Round-off errors and p-adic numbers

D. Bosio and F. Vivaldi

School of Mathematical Sciences, Queen Mary and Westfield College,
London E1 4NS, UK

December 14, 1999

Abstract

We explore some connections between round-off errors in linear planar rotations and algebraic number theory. We discretize a map on a lattice in such a way as to retain invertibility, restricting the system parameter (the trace) to rational values with power-prime denominator p^n. We show that this system can be embedded into a smooth expansive dynamical system over the p-adic integers, consisting of multiplication by a unit composed with a Bernoulli shift. In this representation, the original round-off system corresponds to restriction to a dense subset of the p-adic integers. These constructs are based on symbolic dynamics and on the representation of the discrete phase space as a ring of integers in a quadratic number field.

1 Introduction

The study of round-off errors in spatial discretizations of dynamical systems has attracted considerable interest in recent years, due to its rich dynamics, and its significance in theory and applications. A much-studied problem is that of spatial discretizations of linear planar rotations, where the continuum dynamics is regular and well-understood, and where round-off errors can be isolated from other dynamical phenomena [7, 30, 10, 28, 17, 21].

In this paper we explore some connections between round-off errors and p-adic numbers, in a specific model chosen so as to make these links transparent. The study of function iteration over the p-adics defines a broad area of research, relevant to dynamical systems [14, 27, 29, 2, 3, 1, 4, 5, 6, 16], algebraic number theory [25, 32], the theory of formal groups [22, 18, 19], algebraic geometry [15] and computer science [31]. From our perspective, the p-adics provide a natural language to describe certain aspects of irregular motions in a

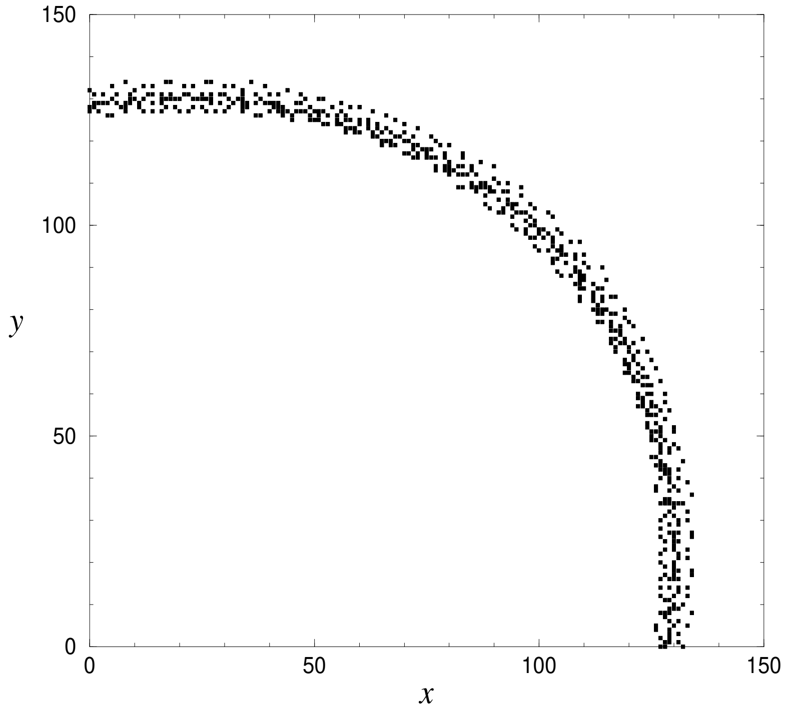

Figure 1: Magnification of an orbit of the discrete mapping (2), with $\alpha = 1/3$. The exact motions (1) are quasi-periodic with irrational rotation number $\nu = \cos^{-1}(1/6)/2\pi = 0.2233\ldots$. The discrete orbit is periodic with period 1952, and it constitutes a fuzzy representation of the Ψ-invariant ellipses $3x^2 + xy - 3y^2 = const.$

discrete setting, and it is hoped that the constructs developed here may find applications beyond the specific model considered.

We consider a linear area-preserving map of the plane, describing elliptic-type motions

$$\Psi : \mathbb{R}^2 \mapsto \mathbb{R}^2 \qquad (x, y) \mapsto (\alpha x - y, x) \qquad |\alpha| < 2. \tag{1}$$

A uniform discretization of the phase space $\mathbb{R}^2$ to the lattice $\mathbb{Z}^2$ can be achieved by introducing the mapping

$$\Phi : \mathbb{Z}^2 \mapsto \mathbb{Z}^2 \qquad \Phi : (x, y) \mapsto (\lfloor \alpha x \rfloor - y, x) \qquad |\alpha| < 2 \tag{2}$$

where $\lfloor \cdot \rfloor$ denotes the floor function (the largest integer not exceeding its argument) [30, 20, 21]. One verifies that Φ is invertible. The map Φ is here regarded as a discrete approximation of Ψ: the discretization length is fixed, and the limit of vanishing discretization corresponds to motions at infinity. A typical orbit for the parameter value $\alpha = 1/3$ is shown in Figure 1. Such orbit is periodic (as apparently are all the orbits of this system —see section 6 below), and it consists of a cloud of points distributed irregularly along an invariant ellipses of the mapping Ψ.

The rounding procedure (2) is chosen so as to make the arithmetic natural. The results presented here extend easily to the case of rounding to the nearest integer, although we shall not consider the latter problem.

We consider a dense set of *irrational* winding numbers ν (where $\alpha = 2\cos(2\pi\nu)$), corresponding to *rational* values of α of the form q/p^n, where p is a *prime*, q is relatively prime to p, and $|q| < 2p^n$. To see that a rational α yields an irrational rotation number, we note that when ν is rational, then α is twice the real part of a primitive root of unity, and standard theory shows that α must be either an integer (in finitely many cases), or an algebraic integer of degree greater than 1 (see, e.g. [23], chapter 2). As α is neither, ν is irrational.

To illustrate the arithmetical rationale behind our choice of parameters, we consider the ring $\mathbb{Z}_p$ of p-adic integers, which may be represented as the set of expressions of the type

$$\chi = b_0 + b_1 p + b_2 p^2 + \cdots \qquad\qquad b_k \in \{0, \ldots, p-1\} \tag{3}$$

which converge with respect to the non-achimedean absolute value $|\cdot|_p$ (one has $|\chi|_p = p^{-k}$, where k is the first non-zero coefficient in the expansion (3) —see, e.g., [13], part II). The main result of this paper is the following theorem, which establishes a connection between the round-off problem and the p-adics

Theorem 1 *There exists a dense embedding* $\mathcal{L} : \mathbb{Z}^2 \mapsto \mathbb{Z}_p$, *such that the mapping* $\Phi^* = \mathcal{L} \circ \Phi \circ \mathcal{L}^{-1}$ *can be extended continuously from* $\mathcal{L}(\mathbb{Z}^2)$ *to the whole of* $\mathbb{Z}_p$, *giving*

$$\chi_{t+1} = \Phi^*(\chi_t) = \sigma^n(\overline{\theta}\, \chi_t)$$

where $\overline{\theta} = \mathcal{L}(q, p^n)$ *is a* p*-adic unit and* σ *is the shift mapping.*

A p-adic unit is a p-adic integer (3) with $b_0 \neq 0$. The shift mapping σ on $\mathbb{Z}_p$ is defined by analogy with its archimedean counterpart [27, 2, 31]. If χ is given by (3), then

$$\sigma(\chi) \;=\; b_1 + b_2 p + b_3 p^2 + \cdots . \tag{4}$$

This is a smooth expansive map (the modulus of its derivative is equal to $|\bar{\theta} p^{-n}|_p = p^n > 1$), with a dense set of unstable periodic orbits. It preserves the standard probability measure on $\mathbb{Z}_p$ (the additive Haar measure), obtained by assigning to the residue class $x \pmod{p^k}$ the measure p^{-k}.

The above theorem will follow from propositions 4.1 and 4.2. In the rest of this section we outline the main constructs and results of this paper.

We first define a natural symbolic dynamics. The round-off error at the point (x, y) affects only the x-coordinate (cf. (2)), and it is given by

$$\frac{xq}{p^n} - \left\lfloor \frac{xq}{p^n} \right\rfloor = \frac{c}{p^n}$$

where c is the smallest non-negative residue of xq modulo p^n

$$c = c(x) \equiv x\,q \pmod{p^n} \qquad\qquad 0 \leq c < p^n. \tag{5}$$

Coding such errors by the value of c defines a symbolic dynamics on p^n symbols. The symbolic sequence of the orbit through (x, y) will be denoted by

$$\mathcal{C} = \mathcal{C}(x, y) = (c_0, c_1, c_2, \ldots) \tag{6}$$

where $c_t = c(x_t)$, and (x_t, y_t) is the t-th point in the orbit with initial condition $(x, y) = (x_0, y_0)$.

In section 2 we characterize the initial conditions of the orbits that share the first k symbols in the code (6). We show that such points are congruent modulo a two-dimensional lattice $\mathcal{M}_k$ in $\mathbb{Z}^2$, which we construct explicitly. In section 3 we provide the necessary arithmetical background, by means of which we prove (proposition 4.1, section 4) that the phase space can be embedded into the integers of a quadratic imaginary number field, where $\mathcal{M}_k$ becomes the $(k+1)n$-th power of a prime ideal divisor of p.

Using a standard number-theoretical construction, we then *localize* the phase space, i.e., we embed it within the p-adic integers $\mathbb{Z}_p$. We show (proposition 4.2, section 4) that the local map can be extended to the whole of $\mathbb{Z}_p$, where the action of the linear map (1) is represented by multiplication by a p-adic unit, while the round-off becomes a Bernoulli shift. Such localization provides $\mathbb{Z}^2$ with a non-archimedean metric, according to which two points are close to each other when their corresponding symbolic orbits share many symbols. The p-adic Newton's method then gives a superconvergent algorithm for the construction of such metric, and other computations.

We then consider the p-adic function that maps the initial conditions to the corresponding code, and show that it is a nowhere differentiable isometry of the p-adic integers (proposition 5.1, section 5). Exploiting the completeness of the code, we construct explicitly all periodic orbits of the embedding system in $\mathbb{Z}_p$ (proposition 5.2, section 5). As a by-product, we construct an embedding dynamical system on the plane, defined on rational points with denominator coprime to p, whose periodic orbits are in bi-unique correspondence with the p-adic ones.

The last section contains concluding remarks.

For background references in arithmetic, see [11] (quadratic integers) and [13] (p-adics).

One of us (FV) is grateful to Charles Leedham-Green for a stimulating conversation on p-adics.

2 Lattices

We begin by defining the *k-code* C_k of an orbit

$$C_k = (c_0, c_1, \ldots, c_{k-1})$$

as the symbolic code of the first k points in the orbit (cf. (5)). We define the sequence of mappings

$$h_k : \mathbb{Z}^2 \to \mathbb{Z}/p^{kn}\mathbb{Z} \qquad h_k(x,y) \equiv a_k x + b_k y \,(\mathrm{mod}\; p^{kn}) \tag{7}$$

where

$$a_1 = 1; \quad b_1 = 0; \qquad \begin{cases} a_{k+1} = q\, a_k + \; p^n\, b_k \\ b_{k+1} = -p^n\, a_k \end{cases} \qquad k \geq 1, \tag{8}$$

and we denote by $\mathcal{M}_k$ the kernel of h_k

$$\mathcal{M}_k \;=\; \{(x,y) \in \mathbb{Z}^2 \;:\; a_k x + b_k y \equiv 0 \,(\mathrm{mod}\; p^{kn})\}. \tag{9}$$

Our first result characterizes the sets $\mathcal{M}_k$ geometrically.

Proposition 2.1 *The sets $\mathcal{M}_k$ form a nested sequence of lattices: $\mathcal{M}_{k+1} \subset \mathcal{M}_k$, with $\mathbb{Z}$-basis*

$$\mathbf{e}_1 \;=\; (p^{kn}, 0); \qquad \mathbf{e}_2 \;=\; (r_k, 1)$$

where

$$r_k \equiv -\frac{b_k}{a_k} \,(\mathrm{mod}\; p^{kn}). \tag{10}$$

In particular, the quotient $\mathbb{Z}^2/\mathcal{M}_k$ has p^{kn} elements.

Proof: The mapping h_k is a homomorphism of additive groups, as easily verified. Its kernel $\mathcal{M}_k$ is therefore an additive subgroup of $\mathbb{Z}^2$. Because $a_{k+1} \equiv q\, a_k \pmod{p^n}$ (equation (8)), and q and a_1 are coprime to p, all the a_k are also coprime to p. Then the image under h_k of (say) the p^{nk} points $(0,y)$, $(1,y)$, …, $(p^{nk}-1,y)$ form a complete residue system modulo p^{nk}. It follows that $h_k(\mathbb{Z}^2)$ has p^{kn} elements, and so does $\mathbb{Z}^2/\mathcal{M}_k$.

By definition, the point $(x,0)$ belongs to $\mathcal{M}_k$ when $a_k\, x \equiv 0 \pmod{p^{kn}}$, and since a_k is coprime to p, p^{kn} divides x. Therefore p^{kn} is the smallest positive value of x for which $(x,0) \in \mathcal{M}_k$, and since $\mathbb{Z}^2/\mathcal{M}_k$ has p^{kn} elements, we can choose as representatives of the latter the points $(0,0), (1,0)$, …, $(p^{kn}-1,0)$. It follows that $\mathcal{M}_k$ has the $\mathbb{Z}$-basis $(p^{kn},0)$ and $(r_k,1)$, where r_k is determined by the condition

$$a_k\, r_k \;+\; b_k \equiv 0 \pmod{p^{kn}}$$

giving

$$r_k \equiv -\,\frac{b_k}{a_k} \pmod{p^{kn}}$$

since a_k is invertible modulo p^{kn}.

It remains to show that $\mathcal{M}_{k+1} \subset \mathcal{M}_k$, that is, that

$$h_{k+1}(z) \equiv 0 \pmod{p^{(k+1)n}} \quad\Longrightarrow\quad h_k(z) \equiv 0 \pmod{p^{kn}}.$$

The above will follow from the estimate

$$a_{k+1}x + b_{k+1}y = q(a_k x + b_k y) + O(p^{kn}) \tag{11}$$

where $O(p^{kn})$ denotes an arbitrary integer divisible by p^{kn}. Equation (11) is true for $k = 1$

$$a_2 x + b_2 y = qx - p^n y = q a_1 x + q b_1 y - p^n y = q(a_1 x + b_1 y) + O(p^n).$$

Assume it true for some $k \geq 1$. We have

$$\begin{aligned} a_{k+2}x + b_{k+2}y &= q a_{k+1}x + p^n b_{k+1}x - p^n a_{k+1}y \\ &= q a_{k+1}x + q b_{k+1}y - p^{2n} a_k x - p^{2n} b_k y \\ &= q(a_{k+1}x + b_{k+1}y) - p^{2n}(a_k x + b_k y) \\ &= q(a_{k+1}x + b_{k+1}y) + O(p^{(k+1)n}). \end{aligned}$$

This completes the inductive proof of (11), and of the proposition.

$\square$

The basis for $\mathcal{M}_k$ may be computed from equation (10) and the recursion (8). Below we shall derive a faster (superconvergent) algorithm for such basis computation.

The next result shows the significance of the lattices $\mathcal{M}_k$ to the symbolic dynamics of the round-off mapping.

Proposition 2.2 *Two points in $\mathbb{Z}^2$ have the same k-code if and only if they are congruent modulo $\mathcal{M}_k$.*

Proof: Let $z, z' \in \mathbb{Z}^2$ and let $z_t = (x_t, y_t)$. From (5) and the fact that q is coprime to p we have that

$$C_k(z_0) = C_k(z'_0) \qquad \Longleftrightarrow \qquad x_t \equiv x'_t \pmod{p^n}, \qquad t = 0, \ldots, k-1. \tag{12}$$

We proceed by induction. Our proposition is true for $k = 1$, from (12) and the fact that $h_1(z_0) \equiv x_0 \pmod{p^n}$. We assume it to be true for some $k \geq 1$ and first prove the implication $\Longrightarrow$ of the proposition for $k+1$.

Let $C_{k+1}(z_0) = C_{k+1}(z'_0)$. Then $C_k(z_1) = C_k(z'_1)$ and by the induction hypothesis, $z_1 \equiv z'_1 \pmod{\mathcal{M}_k}$, that is,

$$a_k\left(\frac{qx_0}{p^n} - \frac{c(x_0)}{p^n} - y_0 - \frac{qx'_0}{p^n} + \frac{c(x'_0)}{p^n} + y'_0\right) + b_k(x_0 - x'_0) \equiv 0 \pmod{p^{kn}}.$$

Multiplying the above congruence by p_n, and recalling that $c(x_0) = c(x'_0)$, we obtain

$$(qa_k + p^n b_k)(x_0 - x'_0) - p^n a_k(y_0 - y'_0) = a_{k+1}(x_0 - x'_0) + b_{k+1}(y_0 - y'_0) \equiv 0 \pmod{p^{(k+1)n}}$$

i.e., $z_0 \equiv z'_0 \pmod{\mathcal{M}_{k+1}}$.

We prove the implication $\Longleftarrow$ for $k+1$. Let $z_0 \equiv z'_0 \pmod{\mathcal{M}_{k+1}}$. Then $z_0 \equiv z_0 \pmod{\mathcal{M}_k}$ (Proposition 2.1), whence $C_k(z_0) = C_k(z'_0)$, from the induction hypothesis. We must show that $z_1 \equiv z'_1 \pmod{\mathcal{M}_k}$. Indeed

$$\begin{aligned} a_k(x_1 - x'_1) + b_k(y_1 - y'_1) &= a_k\left(\frac{qx_0}{p^n} - \frac{qx'_0}{p^n} - y_0 + y'_0\right) + b_k(x_0 - x'_0) \\ &= \frac{1}{p^n}\left[(qa_k + p^n b_k)(x_0 - x'_0) - p^n a_k(y_0 - y'_0)\right] \\ &= \frac{1}{p^n}\left[a_{k+1}(x_0 - x'_0) + b_{k+1}(y_0 - y'_0)\right] = O(p^{kn}). \end{aligned}$$

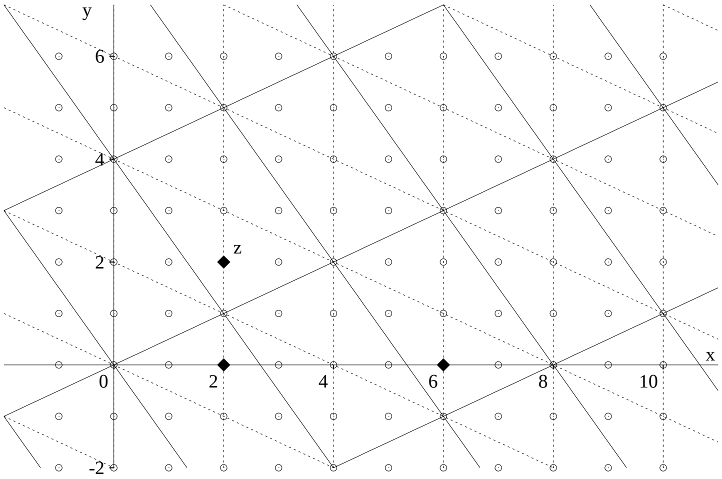

Figure 2: Structure of the phase space $\mathbb{Z}^2$, for the parameter value $\alpha = 1/2$. The lattices $\mathcal{M}_2$ and $\mathcal{M}_3$ are represented by dotted and solid lines, respectively. The point $z = (2, 2)$ is congruent to $(2, 0)$ modulo $\mathcal{M}_2$, to $(6, 0)$ modulo $\mathcal{M}_3$, and to some $(x^{(k)}, 0)$ modulo $\mathcal{M}_k$. Congruent points share the first k symbols. The sequence $\{x^{(k)}\}$ converges to a 2-adic integer.

This completes the proof. ☐

The above result shows that the *finite* symbolic code is complete. The zero k-code $(\underbrace{0, 0, \ldots, 0}_{k})$ corresponds to initial conditions in $\mathcal{M}_k$, while the form of the basis (10) implies that every possible finite code can be generated from initial conditions of the type $(x, 0),\ x \geq 0$. This is the geometric manifestation of an arithmetical phenomenon called *localization,* which will be described in the next section (see Figure 2).

3 The arithmetical environment

The development of the theory requires some arithmetical constructs, related to a prominent set of quadratic integers. The connection between dynamics and arithmetic is established by considering the matrix A associated to the recursion (8)

$$A = \begin{pmatrix} q & p^n \\ -p^n & 0 \end{pmatrix}.$$

Its characteristic polynomial

$$f(X) \;=\; X^2 - q\,X + p^{2n} \tag{13}$$

has discriminant $\Delta \;=\; q^2 - 4\,p^{2n} \;<0$, so that $f(X)$ is irreducible. The complex eigenvalues λ and $\overline{\lambda}$ are given by

$$\lambda \;=\; \frac{q\,-\,\sqrt{q^2-4p^{2n}}}{2}; \qquad \lambda^2 = q\,\lambda - p^{2n}; \qquad \overline{\lambda} = q - \lambda. \tag{14}$$

All the action will take place in the ring $\mathbb{Z}[\lambda]$, which is the set of numbers of the form $x+y\lambda$ with x and y integers. $\mathbb{Z}[\lambda]$ consists of algebraic integers in $\mathbb{Q}(\lambda)$, the field obtained by adjoining λ to the rationals.

From (13), we see that $f(X)$ factors modulo p^{2n} into the product of two polynomials

$$f(X) \equiv X(X-q)\;(\mathrm{mod}\; p^{2n}) \tag{15}$$

which are *distinct* modulo p^{2n}, because p and q are coprime. This implies that the prime p splits in $\mathbb{Z}[\lambda]$ into the product of two distinct prime ideals: $(p) \;=\; P\overline{P}$ (see, e.g., [23], chapter 3). Geometrically, these ideals are two-dimensional lattices, which will play a key role in our construction.

(At various points in what follows, we shall implicitly rely on the unique factorization of powers of P in $\mathbb{Z}[\lambda]$. This is legitimate, because even though $\mathbb{Z}[\lambda]$ may not be the maximal order, the norm of these ideals is relatively prime to the discriminant of $f(X)$, whence to the ring index of $\mathbb{Z}[\lambda]$ —see [11], chapter XIII for details.)

The roots of $f(X)$ modulo p^n are 0 and q. We have

$$f'(X) = 2\,X\;-q; \qquad\qquad f'(0) = -q; \qquad\qquad f'(q) = q,$$

and since q and p are coprime, the derivative of f at such roots does not vanish modulo p. Therefore these roots lift to two distinct p-adic roots θ and $\overline{\theta}$, which are the local images of λ and $\overline{\lambda}$ in $\mathbb{Z}_p$, the ring of p-adic integers. Such roots may be computed via Newton's iteration

$$\theta_{s+1} \;=\; \theta_s - \frac{f(\theta_s)}{f'(\theta_s)} \;=\; \frac{\theta_s^2 - p^{2n}}{2\,\theta_s - q}, \tag{16}$$

with initial conditions $\theta_1 = 0$ and $\overline{\theta}_1 = q$, respectively. The sequence $\theta_s \to \theta$ is superconvergent ([26], section 2.2). One can show that

$$\theta \equiv \theta_s \,(\mathrm{mod}\ p^{2^s n}) \qquad\qquad \overline{\theta} \equiv \overline{\theta}_s \,(\mathrm{mod}\ p^{2^s n}).$$

For instance, letting $n = 1$, $q = 1$ and $p = 2$, three iterations of (16) yield the 2-adic expansion of θ with 16 digits accuracy

$$\theta_4 = \frac{-52}{119} \equiv 56724 \,(\mathrm{mod}\ 2^{16}) \qquad\qquad \theta = 0010100110111011\ldots$$

We find

$$\theta = \frac{p^{2n}}{q} + \frac{p^{4n}}{q^3} + 2\,\frac{p^{6n}}{q^5} + 5\,\frac{p^{8n}}{q^7} + \cdots \tag{17}$$

The integral bases for the powers of P are constructed from the p-adic approximations to θ, as follows

Lemma 3.1 *For all $k \geq 1$, the ideals P^k have the $\mathbb{Z}$-basis*

$$P^k = [p^k, s_k - \lambda] \qquad \text{with} \qquad s_k \equiv \theta \,(\mathrm{mod}\ p^k). \tag{18}$$

Moreover, the even powers of P^n are principal:

$$P^{2kn} = (\lambda^k) \qquad k = 1, 2, \ldots. \tag{19}$$

The odd powers of P^n need not be principal, e.g., for $p = 2$, $q = n = 1$.

Proof: Because the norm of P^k is p^k, and the smallest positive integer contained in P^k is p^k (lest P and $\overline{P}$ would not be distinct), we conclude that the $\mathbb{Z}$-basis of P^k must be of the form (18), for a suitable s_k to be determined modulo p^k. The congruence class of s_k is determined by noting that the local image of λ is θ, and that the local image of each basis element must be congruent to zero modulo p^k.

To prove (19), it suffices to consider the case $k = 1$. Because $\theta \equiv 0 \,(\mathrm{mod}\ p^{2n})$ (see (17)), we can choose $s_{2n} = 0$ in (18). We then find that $-\lambda \in P^{2n}$, so that $(\lambda) \subset P^{2n}$, and since (λ) and P^{2n} have the same norm, they are equal. □

4 Localization

In this section we embed the round-off dynamics (2) into the ring $\mathbb{Z}_p$ of p-adic integers. Firstly, we establish a correspondence between $\mathbb{Z}^2$ and $\mathbb{Z}[\lambda]$, identifying $\mathbb{Z}^2$ with P^n, and the lattice $\mathcal{M}_k$ with $P^{(k+1)n}$ (proposition 4.1). Secondly, we embed homomorphically the ring $\mathbb{Z}[\lambda]$ into $\mathbb{Z}_p$, by means of the prime ideal P. Finally, we construct the local representation of the round-off mapping, and extend it to the whole of $\mathbb{Z}_p$ (proposition 4.2).

We require several mappings. The first mapping embeds $\mathbb{Z}^2$ into $\mathbb{Z}[\lambda]$.

$$\mathcal{L}_1 : \mathbb{Z}^2 \mapsto \mathbb{Z}[\lambda] \qquad (x, y) \mapsto p^n x - \lambda y. \tag{20}$$

The second mapping creates a homomorphic image $\mathcal{R}$ of $\mathbb{Z}[\lambda]$ in $\mathbb{Z}_p$, by identifying λ with its local image θ

$$\mathcal{L}_2 : \mathbb{Z}[\lambda] \ \mapsto \ \mathbb{Z}_p \qquad x + \lambda y \ \mapsto \ x + \theta\, y \tag{21}$$

Composing the above two mappings and scaling, we obtain an embedding of our discrete phase space into the p-adics

$$\mathcal{L} : \mathbb{Z}^2 \mapsto \mathbb{Z}_p \qquad (x, y) \mapsto \frac{1}{p^n}\, \mathcal{L}_2(\mathcal{L}_1(x, y)) \ = \ x - \frac{\theta}{p^n}\, y. \tag{22}$$

The image of the round-off phase space

$$\mathcal{Z} = \mathcal{L}(\mathbb{Z}^2) \ \subset \mathbb{Z}_p \tag{23}$$

is an additive subgroup of the p-adic integers, which is invariant under multiplication by elements of the ring $\mathcal{R} = \mathcal{L}_2(\mathbb{Z}[\lambda])$ (i.e., $\mathcal{Z}$ is a $\mathcal{R}$-module).

The next result describes two features of embedding.

Proposition 4.1 *Let $\mathcal{L}_1$ and $\mathcal{L}$ be given by (20) and (22), respectively. Then*
i)

$$\mathcal{L}_1(\mathbb{Z}^2) = P^n \qquad \mathcal{L}_1(\mathcal{M}_k) \ = \ P^{(k+1)n} \qquad k = 1, 2, \ldots.$$

ii) The function

$$(x, y) \ \mapsto \ \|(x, y)\|_p \ = \ |\mathcal{L}(x, y)|_p \tag{24}$$

where $|\cdot|_p$ is the p-adic absolute value, defines a non-archimedean norm on $\mathbb{Z}^2$, such that $\|z - z'\|_p = p^{-kn}$ if and only the codes of z and z' have precisely the first k symbols in common.

Proof: *i)* We begin to relate the lattices $\mathcal{M}_k$ to the algebraic integer λ, by showing that if a_k and b_k are as in (8), then

$$\lambda^k = a_k\,\lambda + b_k\,p^n \qquad k = 1, 2, \ldots. \tag{25}$$

Indeed for $k = 1$ we have $\lambda = a_1\,\lambda + b_1\,p^n$, as $a_1 = 1$ and $b_1 = 0$. Furthermore, using (14) we find

$$\begin{aligned} \lambda^{k+1} &= \lambda\,\lambda^k = \lambda(a_k\lambda + b_k\,p^n) = a_k\lambda^2 + b_k\lambda\,p^n \\ &= (q\,a_k + p^n\,b_k)\lambda + p^n(-p^n\,a_k) = a_{k+1}\lambda + b_{k+1}p^n \end{aligned}$$

which completes the induction.

Let now θ be the p-adic image of λ, and let r_k be as in proposition 2.1. We shall prove that

$$p^n\,r_k \equiv \theta\,(\text{mod}\ p^{(k+1)n}) \qquad k = 1, 2, \ldots \tag{26}$$

To establish this congruence, we note that from (25) we have that

$$-p^n\,\frac{b_k}{a_k} \;=\; \lambda - \frac{\lambda^k}{a_k}$$

which corresponds to the $\mathbb{Z}_p$ equation

$$-p^n\,\frac{b_k}{a_k} \;=\; \theta - \frac{\theta^k}{a_k}.$$

Because $\theta \equiv 0\,(\text{mod}\ p^{2n})$ and a_k is coprime to p, we have that $\theta^k/a_k \equiv 0\,(\text{mod}\ p^{2kn})$, giving the congruence

$$-p^n\,\frac{b_k}{a_k} \equiv \theta\,(\text{mod}\ p^{2kn}).$$

Equation (26) now follows from proposition 2.1.

From (17) and lemma 3.1 we have that $s_1 \equiv 0\,(\text{mod}\ p^n)$, which shows that the image of $\mathbb{Z}^2$ under $\mathcal{L}_1$ is P^n. From proposition 2.1 we have that every $z \in \mathcal{M}_k$ has the form $z = (p^{kn}\,x + r_k\,y,\, y)$, for some integers x and y. Thus

$$\mathcal{L}_1(z) \;=\; p^n\,(p^{kn}\,x + r_k\,y) - \lambda\,y \;=\; p^{(k+1)n}\,x + (p^n\,r_k - \lambda)y.$$

From lemma 3.1 and congruence (26) we have that $p^n\,r_k \equiv s_{(k+1)n}\,(\text{mod}\ p^{(k+1)n})$, which shows that $\mathcal{L}_1(z) \in P^{(k+1)n}$, that is, $\mathcal{L}_1(\mathcal{M}_k) \subseteq P^{(k+1)n}$. Retracing the above steps, one proves that $\mathcal{L}_1(\mathcal{M}_k) \supseteq P^{(k+1)n}$. This completes the proof of part *i)*.

ii) The statement that $\|\cdot\|_p$ is a non-archimedean metric follows from the fact that $|\cdot|_p$ has the same property and $\mathcal{L}$ is a monomorphism of $\mathbb{Z}$-modules. If z and z' have the same code, then from propositions 2.2 and 4.1 *i*) we have that $\mathcal{L}_1(z-z')$ is divisible by $P^{(k+1)n}$ and no larger power of P. It follows that $\mathcal{L}(z-z')$ is divisible by p^{kn} and no larger power of p, whence $|\mathcal{L}(z-z')|_p = p^{-kn}$. The above chain of implications can be reversed, to yield the converse statement. $\square$

Because $\mathcal{L}$ is a monomorphism, we may define

$$\Phi^* : \mathcal{Z} \mapsto \mathcal{Z} \qquad\qquad \Phi^* \,=\, \mathcal{L}\circ\Phi\circ\mathcal{L}^{-1}. \tag{27}$$

The next result characterizes the above mapping as the composition of multiplication by a unit and the n-fold shift. Together with proposition 4.1, this will establish theorem 1.

Proposition 4.2 *The local round-off mapping* Φ^* *can be extended continuously to the whole of* $\mathbb{Z}_p$*, giving*

$$\chi_{t+1} = \Phi^*(\chi_t) = \sigma^n(\overline{\theta}\,\chi_t) \tag{28}$$

where $\overline{\theta} = \mathcal{L}_2(\overline{\lambda})$*, and* σ *is the shift mapping.*

Proof: Let $\chi = x - y\theta/p^n$, with x and y integer. Then $\chi \in \mathcal{L}_1(\mathbb{Z}[\lambda])$, from proposition 4.1 *i*). Thus

$$\begin{aligned}
\Phi^*(\chi) &= (\mathcal{L}\circ\Phi)(x,y) \,=\, \mathcal{L}\left(\left\lfloor \frac{q\,x}{p^n}\right\rfloor - y, x\right)\\
&= \left\lfloor \frac{q\,x}{p^n}\right\rfloor - y - \frac{\theta}{p^n}\,x \,=\, \frac{1}{p^n}\Big(x\,(q-\theta) - p^n\,y - c(x)\Big)\\
&= \frac{1}{p^n}\Big(x\overline{\theta} - \frac{\theta\overline{\theta}}{p^n}\,y - c(x)\Big) \,=\, \frac{1}{p^n}\Big(\overline{\theta}\,\chi - c(x)\Big)
\end{aligned}$$

where $c(x)$ is the the first symbol of the orbit through (x,y), given by (5). Now, from (17) we have that $y\,\theta/p^n = O(p^n)$, and therefore $qx \equiv q\chi \equiv \overline{\theta}\chi \pmod{p^n}$, which shows that

$$\Phi^*(\chi) \,=\, \sigma^n(\overline{\theta}\chi).$$

Now, if $\chi^{(k)} \to \chi$ is a Cauchy sequence in $\mathcal{Z}$, so is $\sigma^n(\overline{\theta}\chi^{(k)})$, and we can extend the mapping Φ^* to the whole of $\mathbb{Z}_p$. This proves equation (28).

□

We note that the restriction of the local mapping to $\mathcal{Z}$ is invertible (whereas the extended mapping is not). The inverse is most easily found using the reversing symmetry of Φ. We find

$$\Phi^{-1} = G \circ \Phi \circ G \qquad \text{with} \qquad G = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This relation translates into an identical relation of local maps.

5 Coding function and periodic orbits

We consider the function $\mathcal{C}$ that maps the initial point $\chi \in \mathbb{Z}_p$ of a local orbit, into the corresponding symbolic code $(c_0, c_1, \ldots)$. The latter is easily defined, for instance, as the limit of the codes through the points $(x^{(k)}, 0) \in \mathbb{Z}^2$ (cf. (6)), where $x^{(k)} \to \chi$. We shall obtain an explicit representation for the periodic orbits (proposition 5.2), and from it an embedding system for the original round-off mapping, sharing the same periodic orbits structure.

It is useful to represent the code as a p-adic integer, rather than an element of an abstract sequence space. We write

$$\mathcal{C}(\chi) \; = \sum_{k=0}^{\infty} c_k p^{nk}.$$

Then we have

Proposition 5.1 *The function $\mathcal{C}$ defines an isometric bijection of $\mathbb{Z}_p$, which is nowhere differentiable.*

Proof: The metric-preserving property of $\mathcal{C}$ follows from proposition 4.1 *ii*), since for any p-adic integers χ and χ', we have that $\mathcal{C}(\chi) \equiv \mathcal{C}(\chi') \pmod{p^{kn}}$ if and only if $\chi \equiv \chi' \pmod{p^{kn}}$. In particular $\mathcal{C}$ is continuous and injective.

Let now $C = (c_0, c_1, \ldots)$ be an arbitrary code, and let

$$\chi = \frac{1}{\theta} \sum_{t=0}^{\infty} c_t \left(\frac{p^n}{\overline{\theta}} \right)^t. \tag{29}$$

Because $\overline{\theta}$ is a unit, such expansion converges in $\mathbb{Z}_p$ to an element χ, determined uniquely by the sequence C. From (28), we have that, for any $t \geq 0$

$$\chi_t = (\Phi^*)^t(\chi) = \frac{1}{\overline{\theta}} \sum_{k=0}^{\infty} c_{k+t} \left(\frac{p^n}{\overline{\theta}}\right)^k , \tag{30}$$

which shows that χ is the unique initial condition in $\mathbb{Z}_p$ corresponding to the code C. So we may write $\chi = \mathcal{C}^{-1}(C)$. Since the code was arbitrary, $\mathcal{C}$ is a bijection.

It remains to prove the lack of differentiability. We consider a sequence of codes $C^{(k)} = C + p^{kn}$ converging to C, and we let $\chi^{(k)} = \mathcal{C}^{-1}(C^{(k)})$ with $\chi = \mathcal{C}^{-1}(C)$. Then $\chi^{(k)} \to \chi$, by continuity, while $\chi^{(k)} \neq \chi$, since $\mathcal{C}$ is a bijection. We consider the incremental ratio

$$\Delta_k = \frac{C^{(k)} - C}{\chi^{(k)} - \chi} = \frac{\bar{\theta}\, p^{nk}}{\sum_{t=0}^{\infty} \delta_{t,k} \, \left(p^n/\overline{\theta}\right)^t} = \bar{\theta}^{k+1} \tag{31}$$

where we have used (29), and where where $\delta_{t,k}$ is the Kroneker delta function. Thus $\Delta_k = \bar{\theta}^{k+1}$, independent of C, which does not converge, because $\bar{\theta}$ is a non-trivial unit. $\square$

Proposition 5.1 establishes a one-to-one correspondence between periodic codes and periodic orbits, while the metric-preserving property of $\mathcal{C}$ show that the periodic orbits are dense and uniform (with respect to the Haar measure). They are all unstable, with multiplier p^{-nT} (T is the period).

The coding function $\mathcal{C}$ satisfies the scaling property

$$\mathcal{C}(p^{ns}\chi) = p^{ns}\mathcal{C}(\chi\overline{\theta}^s) \qquad s \geq 0, \quad n \geq 1$$

which holds for every p-adic integer χ. This result, which is an immediate consequence of formula (28), allows one to confine the study of the dynamics to the annulus $|\chi|_p > p^{-n}$, corresponding to initial condition not belonging to any of the lattices $\mathcal{M}_k$. For $n = 1$, this is the p-adic unit circle (the p-adic units).

Our last result characterizes the periodic points arithmetically.

Proposition 5.2 *The periodic point χ corresponding to the T-periodic code $C = (\overline{c_0, \ldots, c_{T-1}})$ takes the form*

$$\chi = \frac{1}{m(T)} \left(x - \frac{\theta}{p^n}\, y\right) \tag{32}$$

where x and y are integers given by

$$x = \sum_{r=0}^{T-1} c_r\, U_{T,\,r} \qquad y = \sum_{r=0}^{T-1} c_r\, U_{T,\,r+1} \qquad U_{T,\,r} = p^{nr} a_{T-r} + p^{n(T-r)} a_r; \tag{33}$$

while

$$m(T) = a_T q + 2p^n b_T - 2p^{nT} \tag{34}$$

is an integer coprime to p.

The above result shows that the T-periodic orbits belong to the module $\mathcal{Z}/m(T)$. Those corresponding to orbits of the round-off mapping Φ must lie in the sub-module $\mathcal{Z}$, which is the case when x and y are divisible by $m(T)$.

The domain of definition of $\mathcal{L}$ can be extended to rational pairs $(r,\, s)$, with denominators coprime to p, over which $\mathcal{L}$ remains invertible. The round-off mapping Φ is then extended to such set as the conjugate $\hat{\Phi}$ of Φ^* under $\mathcal{L}^{-1}$, and since $m(T)$ is coprime to p, all the p-adic periodic orbits can be lifted to the plane.

The embedding map $\hat{\Phi}$ is best described by writing the perturbing function as

$$\left\lfloor \frac{q}{p^n} r \right\rfloor = \frac{q}{p^n} r - \frac{qr \,(\mathrm{mod}\; p^n)}{p^n}$$

and noting that in the above formula one only requires that r have a modular inverse modulo p^n. So this formula remains meaningful when the denominator of r is coprime to p. Thus $\hat{\Phi}$ can still be described as a perturbed planar rotation, although the perturbation (which is now everywhere discontinuous) can no longer be interpreted as the result of round-off.

Proof: From the representation (29), and the periodicity of the code $c_{k+T} = c_k$, we obtain

$$\chi = \frac{1}{\bar{\theta}} \sum_{k=0}^{\infty} c_k \left(\frac{p^n}{\bar{\theta}}\right)^k = \frac{1}{\bar{\theta}} \sum_{r=0}^{T-1} c_r \left(\frac{p^n}{\bar{\theta}}\right)^r \sum_{s=0}^{\infty} \left(\frac{p^n}{\bar{\theta}}\right)^{Ts} = \frac{\beta}{\bar{\theta}^T - p^{nT}} \tag{35}$$

where

$$\beta \;=\; \beta(C) \;=\; \sum_{r=0}^{T-1} c_r\, p^{nr}\, \bar{\theta}^{\,T-r-1} \;=\; \sum_{r=0}^{T-1} c_r\, p^{nr} (a_{T-r} - \theta a_{T-r-1})$$

is a p-adic integer. The rightmost sum was derived using the local version of formula (25) (which is valid since $\mathcal{L}_2$ is a ring homomorphism) and defining $a_0 = 0$. Multiplying the numerator and denominator of (35) by $p^{nT} - \theta^T$, we obtain

$$\chi = \frac{1}{m(T)}\,\frac{(p^{nT}-\theta^T)\,\beta}{p^{nT}}; \qquad m(T) = \frac{-1}{p^{nT}}\,N(\lambda^T - p^{nT}) = a_T q + 2p^n b_T - 2p^{nT} \tag{36}$$

where N denotes the norm (the product of algebraic conjugates). The integer $m(T)$ is coprime to p, because so are a_T and q.

With reference to (32), (35) and (36) we write

$$(p^{nT}-\theta^T)\,\beta = A + \theta\,B$$

and we must now show that A is divisible by p^{nT}, and B by $p^{n(T-1)}$. One finds

$$\begin{aligned} A &= \sum_{r=0}^{T-1} c_r p^{nr}\Big[p^{nT}\,a_{T-r} - p^n(b_T a_{T-r} - a_T b_{T-r})\Big] \\ B &= \sum_{r=0}^{T-1} c_r p^{nr}\Big[p^{n(T-1)}\,b_{T-r} - p^n(a_T b_{T-r-1} - b_T b_{T-r-1})\Big] \end{aligned}$$

From the identity

$$a_{i+1}b_{j+1} - b_{i+1}a_{j+1} = p^{2n}(a_i b_j - b_i a_j) \qquad\qquad i,j \geq 1$$

we have $a_T b_k - b_T a_k = p^{n(2k-1)} a_{T-k}$, which, together with the identity $-p^{nr} b_{T-r} = p^{n(r+1)} a_{T-r-1}$ (see (8)) yields

$$\begin{aligned} A &= p^{nT}\sum_{r=0}^{T-1} c_r\,(p^{nr}a_{T-r} + p^{n(T-r)}a_r) \\ B &= -p^{n(T-1)}\sum_{r=0}^{T-1} c_r\,(p^{n(r+1)}a_{T-r-1} + p^{n(T-r-1)}a_{r+1}) \end{aligned}$$

and (33) follows.

$\square$

6 Concluding remarks

The question of the non-existence of unbounded orbits of the mapping Φ is one of the most significant open problems. The conjecture that the system is globally periodic is supported by extensive numerical evidence [30]. However, no proof of global stability is known to the authors for any invertible model of linear irrational rotations.

Stability proofs for planar rotations have been produced for *non-invertible* discretizations of irrational rotations, for one case of invertible discretization of *rational* rotation [21], and finally for invertible discretizations of twist mappings [8].

The completeness of the code yields the full set of periodic points, as p-adic integer χ of the form (32). The difficulties in the study of the periodic orbits of the round-off map Φ are centered around the problem of deciding whether or not such χ belongs to the submodule $\mathcal{Z}$ of $\mathbb{Z}_p$, which is the case when x and y are divisible by $m(T)$. This divisibility question is delicate, and will be dealt with elsewhere. Structurally similar problems arise in the archimedean case, for Bernoulli shifts and hyperbolic toral automorphisms, where the lattices containing all orbits of a given period are easily determined, but one does not know a priori whether a given sublattice contains any. This class of problems are associated to the emergence of non-polynomial time algorithms, and of statistical behaviour in discrete and quantum systems (see [9] and references therein).

Nevertheless, the expansive property of the embedding system justifies intuitively the observed statistical properties of the round-off errors, and one would expect the accumulation of such errors to give rise to a gaussian process. To this extent we note that a recent result of Vladimirov [28], who proved a central limit theorem for round-off errors in linear systems. Our model however, is not directly applicable to that case, since the system (1) has rational entries.

References

[1] S. Albeverio, A. Khrennikov, B. Tirozzi and D De Smedt, p-adic dynamical systems, *Theoretical and Mathematical Physics*, **114**, (1998), 276–287.

[2] D. K. Arrowsmith and F. Vivaldi, Some p-adic representations of the Smale horseshoe, *Phys. Lett. A* **176** (1993) 292–294.

[3] D. K. Arrowsmith and F. Vivaldi, Geometry of p-adic Siegel discs, *Physica D* **71** (1994) 222–236.

[4] R. Benedetto, Fatou components in p-adic dynamics, PhD Thesis, Brown University (1998).

[5] R. Benedetto, p-adic dynamics and Sullivan's No Wandering Domain Theorem, (1998) *Composition Mathematica* at press.

[6] R. Benedetto, Hyperbolic maps in p-adic dynamics, preprint, University of Rochester, (1998) *Ergodic Theory and Dynamical Systems* at press.

[7] M. Blank, Pathologies generated by round-off in dynamical systems, *Physica D* **78** (1994) 93–114.

[8] M. Blank, T. Krüger and L. Pustylnikov, A KAM type theorem for systems with round-off errors, preprint (1997).

[9] B.V. Chirikov and F. Vivaldi, An algorithmic view of pseudochaos, *Physica D* **129** (1999) 223–235.

[10] P. Diamond, P. Kloeden, V. Kozyakin and A. Pokrovskii, Boundedness and dissipativity of truncated rotations on uniform planar lattices, Preprint TR M95/06, School of Computing and Mathematics, Deaking University, Geelong, Vic., Australia (1995).

[11] H. Cohn, *A second course in number theory*, John Wiley & Sons, New York (1962). (Reprinted as *Advanced number theory*, Dover, New York (1980).)

[12] H. Cohn, *Introduction to the construction of class fields*, Cambridge University Press, New York (1985).

[13] H. Hasse, *Number theory*, Springer-Verlag, Berlin (1980).

[14] M. R. Herman and J-C. Yoccoz, Generalization of some theorem of small divisors to non-archimedean fields, *Geometric Dynamics,* LNM 1007, Springer-Verlag, New York, (1983), 408–447.

[15] L. Hsia, A weak Néron model with applications to p-adic dynamical systems, *Compositio Math.* **100**, (1996) 277–304.

[16] L. Hsia, Closure of periodic points over a non-archimedean field, preprint, Department of Mathematics, National Central University, Taiwan (1999) (e-mail: `hsia@math.ncu.edu.tw`).

[17] V. Kozyakin, On finiteness of trajectories for one mapping associated with quasi-inversion of rotation mapping on integer planar lattice, Proceedings of the 15th IMACS World Congress on Scientific Computation, Modelling and Applied Mathematics, August 24-29, 1997, Berlin, Germany, Volume I: Computational Mathematics, Wissenschaft und Technik Verlag, Berlin, (1997). 39–44.

[18] H-C. Li, p-adic dynamical systems and formal groups, *Compositio Mathematica* **104** (1996) 41–54.

[19] H-C. Li, p-adic periodic points and Sen's theorem, *J. Number Theory* **56** (1996) 309–318.

[20] J. H. Lowenstein, S. Hatjispyros and F. Vivaldi, Quasi-periodicity, global stability and scaling in a model of Hamiltonian round-off, *Chaos* **7** (1997) 49–66.

[21] J. H. Lowenstein, and F. Vivaldi, Anomalous transport in a model of Hamiltonian round-off, *Nonlinearity* **5** (1998) 1321–1350.

[22] J. Lubin, Non-archimedean dynamical systems, *Comp. Maths.* **94** (1994) 321–346.

[23] D. A. Marcus, *Number fields,* Springer-Verlag, New York (1977).

[24] W. Narkiewicz, Polynomial cycles in algebraic number fields, *Coll. Math.* **58** (1989) 151–155.

[25] T. Pezda, Polynomial cycles in certain local domains, *Acta Arith.* **LXVI** (1994) 11–22.

[26] J-P. Serre, *A course in arithmetic,* Springer-Verlag, New York (1973).

[27] E. Thiran, D. Verstegen, and J. Weyers, p-adic dynamics, *J. Stat. Phys.* **54** (1989) 893–913.

[28] I. Vladimirov, Quantized linear systems on integer lattices: frequency-based approach I & II, preprint, Deakin University, Geelong, Victoria. (1996).

[29] F. Vivaldi, Dynamics over irreducible polynomials, *Nonlinearity* **5** (1992) 941–960.

[30] F. Vivaldi, Periodicity and transport from round-off errors, *Experimental Mathematics* **3** (1994) 303–315.

[31] C. Woodcock and N. Smart, p-adic chaos and random number generation, *Experimental Mathematics* **7** (1998) 333–342.

[32] M. E. Zieve, Cycles of Polynomial Mappings, Ph.D. thesis, University of California at Berkeley, (1996).