ax^2+bx+c on $\frac{1}{a}\mathbb{Z}_2$ is conjugate to $x^2+ax+ac$ on $\mathbb{Z}_2$ through the conjugacy $x\mapsto ax$. Thus without loss of generality, we need only to consider the quadratic polynomials of the form

$$x^2+bx+c\ (b,c\in\mathbb{Z}_2).$$

We distinguish two cases according to $b\equiv 0\pmod 2$ or $b\equiv 1\pmod 2$

If $b\equiv 0\pmod 2$, x^2+bx+c is conjugate to

$$x^2-\lambda$$

with $\lambda=\frac{b^2-4c-2b}{4}$, through the conjugacy $x\mapsto x+\frac{B}{2}$.

Theorem 6.1. *Consider the polynomial $f(x)=x^2-\lambda$ on $\mathbb{Z}_2$.*

1) *If $\lambda\equiv 0\pmod 4$, then f admits two attracting fixed points, one in $4\mathbb{Z}_2$ with $2\mathbb{Z}_2$ as its attraction basin, and the other one in $1+4\mathbb{Z}_2$ with $1+2\mathbb{Z}_2$ as its attraction basin.*

2) *If $\lambda\equiv 1\pmod 4$, then the whole $\mathbb{Z}_2$ is attracted into a periodic orbit of period 2 with one orbit point in $4\mathbb{Z}_2$ and the other one in $3+4\mathbb{Z}_2$.*

3) *If $\lambda\equiv 2\pmod 4$, then f admits two attracting fixed points, one in $2+4\mathbb{Z}_2$ $2\mathbb{Z}_2$*

as its attraction basin, and the other one in $3+4\mathbb{Z}_2$ *with* $1+2\mathbb{Z}_2$ *as its attraction basin.*

4) *If* $\lambda \equiv 3 \pmod 4$*, then the whole* $\mathbb{Z}_2$ *is attracted into a periodic orbit of period* 2 *with one orbit point in* $1+4\mathbb{Z}_2$ *and the other one in* $2+4\mathbb{Z}_2$*.*

If $b \equiv 1 \pmod 2$, then x^2+bx+c is conjugate to

$$x^2+x-d$$

where $d = \frac{(b-1)^2-4c}{4} \in \mathbb{Z}_2$, through $x \mapsto x + \frac{b-1}{2}$. It is clear that x^2+x-d admits fixed points if and if only $\sqrt{d} \in \mathbb{Z}_2$. Thus we need to study the case x^2+x-d with $\sqrt{d} \in \mathbb{Z}_2$ and the case x^2+x-d with $d \in \mathbb{Z}_2$ but $\sqrt{d} \notin \mathbb{Z}_2$.

If $\sqrt{d} \in \mathbb{Z}_2$ (i.e. x^2+x-d has a fixed point), then x^2+x-d conjugates to

$$x^2+bx$$

with $b = 1-2\sqrt{d}$, through $x \mapsto x+\sqrt{d}$.

If $b=1$, the minimal decomposition of x^2+x is as follows.

Theorem 6.2. *Consider the polynomial* $f(x) = x^2+x$ *on* $\mathbb{Z}_2[x]$*. There is one fixed point* 0*. We have* $f(1+2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$ *and we can decompose* $2\mathbb{Z}_2$ *into*

$$2\mathbb{Z}_2 = \{0\} \bigsqcup \left(\bigsqcup_{n\geq 2} 2^{n-1}+2^n\mathbb{Z}_2 \right).$$

Each $2^{n-1}+2^n\mathbb{Z}_2$ *(*$n \geq 2$*) consists of* 2^{n-2} *pieces of minimal components:*

$$2^{n-1}+t2^n+2^{2n-2}\mathbb{Z}_2, \quad t = 0, \ldots, 2^{n-2}-1.$$

Denote $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. If $b \equiv 1 \pmod 2$ but $b \neq 1$, we distinguish four subcases:

- $b = 1-4m$, $m \in \mathbb{Z}_2 \setminus \{0\}$;
- $b = -1-4m$, $m \in \mathbb{Z}_2$ with $v_2(m) \in 1+2\mathbb{N}$;
- $b = -1-4m$, $m \in \mathbb{Z}_2$ with $v_2(m) \in 2\mathbb{N}^*$;
- $b = -1-4m$, $m \in \mathbb{Z}_2$ with $v_2(m) = 0$.

If $f(x) = x^2+(-1-4m)x$ with $v_2(m) = 0$, then f is conjugate to $g(x) = x^2+(-1-4(-m-1))x$ with $v_2(-m-1) = v_2(m+1) \geq 1$ through $x \mapsto x-4m-2$. Thus the last case is reduces to the second and the third case. So we need only consider the first three cases.

Before the statement of the following results, we would like to give some terminology to simplify our statements.

We say a 1-cycle (x) at level n is of *type* I-$[k]$ if it splits k times then its lifts grow forever. In this case, the ball $x+p^n\mathbb{Z}_p$ is decomposed into p^k pieces of minimal components. Such a component is a ball of radius p^{-n-k}. Sometimes the ball $x+p^n\mathbb{Z}_p$ is said to be of type I-$[k]$.

We say the a 2-cycle (x,y) at level n is of *type* II-$[k]$ if it splits k times then its lifts grow forever. In this case, the union of two balls $(x+p^n\mathbb{Z}_p) \cup (y+p^n\mathbb{Z}_p)$ is decomposed into p^k pieces of minimal components. Such a component is a union of two balls of radius p^{-n-k}. The union $(x+p^n\mathbb{Z}_p) \cup (y+p^n\mathbb{Z}_p)$ is sometimes said to be of type II-$[k]$. Remark that the union $(x+p^n\mathbb{Z}_p) \cup (y+p^n\mathbb{Z}_p)$ may be a ball of radius p^{-n+1}.

If an invariant subset $E \subset \mathbb{Z}_p$ is a union of invariant subsets $F_n \subset \mathbb{Z}_p,\ n \in J \subset \mathbb{N}$ where each F_n is of type I-$[k]$, we will denote it as

$$E = \bigsqcup_{n\in J} F_n - \{\text{I-}[k]\}.$$

Similarly, if each $F_n \subset \mathbb{Z}_p,\ n \in J \subset \mathbb{N}$ where each F_n is a union of two balls of type II-$[k]$, we will denote it as

$$E = \bigsqcup_{n\in J} F_n - \{\text{II-}[k]\}.$$

Now we are ready to state the following theorems.

Theorem 6.3. *Consider $f(x) = x^2 + (1-4m)x$ with $m \in \mathbb{Z}_2 \setminus \{0\}$. Then f admits two fixed points 0 and $4m$, and $f(1+2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$. We can decompose $2\mathbb{Z}_2$ as*

$$2\mathbb{Z}_2 = \{0, 4m\} \bigsqcup E_1 \bigsqcup E_2 \bigsqcup E_3,$$

where

$$\begin{aligned}
E_1 &= \bigsqcup_{2\le n<v_2(m)+3} \left(2^{n-1} + 2^n\mathbb{Z}_2\right) - \{I\text{-}[n-2]\},\\
E_2 &= \bigsqcup_{n>v_2(m)+3} \left(2^{n-1} + 2^n\mathbb{Z}_2\right) - \{I\text{-}[v_2(m)+1]\},\\
E_3 &= \bigsqcup_{n>v(m)+3} \left(4m + 2^{n-1} + 2^n\mathbb{Z}_2\right) - \{I\text{-}[v_2(m)+1]\}.
\end{aligned}$$

Theorem 6.4. *Consider $f(x) = x^2 + (-1-4m)x$ with $v_2(m) \in 1+2\mathbb{N}$. Then f admits two fixed points 0 and $4m+2$, and $f(1+2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$. We can decompose $2\mathbb{Z}_2$ as*

$$2\mathbb{Z}_2 = \{0, 4m+2\} \bigsqcup E_1 \bigsqcup E_2 \bigsqcup E_3,$$

where

$$\begin{aligned}
E_1 &= \bigsqcup_{n\ge 4} \left(4m + 2 + 2^{n-2} + 2^{n-1}\mathbb{Z}_2\right) - \{II\text{-}[1]\},\\
E_2 &= \bigsqcup_{4\le n\le \lfloor v_2(m)/2\rfloor+3} \left(2^{n-2} + 2^{n-1}\mathbb{Z}_2\right) - \{II\text{-}[2n-5]\},\\
E_3 &= \bigsqcup_{n>\lfloor v_2(m)/2\rfloor+3} \left(2^{n-2} + 2^{n-1}\mathbb{Z}_2\right) - \{II\text{-}[v_2(m)+1]\}.
\end{aligned}$$

Theorem 6.5. *Consider $f(x) = x^2 + (-1-4m)x$ with $v_2(m) \in 2\mathbb{N}^*$. Then f admits fixed points 0 and $4m+2$, and $f(1+2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$. The invariant set $2\mathbb{Z}_2$ admits the following form*

$$2\mathbb{Z}_2 = \{0, 4m+2\} \bigsqcup E_1 \bigsqcup E_2 \bigsqcup E_3 \bigsqcup \left(2^{v_2(m)/2+1} + 2^{v_2(m)/2+2}\mathbb{Z}_2\right),$$

where

$$E_1 = \bigsqcup_{n\geq 4} \left(4m+2+2^{n-2}+2^{n-1}\mathbb{Z}_2\right) - \{II\text{-}[1]\},$$
$$E_2 = \bigsqcup_{4\leq n<v_2(m)/2+3} \left(2^{n-2}+2^{n-1}\mathbb{Z}_2\right) - \{II\text{-}[2n-5]\},$$
$$E_3 = \bigsqcup_{n>v_2(m)/2+3} \left(2^{n-2}+2^{n-1}\mathbb{Z}_2\right) - \{II\text{-}[v_2(m)+1]\}.$$

Denote $E = 2^{v_2(m)/2+1} + 2^{v_2(m)/2+2}\mathbb{Z}_2$.

(1) *If* $v_2(m) = 2$ *and* $v_2(m-4) = 3$, *then* E *is of type* II-[4].
(2) *If* $v_2(m) = 2$ *and* $v_2(m-4) \geq 5$, *then* E *is of type* II-[5].
(3) *If* $v_2(m) = 2$ *and* $v_2(m-4) = 4$, *then there exists a* 2*-periodic orbit with one point* $x_1 \in 4+16\mathbb{Z}_2$ *and the other* $x_2 \in 12+16\mathbb{Z}_2$*; and we can decompose* E *as* $E = \{x_1, x_2\} \bigsqcup E_4$, *where*

$$E_4 = \bigsqcup_{k\geq 5} \left((x_1+2^{k-1}+2^k\mathbb{Z}_2) \cup (x_2+2^{k-1}+2^k\mathbb{Z}_2)\right) - \{II\text{-}[5]\}.$$

(4) *If* $v_2(m) \geq 4$ *and* $v_2(m-2^{v_2(m)}) < v_2(m)+3$, *then* E *is of type* II-$[v_2(m-2^{v_2(m)})+1]$.
(5) *If* $v_2(m) \geq 4$ *and* $v_2(m-2^{v_2(m)}) \geq v_2(m)+3$, *then there exists a* 2*-periodic orbit with one point* $x_1' \in 2^{v_2(m)/2+1}+2^{v_2(m)/2+3}\mathbb{Z}_2$ *and the other* $x_2' \in 2^{v_2(m)/2+1}+2^{v_2(m)/2+2}+2^{v_2(m)/2+3}\mathbb{Z}_2$*; and we can decompose* E *as* $E = \{x_1', x_2'\} \bigsqcup E_4'$, *where*

$$E_4' = \bigsqcup_{k\geq v_2(m)/2+4} \left((x_1'+2^{k-1}+2^k\mathbb{Z}_2) \cup (x_2'+2^{k-1}+2^k\mathbb{Z}_2)\right) - \{II\text{-}[v_2(m)+1]\}.$$

Now we are left to study the polynomials $f(x) = x^2+x-d$ with $d \in \mathbb{Z}_2$ but $\sqrt{d} \notin \mathbb{Z}_2$.

We distinguish four cases.

Theorem 6.6. *Consider* $f(x) = x^2+x-d$ *with* $d \equiv 0 \pmod 4$ *and* $\sqrt{d} \notin \mathbb{Z}_2$. *Then* $f(1+2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$ *and* $2\mathbb{Z}_2$ *is decomposed as finite number of minimal components. Let* $n_0 = \lfloor v_2(d)/2 \rfloor + 1$.

(1) *If* $v_2(d) = 2$ *and* $v_2(d-4) = 3$, *then* $2\mathbb{Z}_2$ *consists of three minimal components:* $4\mathbb{Z}_2$, $2+8\mathbb{Z}_2$ *and* $6+8\mathbb{Z}_2$.
(2) *If* $v_2(d) = 2$ *and* $v_2(d-4) = 4$, *then* $2\mathbb{Z}_2$ *consists of five minimal components:* $4\mathbb{Z}_2$, $2+16\mathbb{Z}_2$, $6+16\mathbb{Z}_2$, $10+16\mathbb{Z}_2$, *and* $14+16\mathbb{Z}_2$.
(3) *If* $v_2(d) \geq 3$ *and* $v_2(d)$ *is odd, then* $2\mathbb{Z}_2 = E_1 \bigsqcup E_2$, *where*

$$E_1 = \bigsqcup_{2\leq n\leq n_0} \left(2^{n-1}+2^n\mathbb{Z}_2\right) - \{I\text{-}[n-2]\},$$
$$E_2 = 2^{n_0}\mathbb{Z}_2 - \{I\text{-}[n_0-1]\}.$$

(4) *If* $v_2(d) \geq 3$ *and* $v_2(d)$ *is even, then* $2\mathbb{Z}_2 = E_1' \bigsqcup E_2' \bigsqcup E_3'$, *where*

$$\begin{aligned} E_1' &= \bigsqcup_{2 \leq n \leq n_0 - 1} \left(2^{n-1} + 2^n \mathbb{Z}_2\right) - \{I\text{-}[n-2]\}, \\ E_2' &= 2^{n_0}\mathbb{Z}_2 - \{I\text{-}[n_0 - 2]\}, \\ E_3' &= 2^{n_0 - 1} + 2^{n_0}\mathbb{Z}_2 - \{I\text{-}[v_2(d - 2^{v_2(d)}) - n_0]\}. \end{aligned}$$

Theorem 6.7. *Consider* $f(x) = x^2 + x - d$ *with* $d \equiv 1 \pmod 4$ *and* $\sqrt{d} \notin \mathbb{Z}_2$. *Then* $f(2\mathbb{Z}_2) \subset 1 + 2\mathbb{Z}_2$ *and* $3 + 4\mathbb{Z}_2$ *is of type* II-[1]. *Let* $d = 5 + 8t$ *with* $t \in \mathbb{Z}_2$. *If* $v_2(t) \leq 1$, *then* $1 + 4\mathbb{Z}_2$ *is of type* II-$[v_2(t) + 2]$. *If* $v_2(t) \geq 2$, *then*

$$1 + 4\mathbb{Z}_2 = \{x_1, x_2\} \bigsqcup E_1 \bigsqcup E_2 \bigsqcup E_3,$$

with the form

$$\begin{aligned} E_1 &= (a + 2^4\mathbb{Z}_2) \cup (f(a) + 2^4\mathbb{Z}_2) - \{II\text{-}[3]\}, \\ E_2 &= (b + 2^5\mathbb{Z}_2) \cup (f(b) + 2^5\mathbb{Z}_2) - \{II\text{-}[3]\}, \\ E_3 &= \bigsqcup_{n \geq 6} (x_1 + 2^n\mathbb{Z}_2) \cup (x_2 + 2^n\mathbb{Z}_2) - \{II\text{-}[3]\}, \end{aligned}$$

and x_1, x_2 *is a* 2*-periodic orbit such that* $x_1 \in c + 2^5\mathbb{Z}_2$ *and* $x_2 \in f(c) + 2^5\mathbb{Z}_2$. *Precisely,*

(1) *If* $v_2(t) = 2$ *and* $v_2(t-4) = 3$, *then* $a = 1, b = 25, c = 9$.
(2) *If* $v_2(t) = 2$ *and* $v_2(t-4) \geq 4$, *then* $a = 1, b = 9, c = 25$.
(3) *If* $v_2(t) = 3$, *then* $a = 9, b = 1, c = 17$.
(4) *If* $v_2(t) \geq 4$, *then* $a = 9, b = 17, c = 1$.

Theorem 6.8. *Consider* $f(x) = x^2 + x - d$ *with* $d \equiv 2 \pmod 4$ *and* $\sqrt{d} \notin \mathbb{Z}_2$. *Then* $f(1 + 2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$.

(1) *If* $v_2(d-2) = 2$, *then* $2\mathbb{Z}_2$ *is of type* II-[1].
(2) *If* $v_2(d-2) = 3$, *then* $8\mathbb{Z}_2 \cup (f(0) + 8\mathbb{Z}_2)$ *is of type* II-[1], $(4 + 8\mathbb{Z}_2) \cup (f(4) + 8\mathbb{Z}_2)$ *consists of a* 2*-periodic orbit with one point* $x_1 \in 4 + 8\mathbb{Z}_2$ *and the other* $x_2 \in f(4) + 8\mathbb{Z}_2$, *and for each* $n \geq 4$, $(x_1 + 2^n\mathbb{Z}_2) \cup (x_2 + 2^n\mathbb{Z}_2)$ *is of type* II-[2]*;*
(3) *If* $v_2(d-2) \geq 4$, *then* $4 + 8\mathbb{Z}_2 \cup (f(4) + 8\mathbb{Z}_2)$ *is of type* II-[1], $8\mathbb{Z}_2 \cup (f(0) + 8\mathbb{Z}_2)$ *consists of a* 2*-periodic orbit with one point* $x_1 \in 8\mathbb{Z}_2$ *and the other* $x_2 \in f(0) + 8\mathbb{Z}_2$, *and for each* $n \geq 4$, $(x_1 + 2^n\mathbb{Z}_2) \cup (x_2 + 2^n\mathbb{Z}_2)$ *is of type* II-[2].

Theorem 6.9. *For* $f(x) = x^2 + x - d$ *with* $d \equiv 3 \pmod 4$, *the ball* $2\mathbb{Z}_2$ *is mapped into the ball* $1 + 2\mathbb{Z}_2$ *which is the unique minimal component.*

We prove Theorems 6.1-6.5. The proofs of Theorems 6.6-6.9 will be omitted since they are similar to those of Theorems 6.1-6.5.

Proof of Theorem 6.1. Let $f(x) = x^2 - \lambda$. Then $f'(x) = 2x$ and $(f^2)'(x) = 4x^3 - 4\lambda x$.

1) If $\lambda \equiv 0 \pmod 4$, then $2 + 4\mathbb{Z}_2$ and $3 + 4\mathbb{Z}_2$ are mapped into $4\mathbb{Z}_2$ and $1 + 4\mathbb{Z}_2$ respectively, and $4\mathbb{Z}_2$ and $1 + 4\mathbb{Z}_2$ are mapped into themselves respectively. Consider the cycles (0) and (1) of f_2. We have

$$a_2(0) = f'(0) \equiv 0 \pmod 2 \quad \text{and} \quad a_2(1) = f'(1) \equiv 0 \pmod 2.$$

Thus cycles (0) and (1) grow tails, hence there will form two attracting fixed points, one in $4\mathbb{Z}_2$ with basin $2\mathbb{Z}_2$, and the other one in $1 + 4\mathbb{Z}_2$ with basin $1 + 2\mathbb{Z}_2$.

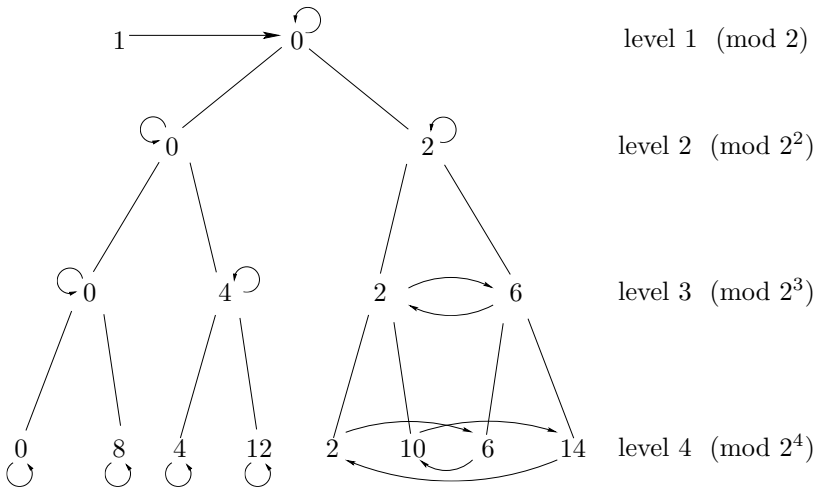
2) If $\lambda \equiv 1 \pmod 4$, then $1+4\mathbb{Z}_2$ and $2+4\mathbb{Z}_2$ are mapped into $4\mathbb{Z}_2$ and $3+4\mathbb{Z}_2$ respectively, and $4\mathbb{Z}_2$ and $3+4\mathbb{Z}_2$ are mapped into $3+4\mathbb{Z}_2$ and $4\mathbb{Z}_2$ respectively. Consider the cycle $(0,3)$ of f_2. We have

$$a_2(0) = (f^2)'(0) \equiv 0 \pmod 2.$$

Thus cycle the cycle $(0,3)$ grows tails, hence there will form an attracting 2-periodic orbit, with one periodic point in $4\mathbb{Z}_2$, and the other one in $3+4\mathbb{Z}_2$. We also see that the attracting basin is the whole $\mathbb{Z}_2$.

The proofs of 3) and 4) are similar to the proofs of 1) and 2). □

Proof of Theorem 6.2. Let $f(x) = x^2 + x$. We will use a diagram to show the structure of the dynamics of f.



At level n, the "$\to$" stands for the transformation of the elements of $\mathbb{Z}/p^n\mathbb{Z}$ under f_n. Thus the diagram shows that

$$f_1(1) = 0,\ f_1(0) = 0, \quad i.e.,\ f(1+2\mathbb{Z}_2) \subset 2\mathbb{Z}_2 \text{ and } f(2\mathbb{Z}_2) \subset 2\mathbb{Z}_2.$$

and

$$f_2(0) = 0,\ f_2(2) = 2, \quad i.e.,\ f(4\mathbb{Z}_2) \subset 4\mathbb{Z}_2 \text{ and } f(2+4\mathbb{Z}_2) \subset 2+4\mathbb{Z}_2.$$

Since $f(1+2\mathbb{Z}_2) \subset 2\mathbb{Z}_2$ and $f^{-1}(1+2\mathbb{Z}_2) = \emptyset$, we need only to consider $2\mathbb{Z}_2$. From the diagram, we also see that (0) is the only cycle of f_1 with length 1, and $(0), (2)$ are two lifts of (0).

We will start our examination from the level 2. Since

$$a_2(0) = f'(0) = 1 \quad \text{and} \quad b_2(0) = \frac{f(0)-0}{2^2} = 0,$$

we have $a_2(0) \equiv 1 \pmod 4$ and

$$A_2(0) = \infty \quad \text{and} \quad B_2(0) = \infty.$$

Thus the cycle (0) strongly splits.

Since

$$a_2(2) = f'(2) = 5 \quad \text{and} \quad b_2(2) = \frac{f(2)-2}{2^2} = 1,$$

we have $a_2(2) \equiv 1 \pmod 4$ and

$$A_2(2) = 2 \quad \text{and} \quad B_2(0) = 0.$$

Thus the cycle (2) strongly grows which implies that the lift of (2) still grows, and so on. Hence $2 + 4\mathbb{Z}_2$ is a minimal component.

By induction we know that for all $n \geq 2$

$$A_n(0) = \infty \quad \text{and} \quad B_n(0) = \infty.$$

Thus the cycle (0) of f_{n-1} always splits to be two cycles (0) and (2^{n-1}) of f_n, and the number 0 should be a fixed point.

Now for $n \geq 2$, let us consider the cycle (2^{n-1}) of f_n. With the same calculations,

$$a_n(2^{n-1}) = 2^n + 1 \quad \text{and} \quad b_n(2^{n-1}) = 2^{n-2}.$$

Thus $a_n(2^{n-1}) \equiv 1 \pmod 4$ and

$$A_n(2^{n-1}) = n \quad \text{and} \quad B_n(2^{n-1}) = n - 2.$$

Hence, the cycle (2^{n-1}) strongly splits and $B_n < \min\{A_n, n\}$. By Proposition 3.2, the lift of (2^{n-1}) splits $B_n - 1 = n - 3$ times then all lifts strongly grow. Thus there are 2^{n-2} pieces of minimal components which constitute $2^{n-1} + 2^n\mathbb{Z}_2$. They are

$$2^{n-1} + t2^n + 2^{2n-2}\mathbb{Z}_2, \quad t = 0, \ldots, 2^{n-2} - 1.$$

This concludes the proof of Theorem 6.2. □

Proof of Theorem 6.3. Let $f(x) = x^2 + (1 - 4m)x$. We see that there are two fixed points 0 and $4m$, and $1 + 2\mathbb{Z}_2$ is mapped into $2\mathbb{Z}_2$. We are concerned with the invariant subset $2\mathbb{Z}_2$.

Consider $2^{n-1} + 2^n\mathbb{Z}_2$ $(n \geq 2)$. We study the cycle (2^{n-1}) at level n. We have

$$a_n(2^{n-1}) = 2^n - 4m + 1 \qquad b_n(2^{n-1}) = 2^{n-2} - 2m,$$

thus $a_n(2^{n-1}) \equiv 1 \pmod 4$ and if $2 \leq n < v_2(m) + 3$,

$$A_n(2^{n-1}) \geq n \qquad B_n(2^{n-1}) = n - 2.$$

If $n = 2$, then the cycle (2^{n-1}) strongly grows. If $n > 2$, then the cycle (2^{n-1}) strongly splits and $B_n < \min\{A_n, n\}$. By Proposition 3.2, the lift of (2^{n-1}) strongly splits $B_n - 1 = n - 3$ times then all lifts strongly grow. Thus we will obtain the part E_1 in Theorem 6.3.

If $n > v_2(m) + 3$,

$$A_n(2^{n-1}) = v_2(m) + 2 \qquad B_n(2^{n-1}) = v_2(m) + 1.$$

Hence, the cycle (2^{n-1}) strongly splits and $B_n < \min\{A_n, n\}$. By Proposition 3.2, the lift of (2^{n-1}) strongly splits $B_n - 1 = v_2(m)$ times then all lifts strongly grow. Hence we have the part E_2.

Consider $4m + 2^{n-1} + 2^n\mathbb{Z}_2$ $(n > v_2(m) + 3)$. Let $s_n \equiv 4m + 2^{n-1} \pmod{2^n}$ and $0 \leq s_n < 2^n$. We study the cycle (s_n) at level n. We have

$$a_n(s_n) = 2s_n - 4m + 1 \qquad b_n(s_n) = \frac{s_n(s_n - 4m)}{2^n},$$

thus $a_n(s_n) \equiv 1 \pmod 4$ and

$$A_n(s_n) = v_2(m) + 2 \qquad B_n(s_n) = v_2(m) + 1.$$

Hence, $B_n < \min\{A_n, n\}$. By Proposition 3.2, the cycle (s_n) strongly splits and the lift of (s_n) strongly splits $B_n - 1 = v_2(m)$ times then all lifts strongly grow. Therefore, we have the part E_3. This completes the proof. □

Proof of Theorem 6.4. Let $f(x) = x^2 + (-1-4m)x$ with $v_2(m) \in 1 + 2\mathbb{N}$. We see that there are two fixed points 0 and $4m+2$, and $1 + 2\mathbb{Z}_2$ is mapped into $2\mathbb{Z}_2$.

Since 0 and $4m+2$ are two fixed points, there are cycles (0) and (t_n) at each level, where $t_n \equiv 4m+2 \pmod{2^n}$ and $0 \le t_n < 2^n$. Consider the cycles (0) and (t_{n-2}) at level $n-2$. By studying the a_{n-2}, b_{n-2} of these two cycles, we know that they weakly split. By Proposition 3.3, after splitting, half of lifts weakly grow. Thus we will obtain two 2-cycles: $(2^{n-2}, 2^{n-2}+2^{n-1})$ and $(s_n, s_n + 2^{n-1})$ at level n, where $s_n \equiv 4m+2+2^{n-2} \pmod{2^{n-1}}$ and $0 \le s_n < 2^{n-1}$.

For each $n \ge 4$, we study the cycle $(s_n, s_n + 2^{n-1})$ at level n. We have

$$a_n(s_n) = 8\left(4\left(\frac{s_n}{2}\right)^3 - 3(4m+1)\left(\frac{s_n}{2}\right)^2 + m(4m+1)s_n + 2m^2 + m\right) + 1$$
$$b_n(s_n) = \frac{1}{2^n} s_n(s_n - 4m - 2)(s_n^2 - 4ms_n - 4m),$$

thus $a_n(s_n) \equiv 1 \pmod 4$ and

$$A_n(s_n) = 3 \qquad B_n(s_n) = 1.$$

Hence, the cycle $(s_n, s_n + 2^{n-1})$ strongly splits and $B_n < \min\{A_n, n\}$. Therefore, by Proposition 3.2, the lift of $(s_n, s_n + 2^{n-1})$ strongly splits $B_n - 1 = 1 - 1 = 0$ times then all lifts strongly grow. Thus we obtain E_1 in Theorem 6.4.

Now we study the cycle $(2^{n-2}, 2^{n-2} + 2^{n-1})$ at level $n \ge 4$. We have

$$a_n(2^{n-2}) = 2^{3n-2} - 3(4m+1)2^{2n-3} + m(4m+1)2^{n+1} + 16m^2 + 8m + 1$$
$$b_n(2^{n-2}) = 2(2^{n-3} - 2m - 1)(2^{2n-6} - m2^{n-2} - m).$$

Thus $a_n(2^{n-2}) \equiv 1 \pmod 4$ and for each $n > \lfloor \frac{v_2(m)}{2} \rfloor + 3$,

$$A_n(2^{n-2}) = v_2(m) + 3 \qquad B_n(2^{n-2}) = v_2(m) + 1.$$

Hence, the cycle $(2^{n-2}, 2^{n-2} + 2^{n-1})$ strongly splits and $B_n < \min\{A_n, n\}$. Therefore, by Proposition 3.2, the lift of $(2^{n-2}, 2^{n-2} + 2^{n-1})$ strongly splits $B_n - 1 = v_2(m) + 1 - 1 = v_2(m)$ times then all lifts strongly grow. Thus we have E_3.

For each $4 \le n \le \lfloor \frac{v_2(m)}{2} \rfloor + 3$,

$$A_n(2^{n-2}) = 2n - 3 \qquad B_n(2^{n-2}) = 2n - 5.$$

Hence, if $n > 4$, then the cycle $(2^{n-2}, 2^{n-2}+2^{n-1})$ strongly splits and $A_n > B_n \ge n$. Therefore, the lift of $(2^{n-2}, 2^{n-2} + 2^{n-1})$ strongly splits at least $n-1$ times. But except this we do not obtain any further more information. Thus Proposition 3.2 is not sufficient for us. Now we do some calculations directly.

For any point $2^{n-2} + t2^{n-1} \in 2^{n-2} + 2^{n-1}\mathbb{Z}_2$, with $t \in \mathbb{Z}_2$, we have

$$f^2(2^{n-2} + t2^{n-1}) - (2^{n-2} + t2^{n-1}) = 2^{n+1}(1+2t) \cdot \Theta, \tag{6·1}$$

where

$$\Theta := (2^{n-3} + t2^{n-2} - 2m - 1)\left((2^{n-3} + t2^{n-2})^2 - m(2^{n-2} + t2^{n-1}) - m\right).$$

Since $4 \leq n \leq \lfloor \frac{v_2(m)}{2} \rfloor + 3$, we have $v_2(\Theta) = 2n-6$, and

$$\begin{aligned} f^2(2^{n-2}+t2^{n-1}) - (2^{n-2}+t2^{n-1}) &\equiv 0 \pmod{2^{3n-5}} \\ &\not\equiv 0 \pmod{2^{3n-4}} \end{aligned}$$

Thus the cycles grow at level $3n-5$. By Corollary 3.9, the cycles grow always. Therefore we obtain the part E_2 which completes the proof. □

Proof of Theorem 6.5. Let $f(x) = x^2 + (-1-4m)x$ with $v_2(m) \in 2\mathbb{N}^*$. We see that there are two fixed points 0 and $4m+2$, and $1+2\mathbb{Z}_2$ is mapped into $2\mathbb{Z}_2$.

As the proof of Theorem 6.4, we study two 2-cycles: $(2^{n-2}, 2^{n-2}+2^{n-1})$ and (s_n, s_n+2^{n-1}) at level n, where $s_n \equiv 4m+2+2^{n-2} \pmod{2^{n-1}}$ and $0 \leq s_n < 2^{n-1}$. The existence of E_1, E_2, E_3 are the same as that of Theorem 6.4.

Consider $2^{n-2}+2^{n-1}\mathbb{Z}_2$ with $n = \frac{v_2(m)}{2} + 3$. We are going to study the cycle $(2^{n-2}, 2^{n-2}+2^{n-1})$ at level n. We study the points $2^{n-2}+t2^{n-1} \in 2^{n-2}+2^{n-1}\mathbb{Z}_2$, with $t \in \mathbb{Z}_2$. With the same calculation in the proof of Theorem 6.4, we have the same equation (6·1). To continue the proof, we will distinguish two cases: $v_2(m) = 2$ and $v_2(m) \geq 4$.

If $v_2(m) = 2$, then $n = v_2(m)/2 + 3 = 4$ and

$$\Theta = (4t-2m+1)[(4-m) + 16(t+t^2) - 4m(1+2t)].$$

Thus if $v_2(m-4) = 3$, then $v_2(\Theta) = 3$ and

$$\begin{aligned} f^2(2^{n-2}+t2^{n-1}) - (2^{n-2}+t2^{n-1}) &\equiv 0 \pmod{2^8} \\ &\not\equiv 0 \pmod{2^9}. \end{aligned}$$

If $v_2(m-4) \geq 5$, then $v_2(\Theta) = 4$ and

$$\begin{aligned} f^2(2^{n-2}+t2^{n-1}) - (2^{n-2}+t2^{n-1}) &\equiv 0 \pmod{2^9} \\ &\not\equiv 0 \pmod{2^{10}}. \end{aligned}$$

Hence we will obtain (1) and (2) of Theorem 6.5.

Since $f^2(x) - x = x(x-4m-2)(x^2-4mx-4m)$, f has 2-periodic orbit if and only if $x^2-4mx-4m = 0$ has solutions different to 0 and $4m+2$ in $\mathbb{Z}_2$. But $x^2-4mx-4mx = 0$ has solution 0 or $4m+2$ only if $m = 0$ or $m = -1$. Thus for the case $v_2(m) \in \mathbb{N}^*$, f has 2-periodic orbit if and if only $\triangle := 16m^2+16m$ has square roots in $\mathbb{Z}_2$. By the standard argument in number theory (see [26], p.18), this is equivalent to $2^{-v_2(m)}m(m+1) \equiv 1 \pmod 8$. By some basic calculations it is then equivalent to $v_2(m-4) = 4$. This is nothing but the rest case we need to study. Thus for $v_2(m-4) = 4$, there exists a 2-periodic orbit.

From the equation $x^2-4mx-4m = 0$, the periodic point can be written as

$$x_1 = 4\left(\frac{m}{2} + \sqrt{\frac{m(m+1)}{4}}\right), \quad x_2 = 4\left(\frac{m}{2} - \sqrt{\frac{m(m+1)}{4}}\right).$$

Recall that we are concerned with $2^{n-2}+2^{n-1}\mathbb{Z}_2$ $(n=4)$ which is the union of two balls $2^{n-2}+2^n\mathbb{Z}_2$ and $2^{n-2}+2^{n-1}+2^n\mathbb{Z}_2$, and we are studying the cycle $(2^{n-2}, 2^{n-2}+2^{n-1})$ at level $n = 4$. Thus we have $x_1 \equiv 4 \pmod{16}$ and $x_2 \equiv 12 \pmod{16}$.

For each $k \geq 5$, we consider the union of the two balls $(x_1 + 2^{k-1} + 2^k\mathbb{Z}_2) \cup (x_2 + 2^{k-1} + 2^k\mathbb{Z}_2)$. We study the cycle (s_1, s_2) where $s_1 \equiv x_1 + 2^{k-1} \pmod{2^k}$,

$s_2 \equiv x_2 + 2^{k-1} \pmod{2^k}$ and $0 \le s_1, s_2 < 2^k$. For every point $x_1 + 2^{k-1} + t2^k \in x_1 + 2^{k-1} + 2^k\mathbb{Z}_2,\ (t \in \mathbb{Z}_2)$, we have

$$\begin{aligned} & f^2(x_1 + 2^{k-1} + t2^k) - (x_1 + 2^{k-1} + t2^k) \\ =& 2^3 \left(\frac{x_1}{4} + 2^{k-3} + t2^{k-2}\right)\left(\frac{x_1}{2} + 2^{k-2} + t2^{k-1} - 2m - 1\right) \cdot \Phi, \end{aligned} \tag{6·2}$$

where

$$\Phi := 2x_1(2^{k-1} + t2^k) + (2^{k-1} + t2^k)^2 - 4m(2^{k-1} + t2^k).$$

Here we have used the property that x_1 is a solution of the equation $x^2 - 4mx - 4m = 0$.

Since $v_2(m) = 2$ and $v_2(x_1) = 2$, we get $v_2(\Phi) = k + 2$. Thus

$$\begin{aligned} f^2(x_1 + 2^{k-1} + t2^k) - (x_1 + 2^{k-1} + t2^k) &\equiv 0 \pmod{2^{k+5}} \\ &\not\equiv 0 \pmod{2^{k+6}}. \end{aligned}$$

Hence we have (3).

Now we are left to treat the case $v_2(m) \ge 4$. In this case the equation $x^2 - 4mx - 4m = 0$ admits solutions if and only if $v_2(m - 2^{v_2(m)}) \ge v_2(m) + 3$.

We still consider $2^{n-2} + 2^{n-1}\mathbb{Z}_2$ with $n = \frac{v_2(m)}{2} + 3$. If $v_2(m - 2^{v_2(m)}) < v_2(m) + 3$, then $v_2(\Theta) = v_2(m - 2^{v_2(m)})$ and for any $t \in \mathbb{Z}_2$

$$\begin{aligned} f^2(2^{n-2} + t2^{n-1}) - (2^{n-2} + t2^{n-1}) &\equiv 0 \pmod{2^{v_2(m-2^{v_2(m)})+n+1}} \\ &\not\equiv 0 \pmod{2^{v_2(m-2^{v_2(m)})+n+2}}. \end{aligned}$$

Then we will obtain (4).

If $v_2(m - 2^{v_2(m)}) \ge v_2(m) + 3$, then $2^{n-2} + 2^{n-1}\mathbb{Z}_2$ consists of a 2-periodic orbit:

$$\begin{aligned} x_1' &= 2^{\frac{v_2(m)}{2}+1}\left(2^{-\frac{v_2(m)}{2}}m + \sqrt{2^{-v_2(m)}m(m+1)}\right), \\ x_2' &= 2^{\frac{v_2(m)}{2}+1}\left(2^{-\frac{v_2(m)}{2}}m - \sqrt{2^{-v_2(m)}m(m+1)}\right). \end{aligned}$$

For each $k \ge \frac{v_2(m)}{2} + 4$, we consider $(x_1' + 2^{k-1} + 2^k\mathbb{Z}_2) \cup (x_2' + 2^{k-1} + 2^k\mathbb{Z}_2)$. For every point $x_1' + 2^{k-1} + t2^k \in x_1' + 2^{k-1} + 2^k\mathbb{Z}_2,\ (t \in \mathbb{Z}_2)$, we have the same calculation as (6·2). Since $k \ge \frac{v_2(m)}{2} + 4$ and $v_2(x_1') = \frac{v_2(m)}{2} + 1$, we get $v_2(\frac{x_1'}{4} + 2^{k-3} + t2^{k-2}) = \frac{v_2(m)}{2} - 2$ and $v_2(\Phi) = \frac{v_2(m)}{2} + k$. Thus

$$\begin{aligned} f^2(x_1' + 2^{k-1} + t2^k) - (x_1' + 2^{k-1} + t2^k) &\equiv 0 \pmod{2^{v_2(m)+k+1}} \\ &\not\equiv 0 \pmod{2^{v_2(m)+k+2}}. \end{aligned}$$

Hence we have (5). This completes the proof. □

References

[1] Y. Amice, *Les Nombres p-adiques*, Presses Universitaires de France, Paris, 1975.

[2] V. S. Anashin, *Uniformly distributed sequences of p-adic integers*, (Russian) Mat. Zametki **55** (1994), no. 2, 3–46, 188; translation in Math. Notes **55** (1994), no. 1-2, 109–133

[3] V. S. Anashin, *Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers*, Computing mathematics and cybernetics, 2. J. Math. Sci. (New York) **89** (1998), no. 4, 1355–1390.

[4] V. S. Anashin, *Uniformly distributed sequences of p-adic integers*, (Russian) Diskret. Mat. **14** (2002), no. 4, 3-64; translation in Discrete Math. Appl. **12** (2002), no. 6, 527-590.

[5] V. S. Anashin, *Ergodic transformations in the space of p-adic integers*, p-adic mathematical physics, 3-24, AIP Conf. Proc., **826**, Amer. Inst. Phys., Melville, NY, 2006.
[6] R. Benedetto, *Fatou components in p-adic dynamics*, Ph. D. thesis. Department of Mathematics, Brown University (1998).
[7] J. Buescu and I. Stewart, *Liapunov stability and adding machines*, Ergod. Th. Dynam. Sys., **15** (1995), no. 2, 271-290.
[8] J.-L. Chabert, A. H. Fan and Y. Fares, *Minimal dynamical systems on a discrete valuation domain*, Discrete and Continuous Dynamical Systems., 25 (2009), no.3, 777-795.
[9] Z. Coelho and W. Parry, *Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers*, In: Topology, ergodic theory, real algebraic geometry, Amer. Math. Soc. Transl. Ser. **2**, **202**, American Mathematical Society (2001), 51-70.
[10] D. L. DesJardins, M. E. Zieve, *Polynomial Mappings mod* p^n, arXiv:math/0103046v1.
[11] V. Dremov, G. Shabat and P. Vytnova, *On the chaotic properties of quadratic*, p-adic mathematical physics, 43-54, AIP Conf. Proc., **826**, Amer. Inst. Phys., Melville, NY, 2006.
[12] A. H. Fan, M. T. Li, J. Y. Yao and D. Zhou, *Strict ergodicity of affine p-adic dynamical systems on* $\mathbb{Z}_p$, Adv. Math., **214** (2007), no. 2, 666-700. See also Ai Hua Fan, Ming-Tian Li, Jia-Yan Yao, Dan Zhou *p-adic affine dynamical systems and applications*, C. R. Math. Acad. Sci. Paris **342** (2006), no. 2, 129-134.
[13] A. H. Fan, L. M. Liao, Y. F. Wang and D. Zhou, *p-adic repellers in* $\mathbb{Q}_p$ *are subshifts of finite type*, C. R. Math. Acad. Sci. Paris **344** (2007), no. 4, 219-224.
[14] A. Yu. Khrennikov, *p-adic quantum mechanics with p-adic valued functions*, J. Math. Phys. **32** (1991), 932-937.
[15] A. Yu. Khrennikov, *p-adic discrete dynamical systems and their applications in physics and cognitive sciences*, Russ. J. Math. Phys. **11** (2004), 45-70.
[16] A. Khrennikov, K.-O. Lindahl, and M. Gundlach, *Ergodicity in the p-adic framework*, In: Operator methods in ordinary and partial differential equations (Stockholm, 2000), Operator Theory: Advances and Applications **132**, Birkhäuser (2002), 245-251.
[17] A. Khrennikov and M. Nilsson, *P-adic deterministic and random dynamics*, Mathematics and its Applications, **574**, Kluwer Academic Publisher, Dordrecht, 2004.
[18] D. E. Knuth, *The art of computer programming. Vol. 1: Fundamental algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont, 1969.
[19] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Second edition, GTM **58**. Springer-Verlag, New York, 1984.
[20] M. V. Larin, *Transitive polynomial transformations of residue rings*, (Russian. Russian summary) Diskret. Mat. **14** (2002), no. 2, 20-32; translation in Discrete Math. Appl. **12** (2002), no. 3, 127-140.
[21] J. Lubin, *Non-archimedean dynamical systems.* Compositio Mathematica **94** (1994), 321-346.
[22] K. Mahler, *p-adic numbers and their functions.* Second edition, Cambridge Tracts in Mathematics, **76**, Cambridge University Press, Cambridge-New York, 1981.
[23] M. Nevins and T. Rogers, *Quadratic maps as dynamical systems on the p-adic numbers*, preprint, (2000).
[24] T. Pezda, *Polynomial cycles in certain local domains*, Acta Arith. **66** (1994), no. 1, 11–22.
[25] W. H. Schikhof, *Ultrametric calculus, An introduction to p-adic analysis*, Cambridge Studies in Advanced Mathematics, **4**, Cambridge University Press, Cambridge, 1984.
[26] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, **7**, Springer-Verlag, New York-Heidelberg, 1973.
[27] P. Walters, *An Introduction to Ergodic Theory.* GTM **79**, Springer-Verlag, New York-Berlin, 1982.
[28] M. Zieve, *Cycles of Polynomial mappings*, Ph. D thesis, UC Berkley 1996.

LAMFA UMR 6140, CNRS, Université de Picardie Jules Verne, 33, Rue Saint Leu, 80039 Amiens Cedex 1, France
E-mail address: ai-hua.fan@u-picardie.fr

LAMFA UMR 8050, CNRS Université Paris-Est Créteil Val de Marne, 61 Avenue du Général de Gaulle, 94010 Créteil Cedex, France & Department of Mathematics, Wuhan University, 430072 Wuhan, China
E-mail address: lingmin.liao@univ-paris12.fr