Complexity of regular invertible p-adic motions

J Pettigrew[1], J A G Roberts[1,2] and F Vivaldi[3]

[1] *Department of Mathematics, La Trobe University, VIC 3086, Australia*
[2] *School of Mathematics, University of New South Wales,*
Sydney NSW 2052, Australia (after July 2001)
[3] *School of Mathematical Sciences, Queen Mary, University of London,*
London E1 4NS, UK

Abstract

We consider issues of computational complexity that arise in the study of quasi-periodic motions (Siegel discs) over the p-adic integers, where p is a prime number. These systems generate regular invertible dynamics over the integers modulo p^k, for all k, and the main questions concern the computation of periods and orbit structure. For a specific family of polynomial maps, we identify conditions under which the cycle structure is determined solely by the number of Siegel discs and two integer parameters for each disc. We conjecture the minimal parametrization needed to achieve — for every odd prime p — a two-disc tessellation with maximal cycle length. We discuss the relevance of Cebotarev's density theorem to the probabilistic description of these dynamical systems.

We characterize regular motions in invertible dynamical systems over a finite phase space, using arithmetical techniques. Regularity is identified with the possibility to decide whether or not two points belong to the same orbit, more efficiently than via direct iteration. For a very simple class of models — one-dimensional linear systems over modular integers — this decision problem is equivalent to the computation of a suitable logarithmic function, which is feasible in polynomial time when the modulus is a large power of a prime number. Under these circumstances, the addition of nonlinearity does not increase the complexity of the motions, affording a full characterization of the orbital structure. By contrast, the fluctuations that derive from changing the underlying prime number are quite unpredictable, and subject to probabilistic laws.

1 Introduction

In this paper we investigate the structure of regular motions for a class of invertible maps on a finite phase space, with emphasis on the realizability of various cycle lengths, and related issues of computational complexity. Unlike for dynamics on manifolds, where 'regular' usually denotes zero metric entropy, on a finite space the situation is less clear. For instance, the character of the motion may depend on the choice of the topology.

Let f be an invertible map on a finite phase space Ω, and let $x, y \in \Omega$. Does y belong to the orbit of x? If so, what is the transit time from x to y, using the dynamics? These questions can be answered by direct iteration, but as the size of the system becomes large, the quest for non-trivial answers becomes compelling, since these determine our ability to predict. (We exclude from consideration *random* maps, that is, maps defined by a table of values, for which direct iteration is the only available option.)

Thus, for all $x, y \in \Omega$, we define the *transit time*

$$\mathcal{T}(x,y) = \begin{cases} \min\limits_{t>0} \{t \mid f^t(x) = y\} & \text{if such } t \text{ exists} \\ \infty & \text{otherwise.} \end{cases}$$

Writing $\mathcal{T}(x)$ for $\mathcal{T}(x,x)$, we have that $\mathcal{T}(x)$ — the *period function* — is the period of the orbit through x (because t is positive). We call the motions 'regular' if, for all x and y, $\mathcal{T}(x,y)$ can be computed in polynomial time in the input size $\log(N)$, where N is the cardinality of Ω. Clearly, it is not possible to prove that a system is *not* regular.

An invertible map is necessarily regular in the above sense when all its cycles are logarithmically short; therefore obstructions to predictability can only originate from the existence of long cycles, although this is by no means sufficient. (Of note is the fact that for random permutations of N elements, the expected maximal cycle length is of order N [32].) The literature abounds with instances of discrete invertible maps with long and seemingly unpredictable cycle lengths (see [29, 17, 33, 35, 11], for a selected sample).

The subtlety of this problem is already manifest in linear modular dynamics (discrete Bernoulli shift) $x \mapsto \omega x \pmod{N}$, where $\omega > 1$ is an integer, and the phase space is the lattice $\mathbf{Z}/N\mathbf{Z}$ of integers modulo N. The transit time $\mathcal{T}(x,y)$ is now the smallest positive t for which $\omega^t x \equiv y \pmod{N}$, given by the formal expression

$$\mathcal{T}(x,y) = \frac{\log(y/x)}{\log(\omega)} \tag{1}$$

involving a yet unspecified logarithmic function.

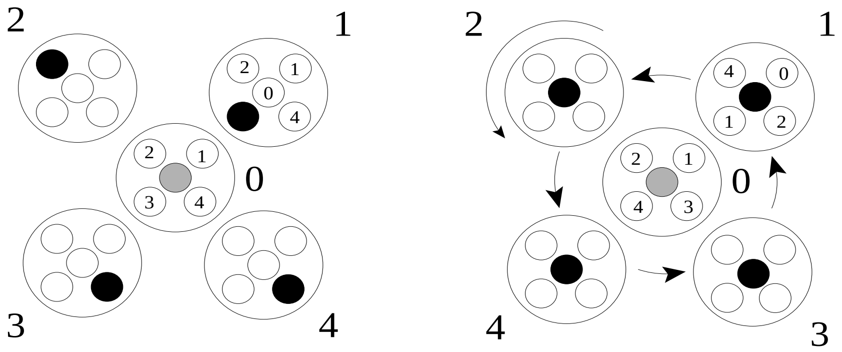

Figure 1: An approximate representation of $\mathbf{Z}_5$, with 2-digit accuracy (the first two digits in (2)). Left: the mapping $F(x) = 2x + (x^5 - x)(x + 2x^2)$ has a fixed point at 0 (grey), and the approximate 4-cycle (black) $(16, 12, 24, 23) \equiv (1, 2, 4, 3) \pmod{5}$. Right: by rearranging the p-adic points, the phase portrait reveals a 2-disc system, with the secondary disc centred on the 4-cycle. This configuration is the p-adic analogue of an integrable nonlinear resonance.

If $N = p$ is a prime number, 'log' is the *discrete logarithm* modulo p; at present, it cannot be computed in polynomial time, which accounts for its importance in cryptography [19]. However, if $N = p^n$ is a large power of a prime p, then 'log' is (essentially) the p-adic logarithmic function, which can be computed in polynomial time, thanks to its analyticity. This peculiar phenomenon originates from an embedding of the phase space with p^n points into the p-adic integers, where the dynamics becomes quasi-periodic rotation on a disc, a system with zero entropy (section 2).

We recall that the ring of p-adic integers consists of expressions of the type (see, e.g., [13])

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

which converge with respect to the non-archimedean absolute value $|\cdot|_p$, defined as $|\xi|_p = p^{-k}$, where b_k is the first nonzero coefficient in the expansion (2). (The non-archimedean property is expressed by the strong triangle inequality: $|x + y|_p \leq \max(|x|_p, |y|_p)$.) The resulting topology organizes the elements of $\mathbf{Z}_p$ hierarchically, making it into a Cantor set. It is customary to write $v(\xi) = k$, and express the size of ξ in terms of the *valuation* v, instead of $|\cdot|_p$.

The study of dynamical systems over the p-adics defines a lively and varied area of investigation (see [22, 20, 16, 5, 1, 7], and references therein). In the p-adic context, a discrete phase space $\mathcal{L}_n = \mathbf{Z}/p^n\mathbf{Z}$, is a coarsened representation of $\mathbf{Z}_p$, with n digit accuracy, with an induced coarsened dynamics (figure 1). In this paper we shall be interested in the case in which such dynamics is analytic, invertible on each $\mathcal{L}_n$, and regular. For these, non-polynomial time problems originate only from computation modulo p, whereas the dynamics modulo p^n will feature the tight hierarchical organization often found in p-adic constructs.

Regular invertible motion over the p-adics is a simplified version of its complex counterpart, which is — up to analytic conjugacy — rotation on Siegel discs (figure 1). If the multiplier ω of the mapping $f(x) = \omega x + O(x^2)$ lies on the unit circle ($|\omega|_p = 1$) and is not a root of unity, then it is possible to construct a conjugacy ϕ of f to its linear part

$$\phi(f(x)) = \omega\, \phi(x), \tag{3}$$

which is defined with its inverse in a neighbourhood of the origin. This construction is made easier by the tame nature of small denominators (the roots of unity accumulate nowhere) [15, 3, 22, 21].

Combining the linearization (3) with Hensel's lemma, one can gain considerable knowledge on the orbit structure of an invertible polynomial map on $\mathcal{L}_n$, from cycles and multiplier data computed modulo p. Hensel's lemma provides conditions under which a cycle modulo p persists modulo p^n for all n (it *lifts,* in jargon, see [13] chapter 3, and section 3 below). These p-adic cycles are then used as the skeleton for the construction of discs, which afford polynomial-time computation of transit times.

However, for a given map, the structure of cycles and multipliers modulo p depends in a very erratic way on the prime considered. Such unpredictability is rooted in the properties of factorization of polynomials over finite fields, which is again a non-polynomial time problem ([9], chapter 3). The asymptotics of this phenomenon is controlled by a probabilistic law, the Cebotarev density theorem, which determines the probability of the existence of cycles of a given length, modulo p, averaged over all primes p ([12], page 129, and section 5 below).

In this paper we deal with a specific family of maps, that afford an adequate degree of control as p varies. We begin to note that if $f(x)$ is invertible with non-vanishing derivative modulo p, then it is invertible on each $\mathcal{L}_n$ (lemma 3.1). By the chain rule of differentiation, the non-vanishing of the derivative modulo p also implies that the multiplier λ of any cycle of $f(x)$ lies on the p-adic unit circle, which is a necessary condition for the existence of discs. With these considerations in mind, we introduce the following family of maps

$$F : \mathbf{Z}_p \to \mathbf{Z}_p \qquad\qquad F(x) = \omega x + (x^p - x)\, h(x) \qquad |\omega|_p = 1 \tag{4}$$

where $h(x)$ is a polynomial over $\mathbf{Z}_p$.

In section 2 we compute the linear transit time (proposition 2.1), and determine sufficient conditions on the multiplier, for the occurrence of a maximal Siegel disc (proposition 2.2). In section 3, we discuss the phenomenon of lifting of periodic orbits, and the occurrence of a full tessellation of $\mathbf{Z}_p$ into discs (proposition 3.2). This affords a polynomial-time computation of the transit function.

We apply the above results to the family (4), requiring that it be invertible, and that it feature, besides the fixed point at the origin, a cycle of maximal period on the unit circle, surrounded by a disc of maximal size[1]. Using resultants, we translate these requirements into conditions on the auxiliary polynomial $H(x) = \omega - h(x)$, prompting the study of the polynomials of minimal degree that achieve maximal periods. Based on experimental evidence, we conjecture that maximal period for all primes can be achieved with quadratic polynomials $H(x)$, while with a cubic polynomials one can also satisfy certain congruence conditions on multipliers (section 4). Finally, in section 5, we discuss the relevance of Cebotarev's density theorem to the probability of occurrence of maximal periods.

Although in this paper — for the sake of concreteness — we mainly deal with a specific model, many of our constructs are easily generalized. For instance, replacing $\mathbf{Z}_p$ with one of its unramified extensions, and the finite field $\mathbf{Z}/p\mathbf{Z}$ with the corresponding finite field extension, the mappings (4) become

$$F(x) = \omega x + (x^q - x)h(x) \qquad q = p^k,$$

where k is the degree of the extension. Most of our results extend to this case with little or no modification.

Acknowledgments. FV gratefully aknowledges the hospitality of the Mathematics Department at La Trobe University, where much of this research was carried out, with support from the Australian Research Council. JP acknowledges support from a La Trobe University Postgraduate Fellowship.

2 p-adic discs

In what follows, p is an odd prime.

A disc in canonical form features in a linear map $f(x) = \omega\, x$, with multiplier $\omega \in \mathbf{Z}_p$ on the unit circle: $|\omega|_p = 1$. Arithmetically, this multiplier is a *unit,* that is, an invertible element of $\mathbf{Z}_p$. The map f is invertible on each $\mathcal{L}_n$, and its cycle structure is characterized by writing

$$\omega^T = 1 + p^s\beta; \qquad T = \frac{p-1}{m} \qquad |\beta|_p = 1 \tag{5}$$

and T is the multiplicative order of ω modulo p, i.e.,

$$\omega^t \not\equiv 1 \pmod{p} \qquad 1 \leq t < T,$$

---

[1] A 'perturbative' model $f(x) = \omega\, x + p^s\, h(x)$, could not achieve such configuration, because, for any choice of $h(x)$, the cycle on the unit circle has one-unit multiplier, see section 2.

(whence m divides $p-1$), and $s = s(\omega^T) = v(\omega^T - 1) \geq 1$. The quantity ω^T is an example of *one-unit,* that is, a p-adic number congruent to 1 modulo p. The parameter s is the *level* of the one-unit. When $m = 1$, we say that ω is *primitive;* if, in addition, $s = 1$, we say that ω is *maximal.* Primitive and maximal multipliers generate the invertible elements modulo p and p^2, respectively.

If $a \in \mathbf{Z}_p$ has order $T(a) = p-1$, then for any unit z, the congruence $a^t \equiv z \pmod{p}$, can be solved for $t := \log_a(z)$; this is the *discrete logarithm* to the base a, which is determined modulo $p-1$. It can be shown that

$$T(\omega) = \frac{p-1}{\gcd(\log(\omega), p-1)} \tag{6}$$

where the logarithm is computed with respect to an arbitrary base.

The *p-adic logarithm* is defined via the usual power series

$$\ln(1+z) = \sum_{k\geq 1} \frac{(-1)^{k+1} z^k}{k} \qquad |z|_p < 1; \tag{7}$$

its domain of definition is the one-units.

Proposition 2.1 *Let p be an odd prime, and let ω be a unit in $\mathbf{Z}_p$. Then, for all $n \geq 1$, the map $x \mapsto \omega x \pmod{p^n}$ has period function*

$$\mathcal{T}(x) = \begin{cases} 1 & n \leq v(x) \\ T & n - s \leq v(x) < n \\ T p^{n - v(x) - s} & 0 \leq v(x) < n - s, \end{cases} \tag{8}$$

where T and s are the parameters of ω. Furthermore, for $x \not\equiv y \pmod{p^n}$, let $x' = \omega^{\mathcal{T}_0} x$, where $\mathcal{T}_0$ is the smallest non-negative integer such that $x' \equiv y \pmod{p}$. If any of the conditions

$$(i) \quad |x/y|_p = 1; \qquad (ii) \quad \frac{\log(y/x)}{\gcd(\log(\omega), p-1)} \in \mathbf{Z}; \qquad (iii) \quad s(y/x') \geq s(\omega^T) \tag{9}$$

is violated, we have $\mathcal{T}(x,y) = \infty$. Otherwise

$$\mathcal{T}(x,y) = \mathcal{T}_0(x,y) + T(\omega) \cdot \mathcal{T}_1(x', y) \tag{10}$$

where

$$\begin{aligned} \mathcal{T}_0(x,y) &\equiv \frac{\log(y/x)}{\log(\omega)} \pmod{p-1} \\ \mathcal{T}_1(x',y) &\equiv \frac{\ln(y/x')}{\ln(\omega^T)} \pmod{p^{n-1-v(x)}} \end{aligned} \tag{11}$$

and $\mathcal{T}_0$ and $\mathcal{T}_1$ are the least non-negative residues for the respective moduli.

The complexity of formula (10) is buried in the computation of $\mathcal{T}_0$ and T, which is non-polynomial in $\log(p)$; when computing modulo p^n, this difficulty fades away as n becomes large, since the number of terms needed in the expansion of the p-adic logarithm is $O(n)$, from (11).

The periodicities of the reduced systems $\mathcal{L}_n$ are uniquely determined by the multiplier's parameters T and s. Specifically, the invariant circle $v(x) = k$ decomposes into $m = (p-1)/T$ orbits, with common period $\mathcal{T}(x)$. The longest cycles lie on the unit circle ($v(x) = 0$), with maximal period occurring when ω is maximal, when the p-adic orbit through x_0 fills densely the circle $|x| = |x_0|$. If the multiplier is not maximal, then every circle decomposes into (the closure of) finitely many orbits.

Proof. Formula (8) follows readily from the estimate of recurrence distance

$$\omega^{Tp^i} x - x = x\, \left(p^{s+i}\beta + O(p^{2s+i})\right) .$$

Now, if $(9\,i)$ is false, then x and y belong to different circles, so $\mathcal{T}(x,y) = \infty$. If $(9\,i)$ is true, but $(9\,ii)$ is false, then x and y belong to the same circle, but are on different orbits, so the transit time is again infinite. Finally, if $(9\,i)$ and $(9\,ii)$ are true, then the multivaluedness of the discrete logarithm can be used to make $\mathcal{T}_0$ nonnegative, integral and minimal. Furthermore, y/x' and $\eta = \omega^T$ are one-units. If condition (iii) is false, then the equation $\eta^\theta = y/x'$ has no solution $\theta \in \mathbf{Z}_p$ (i.e., y/x' does not belong to the $\mathbf{Z}_p$-module generated by η), whence $T(x,y) = \infty$.

Assume now that all conditions (9) are true. Then all logarithms are defined, whence, with reference to equation (10) we have, in $\mathbf{Z}_p$

$$\omega^{\mathcal{T}} x = \eta^{\mathcal{T}_1} \omega^{\mathcal{T}_0} x = \eta^{\mathcal{T}_1} x' = y.$$

Finally, the moduli in (11) are determined by the fact that the original congruence $\omega^{\mathcal{T}} x \equiv y \,(\mathrm{mod}\; p^n)$, upon division by $p^{v(x)}$, becomes a congruence involving units modulo $p^{n-v(x)}$, which are the direct product of two cyclic groups of order $p-1$, and $p^{n-v(x)-1}$, respectively. $\square$

Suppose now $f(x) = \omega x + O(x^2)$ has coefficients in $\mathbf{Z}_p$, then we have $|O(x)|_p \leq |x|_p$, and since $|\omega|_p = 1$, we find

$$|f(x)|_p = |x|_p |\omega + O(x)|_p = |x|_p \qquad |x|_p < 1, \tag{12}$$

that is, all circles of radius less than unity are invariant under f. So, *if* the circle $|x|_p = r$ belongs to the Siegel disc, its period on $\mathcal{L}_n$ can be computed from that of the linear map (equation (8)). It is therefore important to estimate the size of the disc. We do this with the benefit of the following theorem.

Theorem 1 *cf.* ([21], theorem 3.1) *Let $f(x) = \omega x + O(x^2)$ be a power series with coefficients in $\mathbf{Z}_p$, with p odd, and T and $s < \infty$ given by (5). Then $f(x)$ is semi-conjugate to its linear part, i.e., it satisfies (3) for ϕ defined in the domain*

$$v(x) > \frac{1}{T}\left(s + \frac{1}{p-1}\right).$$

We call the region of semi-conjugacy a *semi-disc,* whereas the term disc will refer to the full conjugacy. Because $\phi'(0) \neq 0$, the disc has non-zero radius (theorem 27.5 of [30]), but disc and semi-disc do not necessarily coincide, as in the case of endomorphisms of formal groups, where ϕ vanishes within the semi-disc [3]. Note that the condition $s < kT$, is equivalent to the statement that the semi-disc (3) contains the closed disc $|x|_p \leq p^{-k}$. In particular, when $s < T$, the semi-disc includes the *maximal ideal* $\{x : v(x) \geq 1\}$.

The main unresolved issue concerns the radius of the disc. We address it in the limited context of maximal multipliers.

Proposition 2.2 *For odd p, let $f(x) = \omega x + O(x^2)$ be a power series over $\mathbf{Z}_p$, with maximal multiplier ω. Then the Siegel disc includes the closed disc $p\mathbf{Z}_p$, and this conjugacy restricts to a conjugacy modulo p^n, for all positive n.*

Proof. From theorem 1, with $T = p - 1$, $s = 1$, and $p > 2$, we have that the semi-disc contains the region $v(x) \geq 1$. We choose the conjugacy function so that $\phi'(0) = 1$, or

$$\phi(x) = x\,(1 + c_2x + c_3x^2 + c_4x^3 + \cdots). \tag{13}$$

The recursion relation for the coefficients has the form

$$c_1 = 1; \qquad \omega(\omega^{k-1} - 1)c_k = \sum_{t=1}^{k-1} c_tL_t, \qquad k > 1$$

where L_t is a polynomial in ω with coefficients in $\mathbf{Z}_p$. It follows that, for $k \geq 2$, the coefficient c_k is the ratio of a p-adic integer, and the "small denominator" $D_k = \prod_{t=1}^{k-1}(\omega^t - 1)$ [3, 21]. For $v(x) \geq 1$, and recalling that $v(xy) = v(x) + v(y)$, we find

$$\begin{aligned} v(c_kx^{k-1}) &= v(c_k) + (k-1)v(x) \geq -v(D_k) + k - 1 \\ &= k - 1 - \sum_{t=1}^{k-1} v(\omega^t - 1). \end{aligned}$$

Defining

$$N = \left\lfloor \frac{k-1}{p-1} \right\rfloor \qquad \eta = \omega^{p-1}$$

we find (cf. equation (5))

$$\begin{aligned}\sum_{t=1}^{k-1} v(\omega^t - 1) &= \sum_{t=1}^{N} v(\eta^t - 1) = \sum_{t=1}^{N} \left[v(p) + v\left(\frac{\eta^t - 1}{p}\right)\right] \\ &= N + \sum_{t=1}^{\infty} \left\lfloor \frac{N}{p^t} \right\rfloor \leq N + \sum_{t=1}^{\infty} \frac{N}{p^t} \\ &= N \frac{p}{p-1}.\end{aligned}$$

We obtain

$$v(c_k x^{k-1}) \geq k - 1 - \left\lfloor \frac{k-1}{p-1} \right\rfloor \frac{p}{p-1} \qquad k \geq 1. \tag{14}$$

Now for $v(x) \geq 1$ and $k \geq 2$, the above gives $v(c_k x^{k-1}) \geq 1$. Furthermore, equation (13) gives

$$\phi(x) - \phi(y) = (x - y) \left[1 + \sum_{k \geq 2} c_k \, Q_k(x, y) \right] \qquad Q_k(x, y) = \sum_{l=0}^{k-1} x^l y^{k-l-1}$$

where $v(Q_k(x, y)) \geq (k - 1) \cdot \min(v(x), v(y))$. Therefore, if $v(x), v(y) \geq 1$ and $k \geq 2$, then $v(c_k \, Q_k(x, y)) \geq 1$, whence $|\phi(x) - \phi(y)|_p = |x - y|_p$, i.e., on $p\mathbf{Z}_p$, ϕ is an isometry which leaves every circle $v(x) = const.$ invariant. In particular, ϕ is injective on $p\mathbf{Z}_p$, whence invertible. The same is clearly true on each finite set $\mathcal{L}_n$, where ϕ acts as a permutation of each finite circle. $\square$

We remark that using the procedure developed in [3], one can also construct a weaker (topological) conjugacy between f^T and any linear map $x \mapsto \overline{\omega}^T x$, where the multiplier $\overline{\omega}$ is a unit with the same parameters as ω. Such conjugacy, which exists by virtue of the fact that the two systems have the same period structure on each $\mathcal{L}_n$, is C^∞, except possibly, at the origin, where it is only continuous. If the multipliers coincide, then the conjugacy becomes differentiable at the origin, with unit derivative.

As an example of failure of conjugacy in polynomial maps of the form (4), let $F(x) = 8x + (x^3 - x)x^2$; we have $T = 2$, and $s = 2$, whence $v(r) = 5/4 > 1$. The circle $v(x) = 1$ lies outside the semi-disc; one verifies that for $k \geq 4$, the cycle lengths of $F(x)$ and its linearization differ modulo 3^k.

3 Lifting

The construction of p-adic periodic points rests on Hensel's lemma, which, in the formulation relevant to us, states that if $f(x)$ is a polynomial over $\mathbf{Z}_p$ with a root

a modulo p, and if $f'(a) \not\equiv 0 \,(\mathrm{mod}\ p)$, then $f(x)$ has a root $\alpha \in \mathbf{Z}_p$, such that $\alpha \equiv a \,(\mathrm{mod}\ p)$. The condition $f'(a) \not\equiv 0 \,(\mathrm{mod}\ p)$ may be replaced with the weaker $|f(a)|_p < |f'(a)|_p^2$ ([13], section 3.4).

The periodic points of essential period T of a polynomial $f(x)$ are the roots of the polynomial [34, 6, 25, 26]

$$\Phi_T(x) = \prod_{d|T} \left(f^d(x) - x \right)^{\mu(T/d)} \tag{15}$$

where μ is the Möbius function ([2], chapter 2). (Essential period is minimal period, except, possibly, at bifurcation [27].) If $\Phi_T(x)$ has a root a modulo p, then, by Hensel's lemma, it also has a T-cycle containing $\alpha = a + O(p) \in \mathbf{Z}_p$, provided that $\Phi_T'(a) \not\equiv 0 \,(\mathrm{mod}\ p)$. The vanishing of the derivative signals the fact that a is p-adically close to a bifurcational state, in which case the lifting of the cycle modulo p may or may not take place, and the period may differ from the minimal period. We define the multiplier $\lambda(x)$ of a (not necessarily minimal) T-cycle at x, as

$$\lambda(x) = \left(f^T\right)'(x) = \prod_{t=0}^{T-1} f'(f^t(x)). \tag{16}$$

If $\Phi_T(x)$ has a multiple root at a, then $\lambda(a) = 1$, since the bifurcation involves a collision of orbits of period dividing T [27]. Thus a *sufficient* condition for a T-cycle containing $x \equiv a \,(\mathrm{mod}\ p)$ to lift, is that $\lambda(a) \not\equiv 1 \,(\mathrm{mod}\ p)$, that is, that λ is not a *one-unit*. The lifted T-cycle $\alpha = a + O(p) \in \mathbf{Z}_p$, may be computed via the p-adic Newton's iteration

$$x \mapsto x - \frac{\Phi_T(x)}{\Phi_T'(x)}. \tag{17}$$

with initial conditions $x = a$, which, like its archimedean counterpart, is superconvergent ([31], section 2.2). Formula (17) is useful for computation only when T is small. For large T or p, the recursive solution of $f^T(x) \equiv x \,(\mathrm{mod}\ p^k)$ is more effective.

Our next result provides sufficient conditions, which can be tested modulo p, for $f(x)$ to be a permutation modulo p^n for all n.

Lemma 3.1 *Let $f(x)$ be a power series over $\mathbf{Z}_p$ which is a permutation modulo p, and let $f'(x)$ have no roots modulo p. Then $f(x)$ is a permutation modulo p^n, for all $n \geq 1$.*

Proof. Suppose not. Then there exist $a, b \in \mathbf{Z}_p$ and $n \in \mathbf{N}$ such that $a \not\equiv b \,(\mathrm{mod}\ p^n)$ and $f(a) \equiv f(b) \,(\mathrm{mod}\ p^n)$. As the latter property implies that $f(a) \equiv$

$f(b) \pmod{p}$, we must have $a \equiv b \pmod{p}$, lest $f(x)$ would not be a permutation modulo p. Thus $|a-b|_p = p^{-k}$ for some k with $1 \le k < n$. But then

$$f(a) - f(b) = f'(b)(a-b) + O((a-b)^2) = (a-b)(f'(b) + O(a-b))$$

giving

$$\frac{1}{p^k} = |f(a) - f(b)|_p \le \frac{1}{p^n}$$

which is impossible, since $k < n$. □

From this result, proposition 2.2, and the previous considerations on lifting, we have

Proposition 3.2 *Let $f(x)$ be a power series with coefficients in $\mathbf{Z}_p$, which restricts to a permutation modulo p, with maximal multipliers. Then $\mathbf{Z}_p$ decomposes into p Siegel discs of radius $1/p$.*

For these systems, knowledge of the basic cycles, and of the conjugacy function ϕ, translates into polynomial-time computation of the entire phase space structure. Note that the number of terms needed to evaluate ϕ_n is $O(n)$, from (14).

In the rest of the paper, we specialize our analysis to the polynomial family defined in equation (4). The derivative of $F(x)$ is given by

$$F'(x) = \omega + (x^p - x)\, h'(x) + (p\, x^{p-1} - 1) h(x). \tag{18}$$

Introducing the auxiliary polynomial

$$H(x) = \omega - h(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{19}$$

we see that

$$F(x) \equiv \omega x \pmod{p} \qquad F'(x) \equiv H(x) \pmod{p} \tag{20}$$

where the left congruence follows from Fermat's theorem: $x^p \equiv x \pmod{p}$ for all x.

Without loss of generality, we shall require that the multiplier of the fixed point at zero be unaffected by the nonlinear terms, that is

$$F'(0) = \omega \qquad \Longleftrightarrow \qquad H(0) = \omega, \tag{21}$$

which also ensures that F leaves each circle around the origin invariant, as easily verified (cf. equation (12)).

By lemma 3.1 and equation (20), we have that, if

$$H(x) \not\equiv 0 \pmod{p} \qquad x = 1, \ldots, p-1 \tag{22}$$

then $F'(x)$ has no roots modulo p, whence $F(x)$ is a permutation polynomial modulo p^k for all k, with a fixed point at the origin. Because $x^{p-1}-1 \equiv \prod_{k=1}^{p-1}(x-k) \pmod{p}$, the condition (22) is seen to be equivalent to

$$\gcd(x^{p-1}-1, H(x)) = 1 \tag{23}$$

which can be verified in polynomial time with Euclid's algorithm.

Now, for the members of the family (4), by construction, the function $\Phi_T(x)$, vanishes identically modulo p for all nonzero x, its roots accounting for m T-cycles, where m and T are related by (5). From equations (16) and (20), we see that if (23) is satisfied, each such cycle lifts to a p-adic cycle provided that λ is not a one-unit. The latter condition is written as

$$\lambda(x) \equiv \prod_{t=0}^{T-1} H(\omega^t x) \not\equiv 1 \pmod{p} \qquad |x|_p = 1.$$

The simplest situation occurs when the multipliers are maximal, whence neither one-units nor roots of unity. Then all cycles can be lifted, and are surrounded by discs, which constitute a tessellation of $\mathbf{Z}_p$, from proposition 3.2. This configuration could be regarded as the p-adic equivalent of a nonlinear resonance (figure 1). It remains to show that the conditions on multipliers can actually be achieved for a specific polynomial $H(x)$. We shall deal with this problem in section 4.

The requirement that the multiplier is not a one-unit is not redundant. The next result identifies circumstances in which this phenomenon leads to failure of lifting.

Proposition 3.3 *Let $F(x)$ be given by (4), and let $F'(0) = \omega$ be a one-unit of level 1 (so that $F(x) \equiv x \pmod{p}$, identically). If, for some $a \not\equiv 0 \pmod{p}$, $F'(a)$ is a one-unit, then the fixed point $x \equiv a \pmod{p}$ does not lift.*

One example is given by $F(x) = (1+p)x + (x^p - x)px$.

Proof. Let $\omega = 1 + p\beta$, where $|\beta|_p = 1$. Then $\Phi_1(a) = F(a) - a \equiv 0 \pmod{p}$, and $\Phi_1'(a) = \lambda(a) - 1 = p^s\gamma$, where γ is a unit. We attempt to find a unit δ such that $a + p\delta$ is a fixed point modulo p^2. We have

$$\begin{aligned}
\Phi_1(a+p\delta) &= \Phi_1(a) + \Phi_1'(a)\,p\delta + O(p^2) \\
&= p\beta\, a + h(a)(a^p - a) + O(p^2) \\
&= a\left[p\beta + h(a)(a^{p-1}-1)\right] + O(p^2).
\end{aligned}$$

Since, by assumption, $|a|_p = 1$, for the fixed point to exist, the quantity in square brackets must be $O(p^2)$.

Now, the equation $\Phi_1'(a) = p^s\gamma$ reads

$$p\beta + h'(a)(a^p - a) + h(a)(pa^{p-1} - 1) = p^s\gamma,$$

giving $h(a) = O(p)$, and since $a^{p-1} - 1 = O(p)$ (a is non-zero modulo p) we have

$$\Phi_1(a + p\delta) = ap\beta + O(p^2)$$

and the fixed point modulo p^2 does not exist. □

We conclude this section with a remark on resonance. As the multiplier ω approaches a $(p-1)$th root of unity, corresponding to $s \to \infty$ in equation (5), so do all points of the T-cycles on the unit circle. Indeed let ξ, ξ' be $(p-1)$th roots of unity, and let $\omega = \xi + p^s$. Then, since ξ' is a root of $x^p - x$, we find that, for any choice of $h(x)$

$$F(\xi') = \xi\xi' + O(p^s).$$

Because $\xi\xi'$ is also a $(p-1)$th root of unity, we obtain the desired result by letting $s \to \infty$, which also causes the size of the disc at the origin to shrink to zero. Letting $F(x) = \xi x + O(x^2)$, one finds (for $T \neq 1$) $F^T(x) = x + O(x^3)$, but the details of the motions at resonance require further study.

4 Multipliers

We turn to the problem of identifying maximal multipliers, which requires computation modulo p^2. Clearly, one must first check primitivity modulo p. We thus consider the mapping (4), with ω primitive, and compute modulo p the multiplier λ of the $(p-1)$-cycle on the unit circle.

Equations (16) and (20) give

$$\lambda(x) \equiv (F^{p-1}(x))' = \prod_{k=1}^{p-1} H(k) \pmod{p} \qquad (24)$$

where the right hand side depends on H only, and not on x. The product (24) is taken over all roots of the polynomial $x^{p-1} - 1$ modulo p, whence

$$\lambda \equiv \operatorname{Res}(x^{p-1} - 1,\, H(x)) \pmod{p} \qquad (25)$$

where Res denotes the resultant ([23], page 36). The computation of the resultant, as a determinant, is no faster than the evaluation of the product (24). However, equation (25) leads to useful formulae.

Let $H(x)$ be specified by (19) and (21), and let $\alpha_1, \ldots, \alpha_n$ be the roots of $H(x)$ in some extension of $\mathbf{F}_p$, the field with p elements. Since $p-1$ is even, we have from the properties of the resultant

$$\begin{aligned} \lambda &\equiv \operatorname{Res}(H(x), x^{p-1}-1) \equiv a_n^{p-1} \prod_{i=1}^{n} (\alpha_i^{p-1} - 1) \\ &\equiv \prod_{i=1}^{n} (\alpha_i^{p-1} - 1) \pmod{p}. \end{aligned} \tag{26}$$

In the case in which $h(x) = ax^n$ is a monomial, we have $H(x) = \omega - ax^n$, and the roots of $H(x)$ are $\alpha_i = \zeta^i \alpha$, where $\alpha = \sqrt[n]{\omega/a}$ is a root of $H(x)$ and ζ is a nth root of unity. From equation (26) one finds

$$\lambda \equiv \left((\omega/a)^{(p-1)/d} - 1 \right)^d \pmod{p} \qquad d = \gcd(n, p-1).$$

If $d > 1$, then λ is a dth power, whence $T(\lambda)$ is a divisor of $(p-1)/d$, and λ is not primitive; if $d = 1$, then $\lambda \equiv 0 \pmod{p}$, is again not primitive. In either case, one cannot achieve primitivity, whence maximality.

Beyond monomials, the obvious case is when $H(x)$ is irreducible over $\mathbf{F}_p$. The Galois group $\mathbf{F}_{p^n} : \mathbf{F}_p$ is cyclic, and is generated by the Frobenius automorphism σ: $x \mapsto x^p$ ([23], page 75). We order the roots of $H(x)$ in such a way that $\sigma(\alpha_i) = \alpha_{i+1}$, with i a cyclic index. From equation (26) we obtain

$$\begin{aligned} \lambda &\equiv \prod_{i=1}^{n} \frac{\alpha_i^p - \alpha_i}{\alpha_i} \equiv \frac{a_n}{\omega} \prod_{i=1}^{n} (\alpha_i^p - \alpha_i) \\ &\equiv \frac{a_n}{\omega} \prod_{i=1}^{n} (\alpha_{i+1} - \alpha_i) \pmod{p}. \end{aligned} \tag{27}$$

If $H(x) = \prod_k H_k(x)$ is not irreducible (with factors $H_k(x)$ of degree $n_k \geq 2$, for invertibility), the above formula is generalized by ordering the roots $\alpha_i^{(k)}$ of each factor $H_k(x)$, giving

$$\lambda \equiv \frac{a_n}{\omega} \prod_k \prod_{i=1}^{n_k} (\alpha_{i+1}^{(k)} - \alpha_i^{(k)}) \pmod{p}.$$

If $H(x)$ is quadratic or cubic (or if all its factors $H_k(x)$ are), the quantity λ is connected to its discriminant Δ, given by ([23], page 35)

$$\Delta(H) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \tag{28}$$

When $H(x)$ is quadratic and irreducible modulo p, we find, from (27) and (28)

$$\lambda \equiv \frac{a_2}{\omega}(\alpha_2 - \alpha_1)(\alpha_1 - \alpha_2) = -\frac{\Delta}{\omega a_2} \pmod{p}. \tag{29}$$

Similarly, when $H(x)$ is cubic and irreducible modulo p, we have

$$\lambda \equiv \frac{a_3}{\omega}(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_2)(\alpha_1 - \alpha_3) = \pm\frac{\sqrt{\Delta}}{\omega a_3} \pmod{p}. \tag{30}$$

Note that in the above formula Δ is a square, from Stickelberger's theorem ([9], page 351). In this case there remains a sign ambiguity. Now, if $p \equiv 1 \pmod 4$, then λ is primitive if and only if $-\lambda$ is, so knowledge of the sign is unimportant to primitivity. On the other hand, if $p \equiv 3 \pmod 4$, then if λ is primitive $-\lambda$ is not, so the sign matters, and formula (30) provides less information.

The importance of quadratic and cubic auxiliary polynomials is clarified by the following conjectures

Conjecture 1 *For every maximal ω and λ, there exists a cubic polynomial $H(x) \in \mathbf{Z}[x]$, such that $F(x)$ of (4) has a $(p-1)$-cycle on the unit circle, with multiplier $\lambda^* \equiv \lambda \pmod{p^2}$.*

It should be clear that $\lambda \neq \lambda^*$, in general. If one merely requires that λ be an unspecified primitive element, one has the alternative

Conjecture 2 *For every maximal ω, there exists a quadratic polynomial $H(x) \in \mathbf{Z}[x]$, such that the multiplier λ of the $(p-1)$-cycle of $F(x)$ is also maximal.*

These conjectures are supported by numerical evidence obtained by calculating $\lambda(x) = \prod_{t=1}^{p-1} H(F^t(x)) \pmod{p^2}$ for x such that $F^{p-1}(x) \equiv x \pmod{p^2}$. Conjecture 1 has been verified for every (ω, λ) combination with ω and λ both maximal for $p \leq 17$. Conjecture 2 has been verified for every maximal ω for $p \leq 29$.

In the next section, we show that the families of polynomials of the above conjectures are necessarily infinite.

5 Density and heuristic estimates

Let us consider the factorization modulo p of an irreducible polynomial $H(x) \in \mathbf{Z}[x]$

$$H(x) \equiv H_1(x) \cdots H_r(x) \pmod{p}.$$

For all but finitely many primes (the divisors of the discriminant of $H(x)$, which are excluded from consideration), the factors $H_k(x)$ are distinct. If n is the degree of $H(x)$, and n_k that of $H_k(x)$, the above factorization corresponds to the additive partition $n = n_1 + \cdots + n_r$. Let $\pi(t)$ be the number of primes $\leq t$, and let $A(n_1, \ldots, n_r, t)$ be the number of times such a partition occurs among these primes. The Cebotarev density theorem states that the limit

$$\lim_{t \to \infty} \frac{A(n_1, \ldots, n_r, t)}{\pi(t)} \tag{31}$$

exists, and is equal to the frequency of occurrence of the permutations in the Galois group of $H(x)$, whose cycle decomposition has n_k as cycle lengths [12]. In particular, the limit (31) is a rational number whose denominator divides $n!$. The function sending primes to elements of the Galois group is called the *Artin map* ([10]).

An application of the above theorem will result from the following

Lemma 5.1 *Let $\mathcal{F}$ be a family of polynomials over $\mathbf{Z}$, with the property that, for almost all primes p, at least one member of $\mathcal{F}$ has no roots modulo p. Then $\mathcal{F}$ is infinite.*

The term 'almost all' disregards sets of zero density.

Proof. Assume that $\mathcal{F}$ is finite. Then the roots of all polynomials in $\mathcal{F}$ generate a finite Galois extension $K : \mathbf{Q}$. The set of primes p that split completely in K is mapped under the Artin map to the identity of the Galois group, and hence, from Cebotarev's theorem, its density is no smaller than $1/n!$, where n is the degree of $K : \mathbf{Q}$. Now, if p splits completely in K, it also splits completely in every subfield ([24], page 105), and so for such primes *all* polynomials in $\mathcal{F}$ split completely modulo p, contrary to the assumption. So $\mathcal{F}$ is infinite. $\square$

Let now $\mathcal{F}$ be a set of $H(x)$-polynomials. If $\mathcal{F}$ is finite, then, for a set of primes of positive density, condition (23) will be violated for all elements of $\mathcal{F}$, making the multipliers of all corresponding mappings $F(x)$ vanish modulo p, and, in particular, making them non-maximal. Thus, if conjectures 1 and 2 are true, the corresponding families of $H(x)$-polynomials are necessarily infinite.

In the following example, we combine Cebotarev's theorem, arithmetical considerations, and some heuristic assumptions, to estimate the probability of occurrence of maximal multipliers. We consider the map

$$F(x) = 2x - (x^p - x)(x + x^2).$$

The multiplier $\omega = 2$ is square-free in $\mathbf{Z}$, and is not a root of unity, and so it is a candidate for maximality for any odd prime p. With reference to equations (19) and (29), we find

$$H(x) = 2 + x + x^2; \qquad \Delta = -7; \qquad \lambda \equiv 7/2 \,(\mathrm{mod}\ p) \tag{32}$$

where the right expression holds whenever $H(x)$ is irreducible modulo p. So λ is also a candidate for maximality. Now, the Galois group of $H(x)$ is C_2, giving two partitions $2 = 1 + 1$ and $2 = 2$, corresponding to $H(x)$ being reducible and irreducible, respectively, and each event has density $1/2$, from Cebotarev's theorem. More precisely, using quadratic reciprocity, we find that $H(x)$ is irreducible when $p \equiv 3, 5, 6 \,(\mathrm{mod}\ 7)$. Assuming the validity of the generalized Riemann hypothesis, the probability that a square-free integer be primitive modulo p is given by Artin's constant [28]

$$\mathcal{A} = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558\ldots$$

(Artin's constant has appeared in the dynamics literature, in related contexts [18, 4].) If we assume that $\mathcal{A}$ also describes the probability of primitivity for the primes in the given arithmetic progressions, and that the order of ω and λ are independent, then the probability that both ω and λ are primitive is estimated as $\mathcal{A}^2/2 \simeq 0.070$. Now, the probability that a primitive multiplier be non-maximal is $1/p$ (there are p choices for its second digit, and only one is non-maximal), which for large p can be neglected. So the above estimate can be taken as the probability of occurrence of two maximal multipliers.

Let $\mathcal{C}$ be the set of primes for which $H(x)$ in equation (32) has no roots modulo p (i.e. $p \equiv 3, 5, 6 \,(\mathrm{mod}\ 7)$), and let $\mathcal{P}_a$ the set of primes for which a is a primitive element. The following table displays densities of various sets, computed with the first 10^7 primes.

The Cebotarev and Artin frequencies for both ω and λ (the first three columns), agree with their limit value, within four decimal digits. Taking this as the accuracy of the remaining data, we see from the last column, that the probability that λ and ω are both primitive is some 10% higher than estimated. This discrepancy can be attributed to two factors. First, the presence of correlations between the orders of λ

$\mathcal{C}$	$\mathcal{P}_\omega$	$\mathcal{P}_\lambda$	$\mathcal{P}_\omega \cap \mathcal{P}_\lambda$	$\mathcal{P}_\omega \cap \mathcal{C}$	$\mathcal{P}_\lambda \cap \mathcal{C}$	$\mathcal{P}_\omega \cap \mathcal{P}_\lambda \cap \mathcal{C}$
0.500012	0.373985	0.374038	0.147402	0.383098	0.383193	0.07714

and ω. The probability of both being primitive computed over all primes, should be $\mathcal{A}^2 = 0.13984\ldots$, while column 4 gives a higher figure. Second, primitivity appears to be more frequent in $\mathcal{C}$ than in the set of all primes, which is seen by comparing columns 2 and 3 with 5 and 6, respectively.

To derive a similar estimate for an irreducible polynomial $H(x)$ of higher degree, one requires information on its Galois group G. Specifically, the density 1/2 appearing in the quadratic case is to be replaced by the density of the fixed-point-free elements in G. For a "randomly chosen" integral polynomial $H(x)$ of degree n, we can expect the Galois group to be the symmetric group S_n, whose fixed-point-free elements have density ([8], section 6.7)

$$\sum_{k=0}^{n} \frac{(-1)^k}{k!} \longrightarrow \frac{1}{e}$$

giving the rough estimate $\mathcal{A}^2/e$ for the probability of maximal multipliers, when the degree of $H(x)$ is sufficiently large.

References

[1] S. Albeverio, A. Khrennikov and P. E. Kloeden, Memory retrieval as a p-adic dynamical system, *BioSystems*, **49**, 1999, 105–115

[2] T. M. Apostol, Introduction to analytic number theory, Springer Verlag, (1976).

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

[4] M. Bartuccelli and F. Vivaldi, Ideal orbits of toral automorphisms, *Physica D* **39** (1989) 194–204.

[5] R. Benedetto, p-adic dynamics and Sullivan's no wandering domain theorem, *Compositio Mathematica*, **122**, (2000), 281–298.

[6] T. Bousch, Sur quelques problèmes de la dynamique holomorphe, Ph.D. thesis, Université de Paris-Sud, Centre d'Orsay (1992).

[7] D. Bosio and F. Vivaldi, Round-off errors and p-adic numbers, *Nonlinearity*, **13**, (2000), 309–322.

[8] P. J. Cameron, *Permutation groups,* Cambridge University Press, Cambridge (1999).

[9] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, New York, (1996).

[10] D. A. Cox, *Primes of the form* x^2+ny^2, John Wiley and Sons, New York (1989).

[11] S. N. Coppersmith, L. P. Kadanoff and Z. Zhang, Reversible boolean networks I: distribution of cycle length, *Physica D* **149** (2001) 11–29.

[12] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge, (1990).

[13] F. Q. Gouvêa, *p-adic numbers: an introduction,* Springer-Verlag, Berlin (1993).

[14] H. Hasse, *Number Theory*, Springer-Verlag, Berlin, (1980).

[15] M. R. Herman and J-C. Yoccoz, Generalization of some theorem of small divisors to non-archimedean fields, in *Geometric Dynamics*, vol LNM **10007** Springer-Verlag, New York, (1983) 408–447.

[16] L. Hsia, Closure of periodic points over a non-archimedean field, Preprint, Department of Mathematics, National Central University, Taiwan, (1999).

[17] K. Kaneko, Symplectic cellular automata, *Phys. Lett. A* **129** (1988) 9–16.

[18] J. P. Keating, Asymptotic properties of the periodic orbits of the cat maps, *Nonlinearity* **4** (1991) 277–307.

[19] N. Koblitz, *Algebraic aspects of cryptography*, Springer-Verlag, New York, (1997).

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

[21] K-O Lindhal, On the conjugation of analytic p-adic dynamical systems, preprint, Växjö University (2001), `Karl-Olof.Lindhal@msi.vxu.se`.

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

[23] R. Lidl and H. Niederreiter, Finite fields, *Encyclopedia of Mathematics and Its Applications*, **20**, Cambridge University Press, Cambridge, (1996).

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

[25] P. Morton and P. Patel, The Galois theory of periodic points of polynomial maps, *Proc. London Math. Soc.* **68** (1994) 225–263.

[26] P. Morton and J. Silverman, Periodic points, multiplicities, and dynamical units, *J. Reine Angew. Math.*, **461** (1995) 81–122.

[27] P. Morton and F. Vivaldi, Bifurcations and discriminants for polynomials maps, *Nonlinearity* **8** (1995) 571–584.

[28] M. RamMurty, Artin's conjecture for primitive roots, *Math. Intelligencer* **10** (1988) 59–67.

[29] F. Rannou, Numerical studies of discrete plane area-preserving mappings, *Astron. Astrophys.* **31** (1974) 289–301.

[30] W. H. Schikhof, *Unltrametric calculus,* Cambridge University Press, Cambridge (1984).

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

[32] L. A. Shepp and S. P. Lloyd, Ordered cycle lengths in a random permutation, *Trans. Amer. Math. Soc.* **121** (1996) 340–357.

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

[34] F. Vivaldi and S. Hatjispyros, Galois theory of periodic orbits of rational maps, *Nonlinearity* **5** (1992) 961–978.

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