Pseudo-randomness of round-off errors in discretized linear maps on the plane

Franco Vivaldi and Igor Vladimirov†

School of Mathematical Sciences, Queen Mary, University of London
London E1 4NS, UK
† Mathematics Department, University of Queensland
Brisbane QLD 4072, Australia

April 20, 2001

Abstract

We analyze the sequences of round-off errors of the orbits of a discretized planar rotation, from a probabilistic angle. In [9] it was shown that for a dense set of parameters, the discretized map can be embedded into an expanding p-adic dynamical system, which serves as source of deterministic randomness. For each parameter value, these systems can generate infinitely many distinct pseudo-random sequences over a finite alphabet, whose average period is conjectured to grow exponentially with the bit-length of the initial condition (the seed). We study some properties of these symbolic sequences, deriving a central limit theorem for the deviations between round-off and exact orbits, and obtaining bounds concerning repetitions of words. We also explore some asymptotic problems computationally, verifying, among other things, that the occurrence of words of a given length is consistent with that of an abstract Bernoulli sequence.

KEYWORDS: round-off errors, pseudo-random sequences, p-adic dynamics.

This work was supported by the Engineering and Physical Sciences Research Council Grant GM/M85906 and the Australian Research Council Grant A10027063.

Contents

1 Introduction **3**

2 Preliminaries **6**
2.1 Embeddings and norms . . . 7
2.2 Period function . . . 10

3 Symbolic dynamics **11**
3.1 Short vectors and repeated codewords . . . 12
3.2 Representability of symbols in abstract Bernoulli sequences . . . 14
3.3 Numerical experiments . . . 15

4 Propagation of round-off errors **16**
4.1 Barycentre and inertia tensor of deviation range . . . 18
4.2 Asymptotic growth rate of deviation range . . . 19
4.3 Central limit theorem . . . 20
4.4 Numerical experiments . . . 21

5 Appendix: Proofs **24**
5.1 Proposition 4.1 . . . 24
5.2 Proposition 4.2 . . . 25
5.3 Proposition 4.3 . . . 27
5.4 Proposition 3.3 . . . 28
5.5 Proposition 3.4 . . . 29
5.6 Proposition 3.5 . . . 29
5.7 Theorem 1 . . . 32

1 Introduction

The study of round-off errors in spatial discretizations of dynamical systems has attracted considerable interest in recent years (see [5, 7, 17, 11, 12, 9], and references therein). In this paper we investigate the extent to which round-off fluctuations can generate pseudo-random sequences, using a specific model introduced in [9].

To construct pseudo-random sequences from smooth deterministic chaos one needs two ingredients. Firstly, a strongly chaotic map f on a compactum, with a complete symbolic dynamics. The latter will be the source of pseudo-random symbols. Secondly, a *discrete* embedding into f, which is effectively representable in a computer. The embedding must capture 'useful' ergodic properties of f; for instance, it should be, asymptotically, dense and uniform with respect to the natural invariant measure of f. However, such requirement is not sufficient (see below), and although there is no agreed definition of chaos in discrete systems [18, 10], a compelling indicator is the presence of computationally intractable problems, that is, problems that cannot be solved in polynomial time.

Linear expanding maps of the circle (and their numerous generalizations), provide the dynamical engine for the linear congruential methods for random number generation. A well-known example is the doubling map $f : x \mapsto 2x$ which is (essentially) conjugate to a full Bernoulli shift on two symbols. This system restricts to the set of rational points on the circle with odd denominator, which constitute its periodic set, and where the dynamics is *invertible.* This set foliates into the rationals with fixed odd denominator N, which are naturally identified with the modular lattice $\mathbb{Z}/N\mathbb{Z}$.

The dynamics on $\mathbb{Z}/N\mathbb{Z}$ are the desired discrete embeddings in the circle. An integer orbit $x_0, x_1, \dots$ generates a binary periodic sequence via $\lfloor 2\, x_t/N \rfloor$, where $\lfloor \cdot \rfloor$ is the floor function. Its period $T_N = T_N(x_0)$, which is the same for all 'seeds' x_0 coprime to N, is maximal when $N = p$ is prime. In this case, the computation of the period and, more in general, that of the transit time between two points in an orbit, involve two classic non-polynomial time problems, namely, prime factorization and discrete logarithm. Asymptotics of period length are notoriously difficult to handle. Estimates of the type $T_N \sim N/\log(N)^{e(N)}$, where $e(N) = O(\log\log\log(N))$, can be derived assuming the validity of the Riemann hypothesis for algebraic number fields (see [18], and references therein).

The situation is quite different when $N = p^n$, an odd prime power. The lattice

$\mathbb{Z}/p^n\mathbb{Z}$ can also be embedded in the p-adic integers $\mathbb{Z}_p$, consisting of the series

$$\chi = \sum_{k\geq m} b_k\, p^k \qquad\qquad m \geq 0 \qquad b_k \in \{0,\ldots,p-1\} \tag{1}$$

which converge with respect to the non-achimedean absolute value $|\chi|_p = p^{-m}$ (see, e.g., [15]). In the resulting metric, $\mathbb{Z}_p$ is a compact ring where the integers are dense. Because the multiplier now lies on the unit circle (meaning that $|2|_p = 1$), we also have an embedding into a *regular* p-adic dynamical system, featuring quasi-periodic motions [3]. By sharp contrast with the case of prime moduli, the period function T_{p^n}, and the transit times can now be computed in polynomial time, and hence the dynamics modulus a prime-power has no cryptographical value.

The study of dynamics over the p-adics is undergoing a rapid development, whereby archimedean dynamical constructs are exported to a non-archimedean setting, with a wide range of motivations and applications, see [33, 22, 1, 6, 9], and references therein. In [32] the chaotic p-adic dynamical system $f(x) = (x^p - x)/p$ was proposed as a source of pseudo-random sequences. Such system is topologically conjugate to a shift over p symbols, and for $p = 2$, it reduces to a permutation on every lattice $\mathbb{Z}/p^n\mathbb{Z}$, with long average cycle length. The occasional presence of short cycles creates some problems of implementation.

Here we propose an embedding into a p-adic chaotic system, which combines the two dynamical elements mentioned above — Bernoulli shift and quasi-periodic rotation — together with a straightforward and efficient implementation with integer arithmetic. The starting point is the planar map

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

which describes linear elliptic motions. We discretize it by forcing it onto a lattice, as follows

$$\Phi : \mathbb{Z}^2 \mapsto \mathbb{Z}^2 \qquad (x,y) \mapsto (\lfloor \alpha x \rfloor - y,\, x) \tag{3}$$

[31, 20, 21, 9]. One verifies that Φ is *invertible* (cf. [13]). The discretization length is fixed and equal to unity, while the limit of vanishing discretization is achieved by considering motions at infinity. We consider a dense set of rational values of α of the form q/p^n, where p is a prime, q is relatively prime to p, and $|q| < 2p^n$. A rational α yields an irrational rotation number ν (where $\alpha = 2\cos(2\pi\nu)$), apart from finitely many exceptions (see, e.g. [23], chapter 2). All orbits of this system are believed to be periodic (as opposed to being unbounded), and they consist of points sprinkled irregularly around the invariant ellipses of the mapping Ψ.

In [9] it was shown that 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

$$\chi_{t+1} = \Phi^*(\chi_t) = \sigma^n(\overline{\theta}\, \chi_t) \tag{4}$$

where $\overline{\theta} = \mathcal{L}(q, p^n)$ is a p-adic unit (that is, $|\bar{\theta}|_p = 1$) and σ is the shift mapping, which is defined like its archimedean counterpart [27, 2, 32]; if $\chi = b_0 + b_1 p + b_2 p^2 + \cdots$, then

$$\sigma(\chi) \;=\; b_1 + b_2 p + b_3 p^2 + \cdots. \tag{5}$$

The above result connects the round-off problem with an expanding map over the p-adics, featuring a complete symbolic dynamics over p^n symbols, and 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 each residue class modulo p^k the measure p^{-k}.

The purpose of this paper is to study the sequence of round-off errors of orbits with sufficiently large initial condition (the seed). Even though these orbits form a zero-density subset among all periodic orbits of (4), they appear to enjoy strong statistical properties.

After reviewing the construction underpinning the representation (4), we define an archimedean and a non-archimedean norm in $\mathbb{Z}^2$. These norms originate from two embeddings of the dynamics in $\mathbb{R}^2$ and $\mathbb{Z}_p$, respectively, whose interplay is the underlying theme of this work. We then explore experimentally some asymptotics of the system's period function, which appears to be computationally intractable. The period is seen to grow, on average, exponentially with the bit length of the initial condition (the seed).

In section 3, using arithmetical methods, we compute the length of short vectors in the lattices which generate the symbolic partition, and from it we derive bounds concerning repeated words in a coding sequence (propositions 3.2 and 3.3). We then derive the limit distribution for the occurrence of words of a given length in an abstract Bernoulli sequence (proposition 3.5), and verify experimentally that such distribution describes well the statistics of words in the code of long orbits.

Section 4 is devoted to an analysis of the propagation of round-off errors. The average deviation between exact and round-off orbits is described by a central limit theorem (theorem 1) (which extends results obtained in [29]), while the maximal deviation is computed in proposition 4.3.

Most proofs are confined to an appendix.

The study of space discretization invariably involves two non-commuting limits, diverging time and vanishing discretization length, which give rise to several characteristic time scales. The central limit theorem results from a complete symbolic dynamics, and as such it refers implicitly to a time scale which is logarithmic in the inverse discretization length. Over this time scale, genuine randomness can take place. On the other hand, many interesting aspects of discrete pseudo-randomness occur over much longer time scales, which are largely unexplored via a rigorous analysis, due to considerable mathematical difficulties.

In particular, the numerical experiment of section 4.4 shows that the propagation of round-off errors is consistent with a Gaussian model (at least as far as the first two moments are concerned), for a time scale much longer than what one could expect from the present development of the theory. This phenomenon seems to originate from the strong uniformity of round-off orbits with respect to the p-adic invariant measure.

2 Preliminaries

We begin with symbolic dynamics over the finite alphabet

$$\Pi = \{0, 1, \ldots, p^n - 1\}. \tag{6}$$

The round-off error at the point $z = (x, y)$ affects only the x-coordinate (cf. (3)), and is given by

$$\left\{ \frac{qx}{p^n} \right\} = \frac{c}{p^n},$$

where $\{u\} = u - \lfloor u \rfloor$ denotes the fractional part of a real number u, and c is the smallest non-negative residue of qx modulo p^n

$$c = c(x) \equiv qx \pmod{p^n}, \qquad c \in \Pi. \tag{7}$$

For any initial condition z, the values of c give a symbolic sequence

$$\mathcal{C} \;=\; \mathcal{C}(z) \;=\; (c_0, c_1, c_2, \ldots) \tag{8}$$

where $c_t = c(x_t)$, and $z_t = (x_t, y_t)$ is the t-th point in the orbit with initial condition $z = z_0$. Truncation to the first k symbols yields the *k-code*

$$C_k(z) = (c_0, \ldots, c_{k-1}) \in \Pi^k. \tag{9}$$

We define the sequence of mappings $h_k : \mathbb{Z}^2 \to \mathbb{Z}/p^{kn}\mathbb{Z}$ by

$$h_k(x, y) \equiv a_k x + b_k y \,(\mathrm{mod}\ p^{kn}) \tag{10}$$

where

$$a_1 = 1; \quad b_1 = 0; \qquad \begin{cases} a_{k+1} = q\, a_k + \ p^n\, b_k \\ b_{k+1} = -p^n\, a_k \end{cases} \qquad k \geq 1, \tag{11}$$

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

$$\mathcal{M}_k \ = \ \{(x, y) \in \mathbb{Z}^2 \ : \ a_k x + b_k y \equiv 0 \,(\mathrm{mod}\ p^{kn})\}. \tag{12}$$

The sets $\mathcal{M}_k$ form a nested sequence of lattices: $\mathcal{M}_{k+1} \subset \mathcal{M}_k$, with $\#(\mathbb{Z}^2/\mathcal{M}_k) = p^{kn}$, (here, $\#(\,\cdot\,)$ denotes the cardinality of a finite set). Their significance stems from the fact that two points in $\mathbb{Z}^2$ have the same k-code if and only if they are congruent modulo $\mathcal{M}_k$. In other words, for each k, the map C_k defined in (9) is periodic with period lattice $\mathcal{M}_k$ (i.e., $C_k(z+w) = C_k(z)$ for all $z \in \mathbb{Z}^2$ and $w \in \mathcal{M}_k$) and it maps bijectively any fundamental domain of $\mathcal{M}_k$ onto Π^k.

2.1 Embeddings and norms

The unperturbed mapping Ψ, defined in (2), is represented by the matrix

$$A = \begin{bmatrix} \alpha & -1 \\ 1 & 0 \end{bmatrix}. \tag{13}$$

The recursion (11) is then represented by $p^n A$, with characteristic polynomial

$$f(X) \ = \ X^2 - q\, X + p^{2n}. \tag{14}$$

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

$$\lambda \ = \ \frac{q \ + \sqrt{q^2 - 4p^{2n}}}{2}; \qquad \lambda^2 = q\, \lambda - p^{2n}; \qquad \overline{\lambda} = q - \lambda \tag{15}$$

and are related to the coefficients a_k and b_k of equation (11) by the identity

$$\lambda^k = a_k\,\lambda + b_k\,p^n \qquad k = 1, 2, \ldots. \tag{16}$$

The arithmetical environment relevant to the round-off problem is the ring $\mathbb{Z}[\lambda]$ of numbers of the form $x + y\lambda$ with x and y integers. From (14), we see that $f(X)$ factors modulo p^{2n} into the product of two distinct polynomials

$$f(X) \equiv X(X - q)\,(\mathrm{mod}\; p^{2n}) \tag{17}$$

and therefore 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).

The derivative of f at its modular roots 0 and q does not vanish modulo p, and therefore such roots lift to two distinct p-adic roots θ and $\overline{\theta}$, respectively, which are the local images of λ and $\overline{\lambda}$ in $\mathbb{Z}_p$. These roots may be computed with the p-adic Newton's method ([25], section 2.2), and used to construct an integral basis for P^k

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

To embed the phase space $\mathbb{Z}^2$ into the p-adic integers, we first embed $\mathbb{Z}^2$ into $\mathbb{Z}[\lambda]$

$$\mathcal{L}_1 : \mathbb{Z}^2 \mapsto \mathbb{Z}[\lambda] \qquad (x, y) \mapsto p^n x - \lambda y. \tag{19}$$

The key feature of such embedding is the fact that

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

which gives an arithmetical characterization of the lattices $\mathcal{M}_k$.

Then we create a homomorphic image of $\mathbb{Z}[\lambda]$ in $\mathbb{Z}_p$, by identifying λ with its local image θ

$$\mathcal{L}_2 : \mathbb{Z}[\lambda] \;\mapsto\; \mathbb{Z}_p \qquad x + \lambda y \;\mapsto\; x + \theta\, y. \tag{20}$$

Composing the above two mappings and scaling, we obtain an embedding of $\mathbb{Z}^2$ into the p-adics

$$\mathcal{L} : \mathbb{Z}^2 \mapsto \mathbb{Z}_p \qquad (x, y) \mapsto \frac{1}{p^n}\,\mathcal{L}_2(\mathcal{L}_1(x, y)) \;=\; x - \frac{\theta}{p^n}\,y. \tag{21}$$

The set $\mathcal{Z} = \mathcal{L}(\mathbb{Z}^2)$ is an additive subgroup of the p-adic integers, which is invariant under multiplication by elements of the ring $\mathcal{L}_2(\mathbb{Z}[\lambda])$ (i.e., $\mathcal{Z}$ is a $\mathcal{L}_2(\mathbb{Z}[\lambda])$-module). Because $\mathcal{L}$ is a monomorphism, we define

$$\Phi^* : \mathcal{Z} \mapsto \mathcal{Z} \qquad\qquad \Phi^* \;=\; \mathcal{L} \circ \Phi \circ \mathcal{L}^{-1} \tag{22}$$

which is the construction underpinning formula (4).

The extension of Φ^* to $\mathbb{Z}_p$ induces an extension of the symbolic dynamics, which become complete. The unique initial condition corresponding to the code $C = (c_0, c_1, \dots)$ is given by the expansion

$$\chi = \frac{1}{\bar{\theta}} \sum_{t=0}^{\infty} c_t \left(\frac{p^n}{\bar{\theta}} \right)^t , \tag{23}$$

from which one derives formulae [9] for periodic points. These correspond to *rational* values of x and y in equation (21), with denominator coprime to p. The very rare *integer* solutions are the periodic orbits of the round-off mapping.

The composite structure of the round-off map calls for the introduction of two norms on $\mathbb{Z}^2$. On the one hand, the rotational component (the mapping Ψ) has the invariant Euclidean norm

$$\|(x,y)\| = \sqrt{p^{-n}\, Q(x,y)} \qquad\qquad Q(x,y) = p^n x^2 - qxy + p^n y^2. \tag{24}$$

On the other hand, the symbolic representation of round-off errors defines the non-archimedean norm (cf. (21))

$$\|(x,y)\|_p = |\mathcal{L}(x,y)|_p \tag{25}$$

resulting from the embedding $\mathcal{L}$ in $\mathbb{Z}_p$. The last equation asserts that $\|z\|_p = p^{-nk}$ if $z \in \mathcal{M}_k \setminus \mathcal{M}_{k+1}$.

The above norms extend naturally to the set of rational points on the plane, with denominator coprime to p, which can be embedded simultaneously in $\mathbb{R}^2$ and $\mathbb{Z}_p$.

Associated to the Euclidean norm, are some geometrical parameters of an orbit, the *inner* and *outer radii,* given by

$$\rho_*(z) = \min_{0 \le k < T(z)} \|\Phi^k(z)\|, \qquad\qquad \rho^*(z) = \max_{0 \le k < T(z)} \|\Phi^k(z)\|, \tag{26}$$

respectively ($T(z)$ is the period), and the *width*

$$\rho(z) = \rho^*(z) - \rho_*(z). \tag{27}$$

2.2 Period function

Substantial experimental evidence suggests that all points of $\mathbb{Z}^2$ are periodic under the round-off map, for any choice of parameters. We thus define the *period function* T of the map Φ by

$$T(z) = \min\{k \in \mathbb{N} : \ \Phi^k(z) = z\} \tag{28}$$

and $T(z) = \infty$, if such integer does not exist. This function features wild fluctuations (see Fig. 1, and [8]).

To explore the asymptotics of the function T, we have considered its restriction $T(x,0)$ to the positive x-axis. The average behaviour of such function is best investigated by considering the density $\mathcal{D}(X)$ of the set X of orbits having a representative point on the positive x-axis

$$\mathcal{D}(X) = \lim_{r\to\infty} \mathcal{D}_r; \qquad \mathcal{D}_r = \frac{\#(X \cap E_r)}{\#(\mathbb{Z}^2 \cap E_r)}, \qquad E_r = \{z \in \mathbb{R}^2 \ : \ \|z\| \leq r\}. \tag{29}$$

We shall approximate $\mathcal{D}_r$ by

$$\mathcal{D}'_r = \frac{\sqrt{4p^{2n} - q^2}}{2\pi\, p^n r^2} \sum_{x \leq r}{}' \; T(x,0). \tag{30}$$

where the primed sum includes a single representative point x for each orbit, and is normalized by the area of E_r. The discrepancy between $\mathcal{D}_r$ and $\mathcal{D}'_r$ originates from two sources: the discrepancy between the number of lattice points inside E_r and its area (which decays as $1/r$), and the fact that some orbits will cross the boundary of E_r. The latter contribution results from two terms of comparable size, which can be expected to cancel out, from a detailed balance argument. Regardless of this, the relative contribution each term was found numerically to decay as $r^{-1/3}$. Thus we conjecture

$$\lim_{r\to\infty} \frac{\mathcal{D}_r}{\mathcal{D}'_r} = 1.$$

The data of figure 2, which refer to the dyadic case $q/p^n = 1/2$, required some $2 \cdot 10^{13}$ iterations of the mapping Φ. In spite of the size of the averaging sample, the function $\mathcal{D}'(r)$ still features small-scale fluctuations, which provide only limited evidence of the existence of the density $\mathcal{D}(X)$. By the same token, the average order of the period function $T(x,0)$ is dominated by a linear term, although small fluctuations persist. (Similar results were obtained by restricting the period function to the main diagonal $x = y$.)

We summarize our findings in the following

Conjecture 1 *Let $T(z)$ and $\rho(z)$ be given by given by (28) and (27), respectively. Then*

$$\frac{1}{r^2}\sum_{\|z\|\leq r} T(z) \asymp r, \qquad\qquad \frac{\rho(z)}{\|z\|} \to 0 \qquad \text{as} \qquad \|z\| \to \infty.$$

In [31] it was shown that for almost all irrational rotation numbers ν one has the lower bound $T(z) > c\,\|z\|^{1/2+\epsilon}$, for some $c > 0$ and every positive ϵ. Is is reasonable to assume that the rotation numbers corresponding to rational trace are 'typical' in this sense [28]. In practice, however, the shortest periods seem to grow at least as fast as $\|z\|^{2/3}$, and the complex arrangement of their their values results from the structure of the rational approximants of the rotation number [8].

3 Symbolic dynamics

For any positive integer k, we denote by Δ_k the Euclidean norm of the shortest nonzero vector of the lattice $\mathcal{M}_k$

$$\Delta_k = \min\{\|z\| : \ z \in \mathcal{M}_k \setminus \{0\}\}. \tag{31}$$

The archimedean and the non-archimedean norms (24) and (25) are related via the sequence Δ_k. Indeed, if two distinct points $u, v \in \mathbb{Z}^2$ share the same k-code, that is, $\|u - v\|_p \leq p^{-k}$, then $\|u - v\| \geq \Delta_k$.

We shall compute Δ_k in the next section (lemma 3.1), by relating quadratic forms to ideals. From this we establish that before a sequence begins to repeat due to periodicity, all but the logarithmically short code words are distinct (proposition 3.2).

Knowledge of Δ_k also provides information on successive repetitions of code words. Specifically, let σ_k be the function which sends a point $z \in \mathbb{Z}^2$ to the number of successive repetitions of the k-th initial segment of the coding sequence

$$\sigma_k(z) = \min\{s \in \mathbb{N} : \ C_k(\Phi^{ks}(z)) \neq C_k(z)\}. \tag{32}$$

Clearly, $\sigma_k(z)$ is finite if and only if k is not a period of z. In particular, $\sigma_1(z)$ is the length of the initial run of the symbol $c_0(z)$ in the coding sequence. An upper bound for σ_k is derived in proposition 3.3.

Finally, for any $m \in \mathbb{N}$ with $mp^{nm} \leq T(z)$, we consider the first $s = \lfloor T(z)/m \rfloor$ disjoint successive segments of length m of the coding sequence $\mathcal{C}(z)$

$$C_m(\Phi^{mt}(z)), \qquad 0 \leq t < s.$$

For the corresponding construction with independent random variables, we compute the probability distribution of the number of words that appear a given number of times in a Bernoulli sequence (proposition 3.4), and then verify experimentally that the sequence C_m obeys the same law.

3.1 Short vectors and repeated codewords

We relate the ideal P^n and the form $Q(x, y)$ defined in equation (24). (For background reference, see [14], chapter XII.)

From the congruence (17), we have that $s_n \equiv \theta \equiv 0 \pmod{p^n}$, whence the basis formula (18) gives

$$P^n = [p^n, -\lambda].$$

Letting $\zeta = p^n x - \lambda y$ be a generic element of P^n, one verifies that

$$Q(x, y) = p^n x^2 - qxy + p^n y^2 = \frac{\zeta\bar{\zeta}}{p^n} \tag{33}$$

where the bar denotes algebraic conjugation.

In [9] it was shown that $P^{2nk} = (\lambda^k)$, a principal ideal. Equations (11) and (16) then give

$$P^{n(2k+2)} = (\lambda^{k+1}) = (-p^{2n} a_k + \lambda a_{k+1})$$

which, by virtue of the embedding (19), translates into $(p^n a_k, a_{k+1}) \in \mathcal{M}_{2k+1}$. The value of Q at such point is minimal, and given by (cf. equation (33))

$$Q(p^n a_k, a_{k+1}) = \frac{\lambda^{k+1}\bar{\lambda}^{k+1}}{p^n} = \frac{(\lambda\bar{\lambda})^{k+1}}{p^n} = p^{n(2k+1)}$$

so that the vector $(p^n a_k, a_{k+1})$ is a short vector in the lattice $\mathcal{M}_{2k+1}$.

Likewise, the equation

$$P^{n(2k+1)} = (\lambda^k)\, P^n = [p^n\lambda^k, -\lambda^{k+1}]$$

shows that the lattice $\mathcal{M}_{2k}$ contains vectors of Euclidean norm $p^{n(2k+1)/2}$ (corresponding to either element of the above basis), but not necessarily one of norm p^{nk}. The latter will be the case precisely when P^n is a principal ideal. Indeed, from (33), equation $Q(x,y) = p^{2nk}$ becomes

$$\zeta\bar{\zeta} = \lambda^k\bar{\lambda}^k p^n$$

to be solved for $\zeta \in P^n$. From unique ideal factorization, we find, exchanging conjugates if necessary, $(\zeta) = (\lambda^k)P^n$, which can be solved precisely when $P^n = (\pi)$ is principal, in which case $\zeta = \lambda^k\pi\eta$, for any unit η.

To decide this matter, we note that in the present context (positive definite forms), every form is equivalent to a unique reduced form, and the principal form is reduced, and given by

$$Q^*(x,y) \;=\; \begin{cases} x^2 + xy - \dfrac{q^2 - 4p^{2n} - 1}{4}\, y^2 & q \text{ odd} \\[2ex] x^2 - \dfrac{q^2 - 4p^{2n}}{4}\, y^2 & q \text{ even.} \end{cases} \tag{34}$$

If $|q| < p^n$, then either $Q(x,y)$ or $Q(y,-x)$ (which is properly equivalent to $Q(x,y)$) is reduced, and therefore non-principal. On the other hand, when $|q| > p^n$, then $Q(x,y)$ can be either principal or non-principal (e.g., $q/p^n = 5/3$ and $4/3$, respectively).

We have proved

Lemma 3.1 *The following holds*

$$\begin{array}{rl} \Delta_k = p^{nk/2} & k \text{ odd, or } k \text{ even and } P^n \text{ principal} \\ p^{nk/2} < \Delta_k \le p^{n(k+1)/2} & k \text{ even and } P^n \text{ non-principal.} \end{array}$$

In any case, we have the lower bound

$$p^{nk/2} \le \Delta_k. \tag{35}$$

From the above lemma we immediately obtain

Proposition 3.2 *The code of an orbit with outer radius ρ^* does not have any repeated k-word of length $k > 2\log_{p^n}(2\rho^*)$, until periodicity sets in.*

To place this result in perspective, we note that, experimentally, $\rho^*(z)/\|z\| \to 1$, while $T(z)$ grows linearly with $\|z\|$, on average (section 2.2).

Another consequence of Lemma 3.1 is the following result, proved in the appendix

Proposition 3.3 *For any given $k \in \mathbb{N}$, the function (32) satisfies the asymptotic inequality*

$$\limsup_{\|z\|\to+\infty} \frac{\sigma_k(z)}{\log_{p^n}\|z\|} \leq \frac{2}{k}. \tag{36}$$

3.2 Representability of symbols in abstract Bernoulli sequences

Let ω_t, $0 \leq t < s$, be s independent Bernoulli random elements distributed uniformly on a nonempty finite set Ω. Here Ω is an abstract alphabet, of cardinality $r = \#\Omega$. Define the random functions $\tau_{r,s} : \Omega \to \mathbb{Z}_+$ and $\nu_{r,s} : \mathbb{Z}_+ \to \mathbb{Z}_+$ by

$$\begin{aligned} \tau_{r,s}(w) &= \#\{0 \leq t < s : \ \omega_t = w\}, \\ \nu_{r,s}(k) &= \#\{w \in \Omega : \ \tau_{r,s}(w) = k\}. \end{aligned}$$

Informally, $\nu_{r,s}(k)$ is the number of those symbols of Ω which appear in the sequence ω_t, $0 \leq t < s$, exactly k times. Clearly, $\nu_{r,s}(k) = 0$ for all $k > s$, and

$$\sum_{0\leq k\leq s} \nu_{r,s}(k) = r, \qquad \sum_{1\leq k\leq s} k\,\nu_{r,s}(k) = s.$$

The joint probability distribution of the random variables $\nu_{r,s}(k)$, $0 \leq k \leq s$, is described by the following

Proposition 3.4 *Let $n_0, \dots, n_s \in \mathbb{Z}_+$ be a collection of numbers obeying the constraints*

$$\sum_{0\leq k\leq s} n_k = r, \qquad \sum_{1\leq k\leq s} k\,n_k = s. \tag{37}$$

Then

$$\mathbf{P}(\nu_{r,s}(k) = n_k \ \textit{for all}\ 0 \leq k \leq s) = \frac{r!\,s!\,r^{-s}}{\prod_{k=0}^{s}(n_k!\,(k!)^{n_k})}. \tag{38}$$

The proof will be given in section 5.5. Let $\nu_0, \ldots, \nu_s$ be $(s+1)$ independent $\mathbf{Po}(1/k!)$-distributed random variables. Here, $\mathbf{Po}(\lambda)$ denotes the Poisson distribution with parameter $\lambda > 0$. Recall that the probability for a $\mathbf{Po}(\lambda)$-distributed random variable to take a value $m \in \mathbb{Z}_+$ is equal to $\exp(-\lambda)\lambda^m/m!$. The equality (38) shows that the joint distribution of the random variables $\nu_{r,s}(k),\ 0 \le k \le s$, coincides with the conditional distribution of $\nu_0, \ldots, \nu_s$, given $\sum_{k=0} \nu_k = r$ and $\sum_{k=1} k\nu_k = s$. In turn, this last conditional distribution coincides with the restriction of the direct product $\prod_{k=0}^{s} \mathbf{Po}(1/k!)$ to the $(s-1)$-dimensional simplex in $\mathbb{Z}_+^{s+1}$ described by (37).

Proposition 3.5 *Suppose that the parameters $r, s \in \mathbb{N}$ are unboundedly growing in such a way that their ratio s/r tends to $\lambda > 0$. Then for any given $k \in \mathbb{Z}_+$, the normalized random variable $\nu_{r,s}(k)/r$ is convergent in mean square sense (and consequently, in probability) to* $\exp(-\lambda)\lambda^k/k!$. *That is,*

$$\mathbf{E}\left(\frac{\nu_{r,s}(k)}{r} - \frac{\lambda^k}{k!}\exp(-\lambda)\right)^2 \to 0 \qquad \text{as } r \to +\infty,\ \frac{s}{r} \to \lambda.$$

The proof is given in section 5.6. From the proof, one can see that in the case $r = s$ we have

$$\mathbf{E}\left(\frac{\nu_{r,r}(k)/r}{\exp(-1)/k!} - 1\right)^2 \to 0 \qquad \text{as } r \to +\infty,$$

uniformly in k satisfying $k! = o(r)$.

3.3 Numerical experiments

To adapt proposition 3.5 to the round-off problem, we let $\xi_t,\ \ 0 \le t < mp^{nm}$, be mp^{nm} independent Bernoulli random variables distributed uniformly on the set Π. Divide the sequence into p^{nm} successive segments of length m defined by

$$\omega_{m,t} = (\xi_{mt+j})_{0 \le j < m}, \qquad 0 \le t < p^{nm}.$$

Clearly, $\omega_{m,t}$ are independent Bernoulli random elements distributed uniformly on the alphabet Π^m. Denote by $N_m(k) = \nu_{p^{nm},p^{nm}}(k)$ the number of those symbols of Π^m (that is, words of length m over the alphabet Π) which are encountered among the segments $\omega_{m,t},\ 0 \le t < p^{nm}$, exactly k times. Application of proposition 3.5

yields that for any fixed $k \in \mathbb{Z}_+$, the normalised random variable $N_m(k)/p^{nm}$ converges to $\exp(-1)/k!$ as $m \to +\infty$.

Does this last asymptotic property of Bernoulli sequences hold for the coding sequences corresponding to sufficiently long cycles of the roundoff map? The following experimental result suggests that the answer is affirmative. We computed the numbers $N_m(k)$ for the coding sequence of the cycle of period $T = 3229740$ with initial condition $(200000, 0)$ for the dyadic case $q/p^n = 1/2$. Here, $m = 17$ is the largest integer satisfying $m2^m \leq T$, and $N_m(k)$ appeared to be zero for $k > 8$. The following table illustrates proximity of the normalised quantities $N_m(k)/p^{nm}$ to the theoretically expected Poisson limits $\exp(-1)/k!$.

k	$N_m(k)$	$N_m(k)/p^{nm}$	$\exp(-1)/k!$	rel.gap, %
0	48152	0.367371	0.367879	0.138318
1	48370	0.369034	0.367879	0.313788
2	24055	0.183526	0.183940	0.225422
3	7985	0.060921	0.061313	0.640198
4	2017	0.015388	0.015328	0.392596
5	402	0.003067	0.003066	0.044183
6	79	0.000603	0.000511	17.962545
7	11	0.000084	0.000073	14.976151
8	1	0.000008	0.000009	16.380981

4 Propagation of round-off errors

In this section, we quantify the effects of round-off errors, by studying the k-step deviation between the exact and round-off orbits through $z \in \mathbb{R}^2$, given by

$$d_k(z) = \Psi^k(z) - \Phi^k(z). \tag{39}$$

The process of averaging leads us to consider the k-th *deviation range*

$$D_k = d_k(\mathbb{Z}^2) \tag{40}$$

as well as the *centred deviation range* (Fig. 3)

$$\mathring{D}_k = D_k - \langle D_k \rangle, \qquad\qquad \langle D_k \rangle = \frac{1}{\# D_k} \sum_{w \in D_k} w \tag{41}$$

where $\langle D_k \rangle$ is the *barycentre* of D_k.

The deviation range is related to the width of an orbit (equation (27)) by the bound

$$\rho(z) \leq 2\delta(z), \tag{42}$$

where

$$\delta(z) = \max_{0 \leq k \leq T(z)} \|d_k(z)\|. \tag{43}$$

The straightforward bound (42) seems, however, near optimal (Fig. 4). The graphs in Fig. 5 make it sensible to conjecture that the functions ρ and δ satisfy the asymptotic inequality

$$\limsup_{\|z\| \to +\infty} \log_{\|z\|} \delta(z) \leq 1/2,$$

which, from the fact that

$$2|\sin(\pi\nu T(z))|\,\|z\| = \|(A^{T(z)} - I_2)z\| = \|d_{T(z)}(z)\| \leq \delta(z).$$

should imply

$$\limsup_{\|z\| \to +\infty} \log_{\|z\|} |\sin(\pi\nu T(z))| \leq -1/2.$$

Some elementary properties of the deviation range are summarized in the following proposition.

Proposition 4.1 *Let d_k, $D_k{}^\circ$ and $C_k(z)$ be given by (39), (41), and (9), respectively. The following holds:*

(i) $\qquad d_k(z) = \sum_{t=0}^{k-1} A^{k-1-t} B c_t(z) \qquad B = \begin{bmatrix} p^{-n} \\ 0 \end{bmatrix}$

(ii) $\qquad \overset{\circ}{D}_k = -\overset{\circ}{D}_k$

(iii) $\qquad \# D_k = p^{nk}$

(iv) $\qquad D_{k+1} = D_k + A^k B \Pi \qquad D_0 = \{0\}.$

Some remarks are in place. From (i), we have that d_k inherits the $\mathcal{M}_k$-periodicity from the map C_k. Part (ii) says that the k-th deviation range D_k is centrally symmetric, while (iv) says the the sets (40) form an increasing sequence (here the symbol '$+$' denotes the Minkowski sum of sets).

Below, we shall study geometric properties of the deviation range, using probabilistic considerations. We shall derive expressions for the barycentre and the inertia tensor of the the deviation range (proposition 4.2), and characterize its asymptotic growth rate (proposition 4.3 and theorem 1).

In preparation, we say that a set $\Omega \subset \mathbb{Z}^2$ is *k-complete* if its elements constitute a complete set of representatives for the set $\mathbb{Z}^2/\mathcal{M}_k$. Equivalently, Ω is k-complete if the map $C_k|_\Omega : \Omega \to \Pi^k$ (or the map $d_k|_\Omega : \Omega \to D_k$) is bijective. This property is invariant under translation: if Ω is k-complete then so is the set $\Omega + z = \{w + z : w \in \Omega\}$ for every $z \in \mathbb{Z}^2$.

It is easy to see that if ω is a random vector distributed uniformly on a k-complete set, then the entries of the vector $C_k(\omega)$ are independent Bernoulli random variables distributed uniformly on Π, and $d_k(\omega)$ is a random vector distributed uniformly on D_k.

4.1 Barycentre and inertia tensor of deviation range

Let $(\xi_t)_{t\in\mathbb{Z}_+}$ be a sequence of independent Bernoulli random variables distributed uniformly on the set (6). The common expectation and variance of these are

$$\mathbf{E}\,\xi_0 = \langle\Pi\rangle = \frac{p^n - 1}{2}, \qquad \mathbf{Var}\,\xi_0 = \mathbf{E}\,(\overset{\circ}{\xi}_0)^2 = \frac{p^{2n} - 1}{12}, \tag{44}$$

where $\xi^\circ = \xi - \mathbf{E}\,\xi$ denotes the result of centring a random variable or vector ξ. Similarly to proposition 4.1 (i), for every $k \in \mathbb{N}$, define a two-dimensional random vector η_k by

$$\eta_k = \sum_{t=0}^{k-1} A^{k-1-t} B \xi_t. \tag{45}$$

Note that η_k is uniformly distributed on the set D_k defined in (40) as is the random vector $\sum_{t=0}^{k-1} A^t B \xi_t$ (since $(\xi_t)_{0\le t<k}$ remains uniformly distributed on Π^k under any deterministic permutation of its entries).

Proposition 4.2 *The expectation and covariance matrix of the random vector (45) are representable as*

$$\begin{aligned} \mathbf{E}\,\eta_k &= \langle D_k\rangle = \mu(A^k - I_2)\,\mathbf{1}_2, && (46)\\ \mathbf{Cov}\,\eta_k &= \mathbf{E}\,(\overset{\circ}{\eta}_k(\overset{\circ}{\eta}_k)') = k\,\Sigma + O(1), && (47) \end{aligned}$$

where

$$\mu = \frac{p^n - 1}{2(q - 2p^n)}, \tag{48}$$

$$\Sigma = \frac{1 - p^{-2n}}{24} R^{-1}, \qquad R = \begin{bmatrix} 1 & -\alpha/2 \\ -\alpha/2 & 1 \end{bmatrix} \tag{49}$$

Here, $\mathbf{1}_r$ *denote the* r*-dimensional column-vector consisting of ones, respectively, and* $O(1)$ *is a bounded matrix-valued function of* $k \in \mathbb{N}$*.*

As (46) shows, the barycentre $\langle D_k \rangle$ moves along the ellipse $\{w \in \mathbb{R}^2 : \ \|w + \mu \mathbf{1}_2\| = |\mu| \, \|\mathbf{1}_2\|\}$ centred at $-\mu \mathbf{1}_2$ and passing through the origin. The covariance matrix $\mathbf{Cov}\, \eta_k$ can be interpreted as the inertia tensor of a unit mass distributed uniformly over the centred deviation range, defined in (41). From (47) and (49), it follows that

$$\lim_{k \to +\infty} \left(\frac{1}{k} \mathbf{E} \, \| \overset{\circ}{\eta}_k \|^2 \right) = \mathrm{Tr}\, (R\Sigma) = \frac{1 - p^{-2n}}{12},$$

where $\mathrm{Tr}\,(\,\cdot\,)$ denotes the trace of a matrix. The finiteness of $\sup_{k \in \mathbb{N}} \mathbf{E} \, \|k^{-1/2} \, \eta_k{}^{\circ} \, \|^2$ implies the uniform integrability [26] of the random sequence $(k^{-1/2} \, \eta_k{}^{\circ})_{k \in \mathbb{N}}$.

4.2 Asymptotic growth rate of deviation range

Proposition 4.3 *The convex hull* $\mathbf{co}\,(D_k)$ *of the set (40) is a polygon with* $2k$ *vertices whose asymptotic behaviour satisfies*

$$\mathbf{dist}\, (k^{-1} \mathbf{co}\, (\overset{\circ}{D}_k), \, G) \to 0 \qquad \text{as } k \to +\infty, \tag{50}$$

where $\mathbf{dist}\,(\,\cdot, \cdot\,)$ *denotes the Hausdorff distance between sets, and*

$$G = \{w \in \mathbb{R}^2 : \ \|w\| \leq (1 - p^{-n})/\pi\}. \tag{51}$$

As was shown in the previous section (cf. equation (46)), $\langle D_k \rangle = O(1)$, and hence, proposition 4.3 implies that

$$k^{-1} \max_{w \in D_k} \|w\| \to \frac{1 - p^{-n}}{\pi} \quad \text{as } k \to +\infty. \tag{52}$$

At the same time, the random sequence $(\eta_k)_{k\in\mathbb{N}}$ satisfies the strong law of large numbers, so that $\frac{1}{k}\eta_k \to 0$ almost surely as $k \to +\infty$. Indeed, the random vectors $\sum_{t=1}^{k-1}(t^{-1}A^{-t}B\,\xi_t{}^\circ)$ form a square integrable martingale which is almost surely convergent by the Doob theorem [16]. Therefore, by the Kronecker lemma,

$$k^{-1}\sum_{t=0}^{k-1} A^{-t}B\,\overset{\circ}{\xi}_t \to 0$$

with probability one. It now remains to notice that

$$\|\,\overset{\circ}{\eta}_k\,\| = \left\|\sum_{t=0}^{k-1} A^{-t}B\,\overset{\circ}{\xi}_t\right\|.$$

This shows that for large k, the fraction of those points $w \in D_k$, for which $\|w\|/k$ is close to the limit on the right of (52), is negligibly small. Moreover, proposition 4.2 indicates that "typical" values of the norm $\|\cdot\|$ on the set D_k should be of order $\sqrt{k}$. This qualitative comparison will be refined in the next section.

4.3 Central limit theorem

Theorem 1 *The normalised random vector $k^{-1/2}\,\eta_k{}^\circ$ is asymptotically Gaussian distributed with zero mean and covariance matrix Σ defined by (49), in the sense that*

$$\lim_{k\to+\infty}\mathbf{E}\,f(k^{-1/2}\,\overset{\circ}{\eta}_k) = \frac{1}{2\pi\sqrt{\det\Sigma}}\int_{\mathbb{R}^2} f(u)\exp\left(-\frac{1}{2}u'\Sigma^{-1}u\right)du \qquad (53)$$

for any function $f:\mathbb{R}^2\to\mathbb{R}$ whose discontinuity set is of two-dimensional Lebesgue measure zero and for which the integral on the right exists.

Since $\mathbf{E}\,\eta_k = O(1)$, theorem 1 applies to the random vector $k^{-1/2}\eta_k$ as well. In particular, the random variable

$$\rho_k^2 = \frac{1}{k}|\Sigma^{-1/2}\eta_k|^2 = \frac{24}{k\,(1-p^{-2n})}\|\eta_k\|^2 \qquad (54)$$

is asymptotically distributed according to the χ^2-law with two degrees of freedom which coincides with the exponential distribution,

$$\lim_{k\to+\infty}\mathbf{P}(\rho_k > a) = \exp(-a^2/2) \qquad \text{for all } a \geq 0, \qquad (55)$$

where $\mathbf{P}(\,\cdot\,)$ denotes the probability of an event. Theorem 1 implies the following asymptotic geometric property of the deviation ranges (40) under appropriate scaling. For any Jordan measurable set $J \subset \mathbb{R}^2$ (a bounded set whose boundary has two-dimensional Lebesgue measure zero)

$$p^{-nk}\#(J \bigcap (k^{-1/2}D_k)) \to \frac{1}{2\pi\sqrt{\det\Sigma}}\int_J \exp(-\frac{1}{2}w'\Sigma^{-1}w)dw \qquad \text{as } k \to +\infty$$

In particular, (54) and (55) read

$$p^{-nk}\#\left\{w \in D_k : \ \|w\| \le \sqrt{\frac{(1-p^{-2n})k}{24}}\,a\right\} \to 1 - \exp(-a^2/2) \qquad \text{as } k \to +\infty. \tag{56}$$

4.4 Numerical experiments

A long cycle $z_0, \ldots, z_{T-1} \in \mathbb{Z}^2$ of the roundoff map, with (remote) initial condition z_0 and (large) period T, forms a rich probability space where the points of the orbit play the role of primary outcomes. Considered on this set, the maps c_k constitute a strictly stationary random sequence, whose one-dimensional empirical distribution (along the cycle) is close to the uniform one on the set Π. If, hypothetically, the set $\{z_t : \ 0 \le t < T\}$ were k-complete (with $k = \log_{p^n} T$), then, the k-code map C_k would be uniformly distributed on Π^k, with the k-th deviation map d_k following Theorem 1 for large k.

In spite of the fact that the cycles are never organised in such a simple manner, the numerical experiment described below shows that the empirical distribution of d_k behaves in accordance with the central limit theorem (at least as far as the first two moments are concerned), for k much greater than the logarithm of the period, which is what one would expect from euristic considerations.

Consider the empirical means and covariance matrices of the deviation maps (39), computed as a time-average over an individual cycle

$$\mathbf{E}_e d_k = \frac{1}{T}\sum_{t=0}^{T-1} d_k(z_t), \tag{57}$$

$$\mathbf{Cov}_e d_k = \mathbf{E}_e(d_k - \mathbf{E}_e d_k)(d_k - \mathbf{E}_e d_k)', \tag{58}$$

where $\mathbf{E}_e(\,\cdot\,)$ denotes the operator of empirical expectation (time-average over a single cycle). Notice that the diagonal entries of the matrices (58) satisfy the identity

$$(\mathbf{E}_e d_{k+1})_{22} = (\mathbf{E}_e d_k)_{11}$$

for all $k \in \mathbb{N}$. Using Proposition 4.1(i) and following the proof of Proposition 4.2, we obtain

$$\mathbf{E}_e d_k = \sum_{m=0}^{k-1} A^{k-1-m} B \mathbf{E}_e c_m = (A^k - I_2)(A - I_2)^{-1} B \mathbf{E}_e c_0,$$

where we have used the property that the average

$$\mathbf{E}_e c_m = \frac{1}{T}\sum_{t=0}^{T-1} c_m(z_t) = \frac{1}{T}\sum_{t=0}^{T-1} c_0(z_t) = \frac{1}{T}\sum_{t=0}^{T-1} c_t(z_0) = \mathbf{E}_e c_0$$

is independent of m due to the T-periodicity of the corresponding coding sequence. Hence, if the average $\mathbf{E}_e c_0$ is close to $\langle \Pi \rangle = (p^n - 1)/2$, then $\mathbf{E}_e d_k$ in (57) is close to $\mathbf{E}\,\eta_k$ in (46) uniformly in k.

The analysis of (58) is more complicated and less complete. Again, using Proposition 4.1(i) and the line of the proof of Proposition 4.2, we have

$$\begin{aligned}
\mathbf{Cov}_e d_k &= \sum_{s,t=0}^{k-1} A^s BB'(A^t)'\,\Theta_{s-t} \\
&= \Theta_0 \sum_{t=0}^{k-1} A^t BB'(A^t)' + \sum_{0 \le s,t<k:\ s \ne t} A^s BB'(A^t)'\,\Theta_{s-t}
\end{aligned} \tag{59}$$

where

$$\Theta_t = \mathbf{Cov}_e(c_0, c_t) = \mathbf{E}_e(c_0 - \mathbf{E}_e c_0)(c_t - \mathbf{E}_e c_0)'$$

is the empirical covariance function for the coding sequence. Notice that Θ_t is even (that is, $\Theta_{-t} = \Theta_t$) and T-periodic in $t \in \mathbb{Z}$ with $\sum_{t=0}^{T-1} \Theta_t = 0$. From the proof of Proposition 4.2, it is easy to extract the following asymptotically linear evolution for the first sum on the right of (59),

$$\begin{aligned}
\sum_{t=0}^{k-1} A^t BB'(A^t)' &= k\frac{12}{p^{2n} - 1}\Sigma + O(1) \\
&= \frac{k}{2p^{2n} - q^2/2}\begin{bmatrix} 1 & \alpha/2 \\ \alpha/2 & 1 \end{bmatrix} + O(1).
\end{aligned}$$

There is a characteristic transient time $\mathcal{T}_1$ needed for this last asymptotics to settle, which is independent of the particular cycle considered. On the other hand, as long as the empirical correlation coefficients Θ_t/Θ_0 of the coding sequence are close to zero, the double sum on the right of (59) remains small compared to the first term up to another characteristic time $\mathcal{T}_2$, which is cycle-dependent. For $k > \mathcal{T}_2$, the double sum saturates, leading to a breakdown of such linear evolution. Thus, for $\mathcal{T}_1 < k < \mathcal{T}_2$, the empirical covariance matrix $\mathbf{E}_e d_k$ is proportional to $k\Sigma$ with high accuracy, and the proximity of the scalar proportionality factor to 1 is determined by that of Θ_0 to the variance $(p^{2n}-1)/12$ of the uniform distribution on the set Π.

As an example, we have calculated the empirical covariance matrices of the deviation maps for the cycle of the roundoff map in the dyadic case $q/p^n = 1/2$, with initial condition $z_0 = (10^4, 0)$ and period $T = 64366$. For this cycle,

$$\mathbf{E}_e c_0 = 0.50402\ldots,$$

which is 0.8% close to the limiting value 1/2. Hence, as discussed above, $\mathbf{E}_e d_k$ automatically reproduces $\mathbf{E}_e \eta_k$ with high accuracy uniformly in $k \in \mathbb{N}$.

Calculation of the empirical variance of the coding sequence for the same cycle yielded

$$\Theta_0 = 0.2499838\cdots,$$

which is 0.0065% close to 1/4, the variance of the uniform distribution on $\{0, 1\}$. (Such accuracy is explained by noting that, for the chosen parameters, $\Theta_0 = 1/4 - (\mathbf{E}_e c_0 - 1/2)^2$.) The correlation function Θ_t/Θ_0, $1 \leq t < T$, is plotted in Fig. 6. It appears to be strongly oscillating in t. The figure also displays the empirical distribution function for the correlation coefficients, which shows that an overwhelming majority (more than 90%) of them do not exceed 0.01 in absolute value. This last circumstance is apparently responsible for the subtle cancellation of the double sum on the right of (59), as discussed above and as Fig. 7 demonstrates. The figure shows that, for the cycle under consideration, the breakdown of the linear evolution for the covariances of the deviation maps d_k predicted by Proposition 4.2 happens for $k > \mathcal{T}_2 \sim T/2$. However, estimating (indeed, defining!) the critical time $\mathcal{T}_2$ is a delicate problem, which requires further investigation.

5 Appendix: Proofs

5.1 Proposition 4.1

Proof. The proof of (i) proceeds by induction on $k \in \mathbb{N}$. The basis of induction follows immediately from the definitions (13), (39) and (7) by which

$$d_1(z) = Az - \Phi(z) = Bc_0(z). \tag{60}$$

Suppose that the assertion (i) holds for some $k \in \mathbb{N}$. Rewrite the $(k+1)$-st deviation map as

$$\begin{aligned} d_{k+1}(z) &= A^{k+1}z - \Phi(\Phi^k(z)) \\ &= A^{k+1}z - (A\Phi^k(z) - Bc_0(\Phi^k(z))) \\ &= Ad_k(z) + Bc_k(z) = \sum_{t=0}^{k} A^{k-t}Bc_t(z), \end{aligned}$$

where we have used (60) along with the equality $c_0(\Phi^k(z)) = c_k(z)$. This completes the inductive step.

The assertion (i) easily implies that the k-th deviation range D_k is obtained by a linear transformation over the set Π^k,

$$D_k = \left[\ A^{k-1}B \,\middle|\, \ldots \,\middle|\, B\ \right] \Pi^k. \tag{61}$$

(the t-th column of the $(2 \times k)$-matrix of this transformation is $A^{k-t}B$). Hence, D_k inherits the central symmetry about its barycentre claimed in (ii) from a similar property of the set Π^k which in turn follows from the symmetry of Π about its barycentre $(p^n - 1)/2$. Also, the representation (61) implies the recursions

$$D_{k+1} = AD_k + B\Pi = D_k + A^k B\Pi,$$

of which the last is the content of the assertion (iv).

The assertion (iii) follows from the special structure of the matrix A. Namely, one shows by induction that for any $k \in \mathbb{N}$, the $(1,1)$-th entry $(A^k)_{11}$ of the matrix A^k can be represented as q_k/p^{nk} where $q_k \in \mathbb{Z} \setminus \{0\}$ is not divisible by p. Now assume that $\#D_k < p^{nk}$ for some $k \in \mathbb{N}$. This implies that there exist two distinct collections $c_0, \dots, c_{k-1}$ and $c'_0, \dots, c'_{k-1}$ of numbers from Π satisfying

$$\sum_{t=0}^{k-1} A^t \begin{bmatrix} 1 \\ 0 \end{bmatrix} (c_t - c'_t) = 0.$$

Rewrite the first entry of the two-dimensional vector on the left of the last equality as

$$q_m p^{-nm}(c_m - c'_m) + \sum_{t=0}^{m-1} q_t p^{-nt}(c_t - c'_t) = 0, \tag{62}$$

where $m = \max\{0 \le t < k : \; c_t \ne c'_t\}$. Note that $c_m - c'_m$ is nonzero and not divisible by p. Hence, the first term on the left of (62) belongs to $(p^{-nm}\mathbb{Z}) \setminus (p^{-n(m-1)}\mathbb{Z})$. On the other hand, the second term on the left of (62) belongs to $p^{-n(m-1)}\mathbb{Z}$. Consequently, the terms can not yield zero sum. The contradiction shows that $\#D_k = p^{nk}$, thereby completing the proof of (iii).

Notice that we have in fact established a stronger property than the one stated in (iii): not only the set D_k itself but also its projection to the x-axis consists of p^{nk} pairwise distinct points.

5.2 Proposition 4.2

Proof. We shall use the following representation for the matrix (13)

$$A = VUV^{-1}, \tag{63}$$

where U is an orthogonal matrix and V is a matrix of eigen-vectors of A,

$$U = \begin{bmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{bmatrix}, \qquad V = \begin{bmatrix} r_- & -r_+ \\ r_- & r_+ \end{bmatrix}, \qquad r_\pm = \frac{1}{\sqrt{2 \pm \alpha}}, \tag{64}$$

with $\gamma = 2\pi\nu$. The scalar product and the corresponding Euclidean norm

$$\langle u, v \rangle = u' R v, \qquad \|u\| = \sqrt{\langle u, u \rangle}, \qquad R = (VV')^{-1}$$

(R was defined in (49)) satisfy the invariance $\langle Au, Av \rangle = \langle u, v \rangle$ for all $u, v \in \mathbb{R}^2$.

By the first of the equalities in (44) and by $\sum_{t=0}^{k-1} A^t = (A^k - I_2)(A - I_2)^{-1}$, the expectation of η_k (or equivalently, the barycentre of the k-th deviation range) is computed as

$$\begin{aligned}
\mathbf{E}\,\eta_k &= \langle D_k \rangle = \sum_{t=0}^{k-1} A^t B\,\mathbf{E}\,\xi_0 \\
&= \frac{p^n - 1}{2}(A^k - I_2)(A - I_2)^{-1}B.
\end{aligned}$$

One easily verifies that this last expression coincides with (46) since, by the notation (48),

$$\frac{p^n - 1}{2}\,(A - I_2)^{-1}B = \mu\,\mathbf{1}_2.$$

Now prove (47). Using the independence of the random variables ξ_t along with the second of the equalities (44) and recalling the representation (63)–(64), we obtain

$$\mathbf{Cov}\,\eta_k = \frac{p^{2n} - 1}{12}\sum_{t=0}^{k-1} A^t BB'(A^t)' = \frac{p^{2n} - 1}{12}\,V\sum_{t=0}^{k-1} U^t F U^{-t} V', \tag{65}$$

where

$$F = V^{-1}BB'(V^{-1})'. \tag{66}$$

A straightforward computation, using the well-known asymptotic equalities

$$\sum_{t=0}^{k-1}(\cos(\gamma t))^2 = \frac{k}{2} + O(1),$$

$$\sum_{t=0}^{k-1}(\sin(\gamma t))^2 = \frac{k}{2} + O(1),$$

$$\sum_{t=0}^{k-1}\cos(\gamma t)\sin(\gamma t) = O(1)$$

for the case where the rotation number $\nu = \gamma/2\pi$ is irrational, shows that

$$\sum_{t=0}^{k-1} U^t F U^{-t} = \frac{k}{2}\mathrm{Tr}\,F + O(1). \tag{67}$$

Noticing from (66) that $\operatorname{Tr} F = |V^{-1}B|^2 = \|B\|^2 = p^{-2n}$, and combining (65) with (67), we obtain

$$\mathbf{Cov}\,\eta_k = \frac{p^{2n}-1}{12}\frac{k}{2}p^{-2n}VV' + O(1) = k\frac{1-p^{-2n}}{24}R^{-1} + O(1),$$

which, taking into account (49), coincides with (47), thereby completing the proof. $\square$

5.3 Proposition 4.3

Proof. Let $S(\,\cdot, W) : \mathbb{R}^2 \to \mathbb{R}$ denote the support function of a compact set $W \subset \mathbb{R}^2$, in the sense of the invariant scalar product for the original linear map Ψ

$$S(u, W) = \max_{w \in W} \langle u, w \rangle.$$

By general results from convex analysis [4, 24], the set $\mathbf{co}\,(W)$ has the same support function as W, and can be uniquely recovered from the restriction of $S(\,\cdot, W)$ to the unit ellipse $\{u \in \mathbb{R}^2 : \ \|u\| = 1\}$. Considered on the unit ellipse, the support function of the k-th centred deviation range is computed as

$$\begin{aligned} S(u, \overset{\circ}{D}_k) &= \frac{p^n-1}{2}\sum_{t=0}^{k-1} |\langle u, A^t B\rangle| \\ &= \frac{p^n-1}{2}\sum_{t=0}^{k-1} \left|(V^{-1}u)'U^t V^{-1}B\right| \\ &= \frac{p^n-1}{2}\|B\|\sum_{t=0}^{k-1} |\cos(\gamma t - \tau)| \qquad (68) \end{aligned}$$

where the vector u is uniquely determined by the angle τ counted counter clock-wise from the vector $V^{-1}B$ to $V^{-1}u$, so that

$$\cos\tau = \frac{\langle u, B\rangle}{\|B\|}, \qquad \sin\tau = \frac{\det\,[\,B, u\,]}{\det V}.$$

The function (68) is piece-wise smooth in $\tau \in [0, 2\pi)$ and, by the irrationality of the rotation number $\nu = \gamma/2\pi$, has exactly $2k$ points where it is not differentiable.

This implies that the polygon $\mathbf{co}\,(D_k)$ has $2k$ sides. Since the sequence $(\{\nu t\})_{t\in\mathbb{Z}_+}$ is asymptotically uniformly distributed over $[0,1)$, we obtain that

$$\lim_{k\to+\infty} S(u, k^{-1}\overset{\circ}{D}_k) = \frac{p^n-1}{2}\|B\|\frac{1}{2\pi}\int_0^{2\pi}|\cos v|dv = \frac{1-p^{-n}}{\pi},$$

and moreover, this convergence is uniform in $u\in\mathbb{R}^2$ satisfying $\|u\|=1$. Since the right hand side of the last relationship is the support function $S(u,G)$ of the elliptic disk (51), the convergence (50) follows, thereby finalising the proof.

□

5.4 Proposition 3.3

Proof. Fix arbitrary $z\in\mathbb{Z}^2$ and $k\in\mathbb{N}$ so that k is not a period of z. From the definition (32), it follows that the code $C_{k\sigma_k(z)}(z)$ is obtained by the $\sigma_k(z)$-fold concatenation of the word $C_k(z)$. Hence, the points z and $\Phi^k(z)$ share the $k(\sigma_k(z)-1)$-code, or equivalently,

$$\Phi^k(z) - z \in \mathcal{M}_{k(\sigma_k(z)-1)}.$$

Combining this last inclusion with equation (39) and recalling (31) with the lower bound (35), we obtain that

$$\begin{aligned} \|\Phi^k(z)-z\| &= \|(A^k-I_2)z-d_k(z)\| \\ &\geq \Delta_{k(\sigma_k(z)-1)} \geq p^{nk(\sigma_k(z)-1)/2}. \end{aligned}$$

One verifies that for any $k\in\mathbb{Z}$ and $w\in\mathbb{R}^2$

$$\|(A^k-I_2)w\| = 2|\sin(\pi\nu k)|\,\|w\|,$$

where I_r denotes the identity matrix of order r. Consequently,

$$\sigma_k(z) \leq 1 + \frac{2}{k}\,\log_{p^n}(2|\sin(\pi\nu k)|\,\|z\| + \|d_k(z)\|). \tag{69}$$

Since $\|d_k(z)\| \leq \max_{w\in D_k}\|w\|$ uniformly in $z\in\mathbb{Z}^2$, the inequality (69) implies (36), thereby completing the proof of the proposition.

□

5.5 Proposition 3.4

Proof. Let $n_0, \ldots, n_s$ be arbitrary positive integers, and let $\{\Omega_k : \ 0 \le k \le s\}$, be a partition of the alphabet Ω, satisfying $\#\Omega_k = n_k$. The total number of such partitions is

$$\prod_{k=0}^{s} \binom{r - n_0 - \ldots - n_{k-1}}{n_k} = \frac{r!}{\prod_{k=0}^{s} n_k!}, \tag{70}$$

where $\binom{r}{m}$ is the binomial coefficient, and the first of the equalities (37) is used. Assume that such a partitioning is fixed, but otherwise arbitrary. Consider all those words of length s over the alphabet Ω in which every symbol $w \in \Omega_k$ is represented exactly k times for all $0 \le k \le s$. The total number of such words is

$$\prod_{k=1}^{s} \prod_{j=0}^{n_k - 1} \binom{s - \sum_{m=1}^{k-1} m n_m - jk}{k} = \frac{s!}{\prod_{k=0}^{s} (k!)^{n_k}} \tag{71}$$

and completely determined by the cardinality structure of the partitioning, where the second of the equalities (37) has been used. Hence, the product of (70) and (71) divided by $\#(\Omega^s) = r^s$ is the probability of the random event in (38). $\square$

5.6 Proposition 3.5

Proof. Consider the z-transform of the joint distribution of $\nu_{r,s}(k), \ 0 \le k \le s$, defined as the function $\Psi_{r,s} : \mathbb{C}^{s+1} \to \mathbb{C}$ by

$$\Psi_{r,s}(z_0, \ldots, z_s) = \mathbf{E} \prod_{k=0}^{s} z_k^{\nu_{r,s}(k)}. \tag{72}$$

This is a polynomial in $(s+1)$ complex variables $z_0, \ldots, z_s$. From (38), it is straightforward to obtain that

$$\begin{aligned} \Psi_{r,s}(z_0, \ldots, z_s) &= \frac{r!\, s!}{r^s} \sum_{n_0, \ldots, n_s \in \mathbb{Z}_+ \text{ satisfying } (37)} \prod_{k=0}^{s} \frac{(z_k/k!)^{n_k}}{n_k!} \\ &= r^{-s} \frac{\partial^{r+s}}{\partial u^r \partial v^s} \exp\left(u \sum_{k=0}^{s} \frac{v^k z_k}{k!} \right) \Bigg|_{u=v=0} \end{aligned}$$

$$= r^{-s} \frac{\partial^s}{\partial v^s} \left(\sum_{k=0}^{s} \frac{v^k z_k}{k!} \right)^r \Bigg|_{v=0} . \tag{73}$$

Correspondingly, for any given $0 \le k \le s$, the z-transform of the marginal distribution of the k-th random variable $\nu_{r,s}(k)$ is computed as

$$\begin{aligned}
\mathbf{E}\, z^{\nu_{r,s}(k)} &= \Psi_{r,s}(\underbrace{1, \ldots, 1}_{k \text{ times}}, z, \underbrace{1, \ldots, 1}_{s-k \text{ times}}) \\
&= r^{-s} \frac{\partial^s}{\partial v^s} \left(\frac{v^k}{k!}(z-1) + \sum_{m=0}^{s} \frac{v^m}{m!} \right)^r \Bigg|_{v=0}, \qquad z \in \mathbb{C}.
\end{aligned}$$

This allows for computing the moments of $\nu_{r,s}(k)$. We shall restrict ourselves to the first two. The following identity will be used,

$$\frac{\partial^t}{\partial v^t} \left(\sum_{m=0}^{s} \frac{v^m}{m!} \right)^r \Bigg|_{v=0} = r^t$$

which holds for all $r, s, t \in \mathbb{Z}_+$ satisfying $t \le s$. The expectation of $\nu_{r,s}(k)$ is

$$\begin{aligned}
\mathbf{E}\, \nu_{r,s}(k) &= \frac{\partial \mathbf{E}\, z^{\nu_{r,s}(k)}}{\partial z} \Bigg|_{z=1} \\
&= r^{1-s} \frac{\partial^s}{\partial v^s} \left(\frac{v^k}{k!} \left(\sum_{m=0}^{s} \frac{v^m}{m!} \right)^{r-1} \right) \Bigg|_{v=0} \\
&= r^{1-s} \binom{s}{k} \frac{\partial^{s-k}}{\partial v^{s-k}} \left(\sum_{m=0}^{s} \frac{v^m}{m!} \right)^{r-1} \Bigg|_{v=0} \\
&= r^{1-s} \binom{s}{k} (r-1)^{s-k}.
\end{aligned} \tag{74}$$

Similarly,

$$\begin{aligned}
\mathbf{E}\, \nu_{r,s}(k)(\nu_{r,s}(k)-1) &= \frac{\partial^2 \mathbf{E}\, z^{\nu_{r,s}(k)}}{\partial z^2} \Bigg|_{z=1} \\
&= r^{1-s}(r-1) \frac{\partial^s}{\partial v^s} \left(\left(\frac{v^k}{k!} \right)^2 \left(\sum_{m=0}^{s} \frac{v^m}{m!} \right)^{r-2} \right) \Bigg|_{v=0}
\end{aligned}$$

$$
\begin{aligned}
&= r^{1-s}(r-1)\left(\begin{array}{c} s \\ 2k \end{array}\right)\frac{(2k)!}{(k!)^2}\,\frac{\partial^{s-2k}}{\partial v^{s-2k}}\left(\sum_{m=0}^{s}\frac{v^m}{m!}\right)^{r-2}\Bigg|_{v=0} \\
&= r^{1-s}(r-1)\left(\begin{array}{c} s \\ 2k \end{array}\right)\frac{(2k)!}{(k!)^2}(r-2)^{s-2k}. \qquad (75)
\end{aligned}
$$

Note that the right hand side of the last equality is zero if $2k > s$. Now rewriting the equality (74) in the form

$$
\mathbf{E}\,\frac{\nu_{r,s}(k)}{r} = \frac{(s/r)^k}{k!}\left(1-\frac{1}{r}\right)^{s-k}\prod_{t=0}^{k-1}\left(1-\frac{t}{s}\right)
$$

gives that for any fixed $k \in \mathbb{Z}_+$,

$$
\mathbf{E}\,\frac{\nu_{r,s}(k)}{r} \to \frac{\lambda^k}{k!}\exp(-\lambda) \qquad \text{as } r \to +\infty,\ \frac{s}{r} \to \lambda. \qquad (76)
$$

Similarly, (75) implies that

$$
\begin{aligned}
\mathbf{E}\,\frac{\nu_{r,s}(k)(\nu_{r,s}(k)-1)}{r^2} &= \left(1-\frac{1}{r}\right)\frac{(s/r)^{2k}}{(k!)^2}\left(1-\frac{2}{r}\right)^{s-2k}\prod_{t=0}^{2k-1}\left(1-\frac{t}{s}\right) \\
&\to \left(\frac{\lambda^k}{k!}\exp(-\lambda)\right)^2 \qquad \text{as } r \to +\infty,\ \frac{s}{r} \to \lambda. \qquad (77)
\end{aligned}
$$

Combining (74) with (75) yields that the variance of the normalised random variable $\nu_{r,s}(k)/r$ vanishes since

$$
\begin{aligned}
\mathbf{Var}\,\frac{\nu_{r,s}(k)}{r} &= \mathbf{E}\,\frac{\nu_{r,s}(k)(\nu_{r,s}(k)-1)}{r^2} + \frac{1}{r}\mathbf{E}\,\frac{\nu_{r,s}(k)}{r} - \left(\mathbf{E}\,\frac{\nu_{r,s}(k)}{r}\right)^2 \\
&\to 0 \qquad \text{as } r \to +\infty,\ \frac{s}{r} \to \lambda.
\end{aligned}
$$

This last convergence, together with (76), implies that

$$
\begin{aligned}
\mathbf{E}\left(\frac{\nu_{r,s}(k)}{r} - \frac{\lambda^k}{k!}\exp(-\lambda)\right)^2 &= \mathbf{Var}\,\frac{\nu_{r,s}(k)}{r} + \left(\mathbf{E}\,\frac{\nu_{r,s}(k)}{r} - \frac{\lambda^k}{k!}\exp(-\lambda)\right)^2 \\
&\to 0 \qquad \text{as } r \to +\infty,\ \frac{s}{r} \to \lambda,
\end{aligned}
$$

which completes the proof of the proposition. $\square$

5.7 Theorem 1

Proof. Denote by φ the common characteristic function of the centred random variables $\overset{\circ}{\xi_t}$ which sends $u \in \mathbb{R}$ to

$$\varphi(u) = \mathbf{E}\,\exp\left(iu\,\overset{\circ}{\xi_0}\right) = p^{-n}\exp\left(-i\frac{p^n-1}{2}u\right)\sum_{t=0}^{p^n-1}\exp(iut) = \frac{\sin(p^n u/2)}{p^n\sin(u/2)}. \quad (78)$$

Note that φ takes real values due to the aforementioned central symmetry of the set Π about its barycentre. Clearly,

$$\varphi(u) = 1 - \frac{p^{2n}-1}{24}u^2 + O(u^4) \qquad \text{as } u \to 0.$$

By the independence of ξ_t, the characteristic function ψ_k of the centred random vector $\overset{\circ}{\eta_k}$ maps $w \in \mathbb{R}^2$ to

$$\psi_k(w) = \mathbf{E}\,\exp\left(iw'\,\overset{\circ}{\eta_k}\right) = \prod_{t=0}^{k-1}\varphi(w'A^tB). \quad (79)$$

Hence, taking proposition 4.2 into account, the logarithm of the characteristic function of $k^{-1/2}\,\overset{\circ}{\eta_k}$ affords the representation

$$\begin{aligned}\ln\psi_k(k^{-1/2}w) &= \sum_{t=0}^{k-1}\ln\varphi(k^{-1/2}w'A^tB) = -\frac{1}{2k}w'\,\mathbf{Cov}\,\eta_k\,w + O(1/k)\\ &= -\frac{1}{2}w'\Sigma w + O(1/k) \qquad \text{as } k \to +\infty,\end{aligned}$$

which implies that

$$\lim_{k\to+\infty}\psi_k(k^{-1/2}w) = \exp\left(-\frac{1}{2}w'\Sigma w\right).$$

The limit on the right is the characteristic function of the two-dimensional Gaussian distribution with zero mean and covariance matrix Σ. Since this last convergence holds for every $w \in \mathbb{R}^2$, application of the well-known criterion of the weak convergence of probability measures [26] yields (53) for any bounded and continuous function $f : \mathbb{R}^2 \to \mathbb{R}$. The validity of the limit for the wider class of functions f specified in the proposition, follows from the uniform integrability of the sequence $(k^{-1/2}\,\overset{\circ}{\eta_k})_{k\in\mathbb{N}}$, which completes the proof. $\square$

References

[1] S. Albeverio and A. Khrennikov and 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] J.-P. Aubin and H. Frankowska, *Set-valued Analysis* (Birkhäuser, Boston) (1990).

[5] C. Beck and G. Roepstorff, Effects of phase space discretization on the long-time behavior of dynamical systems, *Physica D* **25** (1987) 173–180.

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

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

[8] D. Bosio, Ph.D. thesis, Queen Mary and Westfield College, University of London (2000).

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

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

[11] 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).

[12] P. Diamond and I. Vladimirov, Asymptotic independence and uniform distribution of quantization errors for spatially discretized dynamical systems, *International Journal of Bifurcation and Chaos*, **8**, 7, (1998) 1479–1490.

[13] P. Diamond and I. Vladimirov, Loss of invertibility of smooth diffeomorphisms under spatial discretization, *Numerical Functional Analysis and Optimization*, (2000) to appear.

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

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

[16] P. Hall, and C. C. Heyde, *Martingale limit theory and its application*, Academic Press, New York (1980).

[17] V. Kozyakin, N. Kuznetsov, A. Pokrovskii and I. Vladimirov, Some problems in analysis of discretizations of continuous dynamical systems, Proceedings of the Second World Congress of Nonlinear Analysts, Part 2 (Athens, 1996), *Nonlinear Analysis and Its Applications*, **30**, 2, (1997) 767–778.

[18] T. Krüger and S. Troubetzkoy, Complexity, randomness, discretization: some remarks on a program of J. Ford, *Physica D* **105** 97 (1997).

[19] N. Kuznetsov and P. Kloeden, The problem of information stability in computer studies of continuous systems, *Mathematics & Computation in Simulation*, **43**, (1997) 143–158.

[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] R.T. Rockafellar, *Convex Analysis*, Princeton University Press, Princeton, N.J., 1970.

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

[26] A. N. Shiryaev *Probability*, 2nd Edition, Springer-Verlag New York (1995).

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

[28] A. Van der Poorten, private communication.

[29] I. Vladimirov, Quantized linear systems on integer lattices: frequency-based approach I & II, CASDEM Reports **96-032, 96-033**, Centre for Applied Dynamical Systems and Environmental Modeling, Deakin University, Geelong, Victoria. (1996).

[30] Vladimirov I., Kuznetsov N., and Diamond P., Frequency measurability, algebras of quasiperiodic sets and spatial discretizations of smooth dynamical systems, *Math. Comput. Simulation*, **52** (2000), no. 3–4, 251–272.

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

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

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

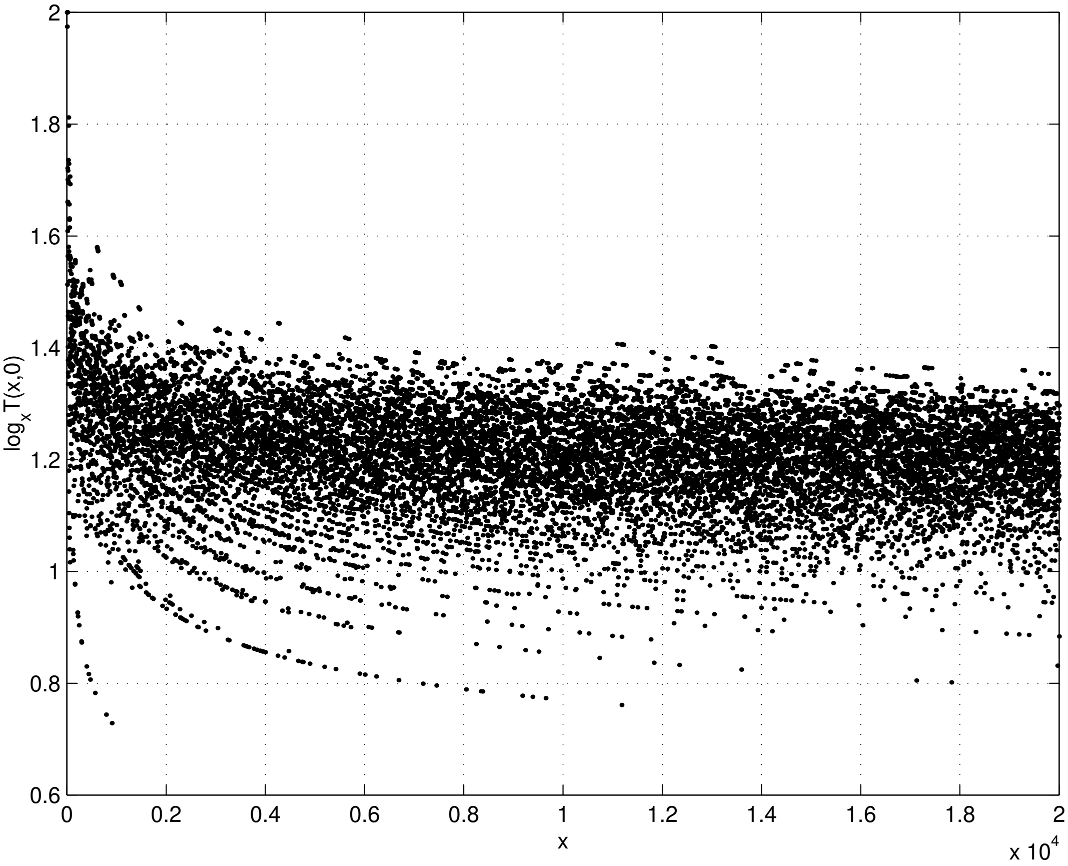


Figure 1: The period function $\log_x T(x,0)$, for x in the range $2 \leq x \leq 2 \cdot 10^4$, and parameters $q/p^n = 1/2$.

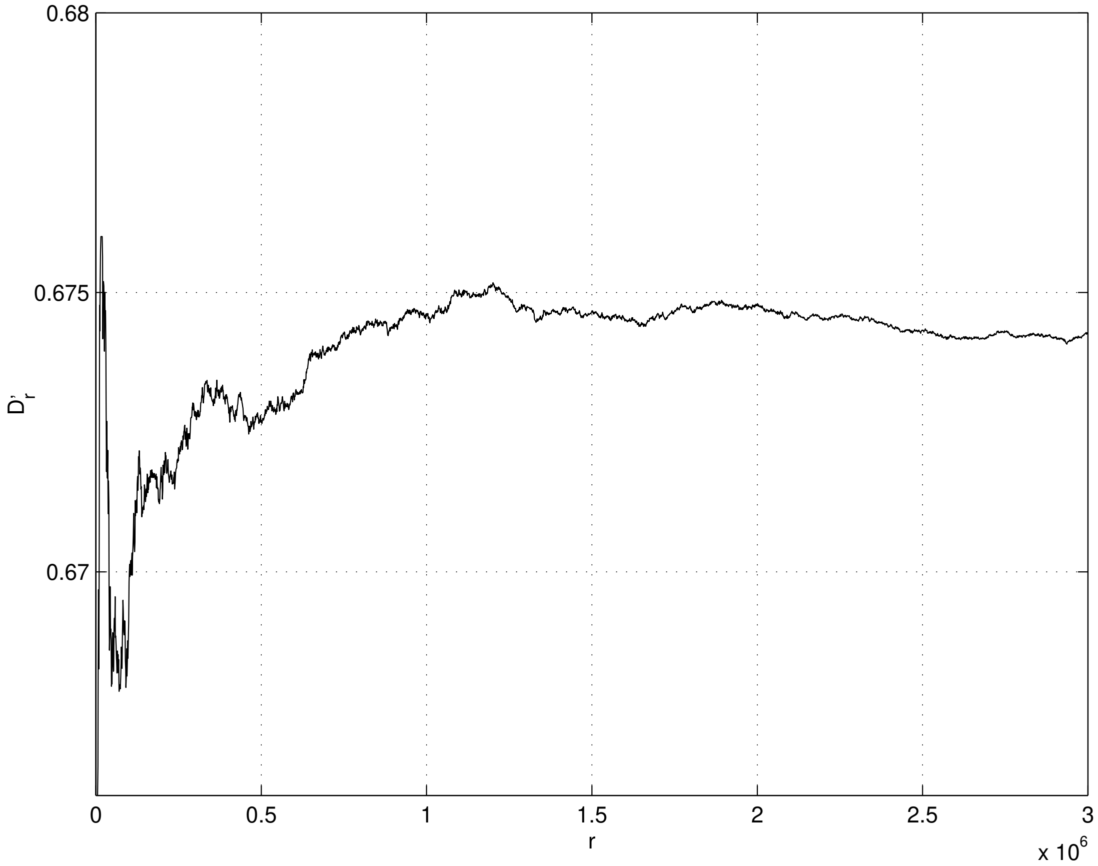


Figure 2: The density $\mathcal{D}'_r$ (equation (30)) of orbits with a point on the positive x-axis, for the dyadic case $q/p^n = 1/2$.

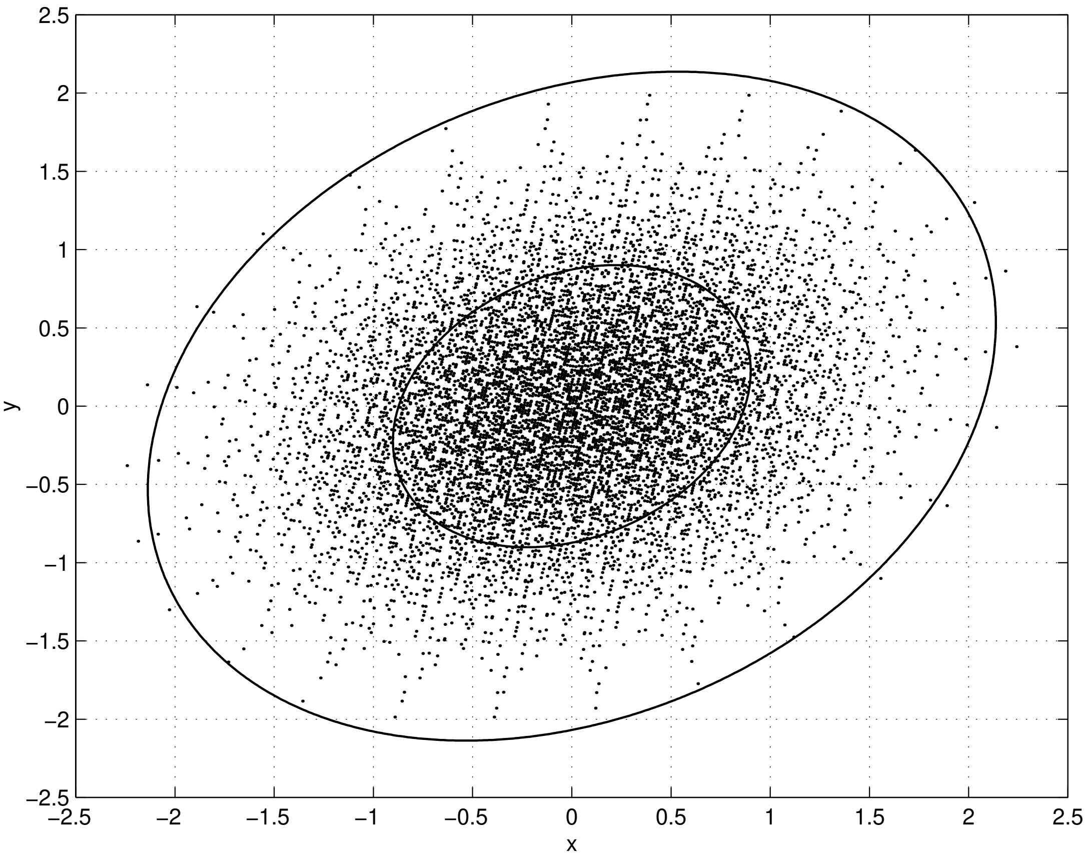


Figure 3: The 13-th centered deviation range $D_{13}{}^{\circ}$ for the dyadic case $q/p^n = 1/2$ (see section 4). The inner and outer ellipses correspond to the probabilistic and deterministic bounds, respectively, given by equation (56) with $a = 1$, and (52), respectively.

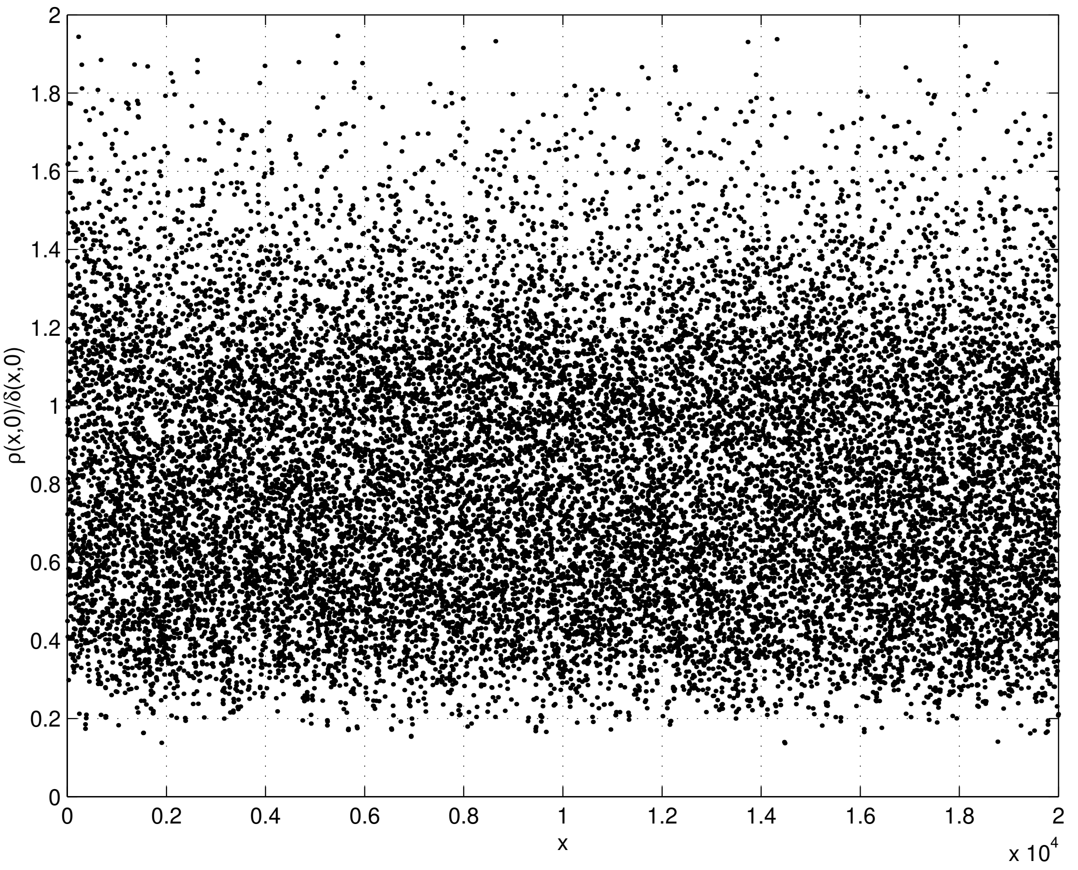


Figure 4: The ratio $\rho(x,0)/\delta(x,0)$ of the functions in (27) and (43) versus $1 \leq x \leq 2 \cdot 10^4$ for the dyadic case $q/p^n = 1/2$. The experimental upper bound is very close to the theoretical estimate (42).

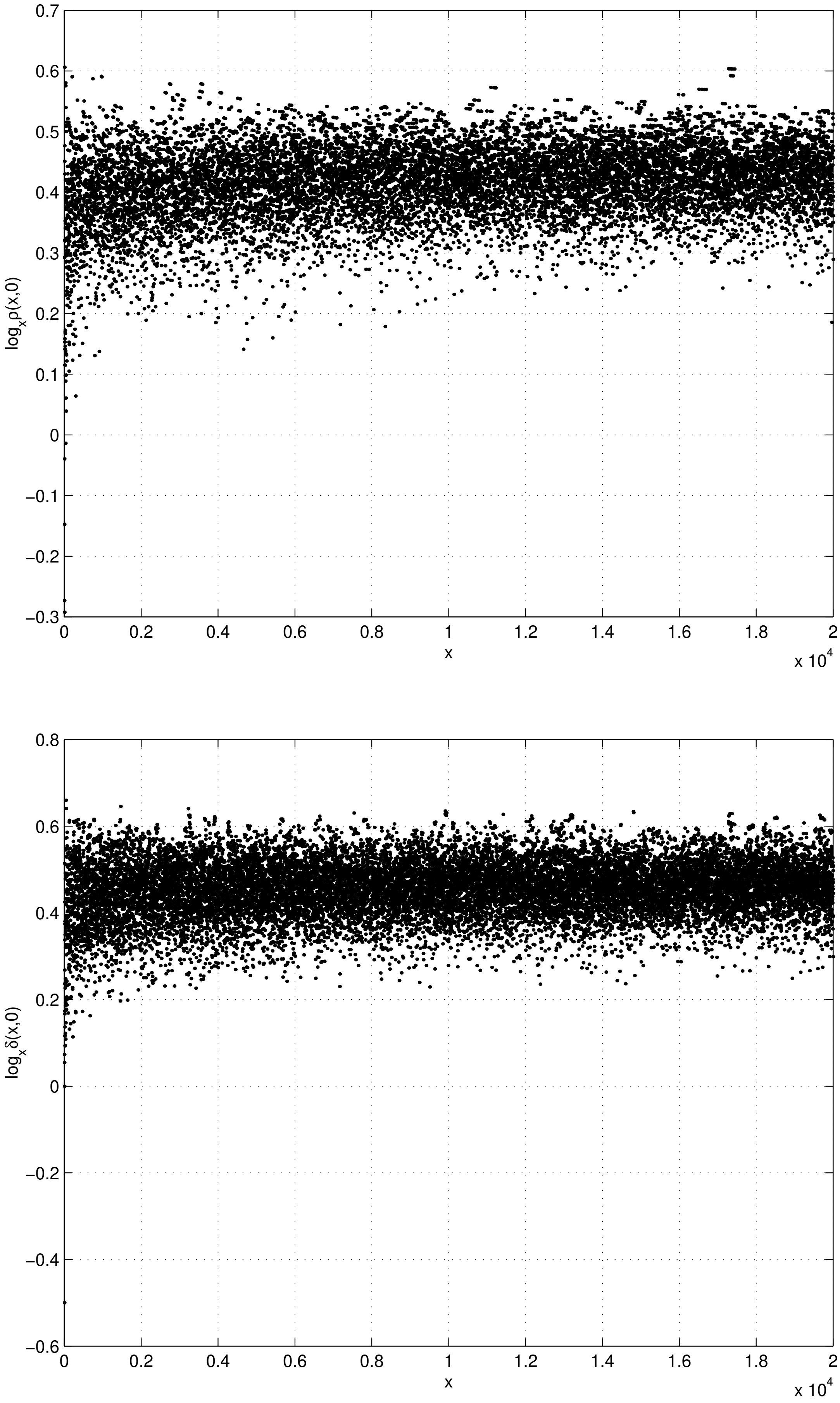
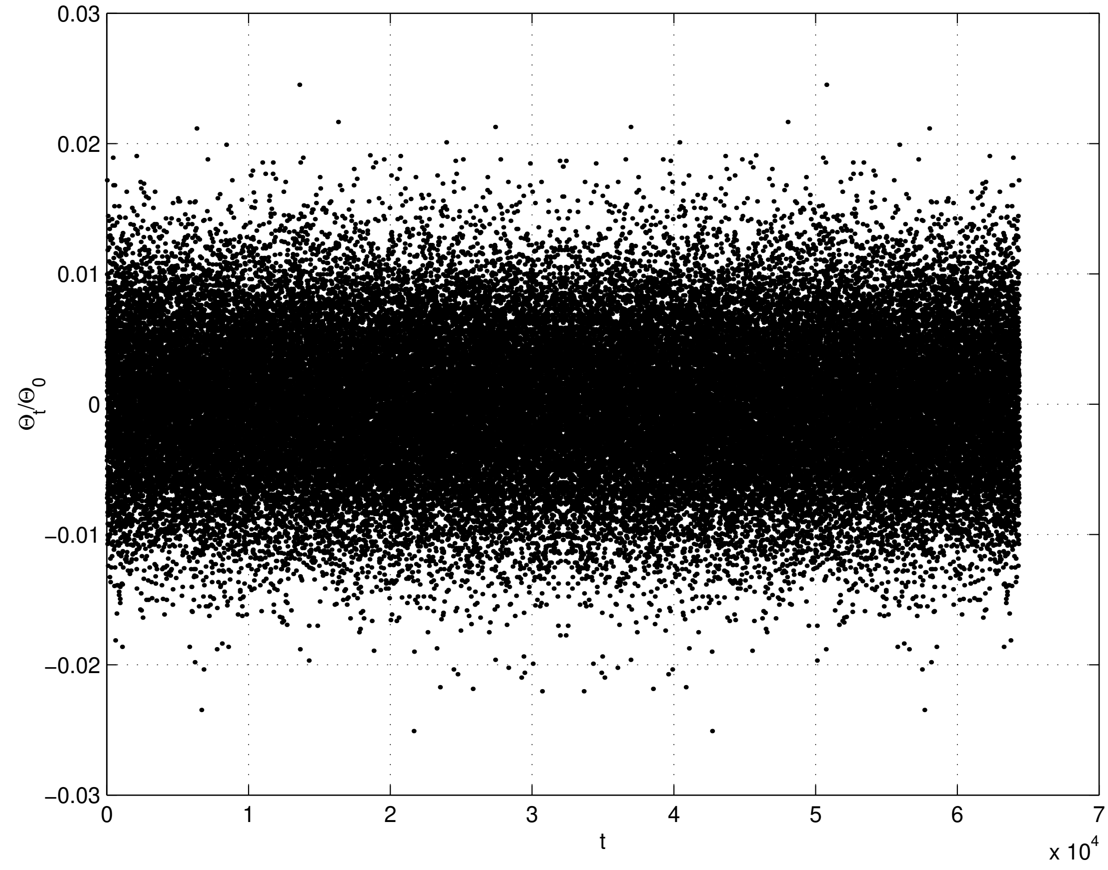


Figure 5: The logarithms $\log_x \rho(x,0)$ and $\log_x \delta(x,0)$ of the functions (27) and (43) versus $2 \leq x \leq 2 \cdot 10^4$, for the dyadic case $q/p^n = 1/2$.



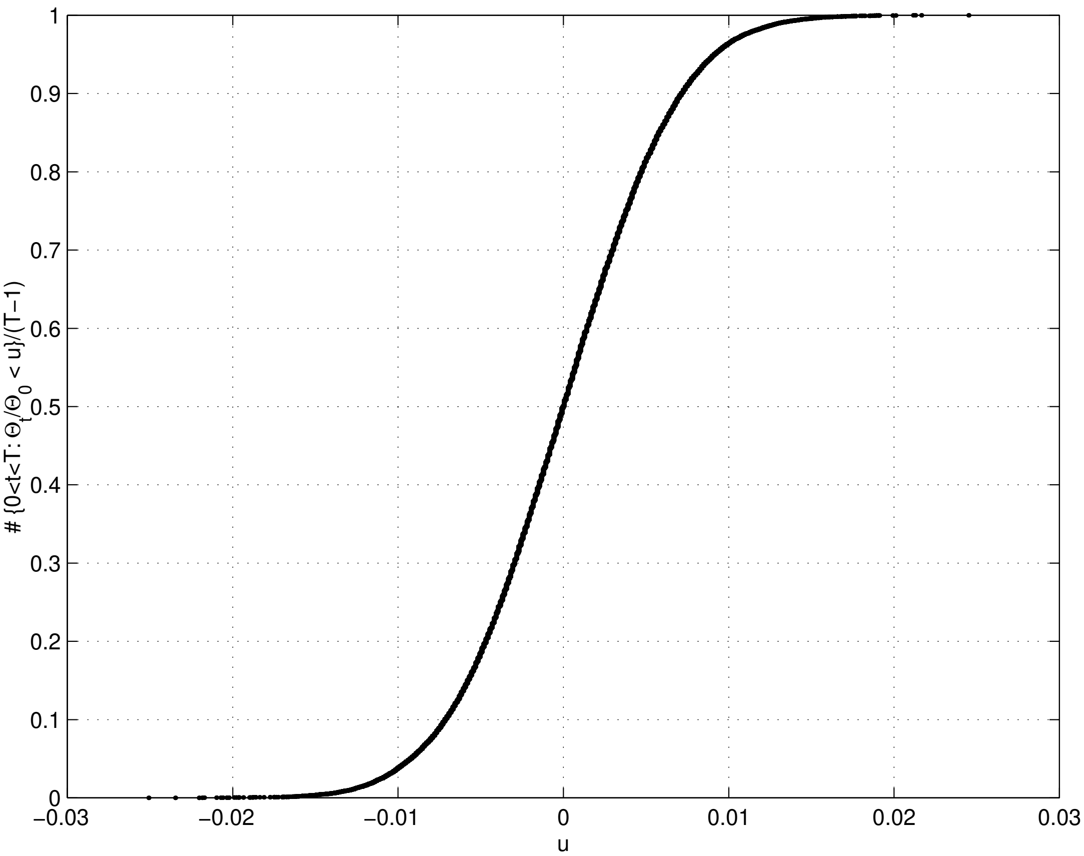


Figure 6: The correlation coefficients Θ_t/Θ_0, $1 \leq t < T$, of the coding sequence and their empirical distribution function for the cycle of the round-off map with initial condition $(10^4, 0)$ and period $T = 64366$, in the dyadic case $q/p^n = 1/2$ (see section 4.4).

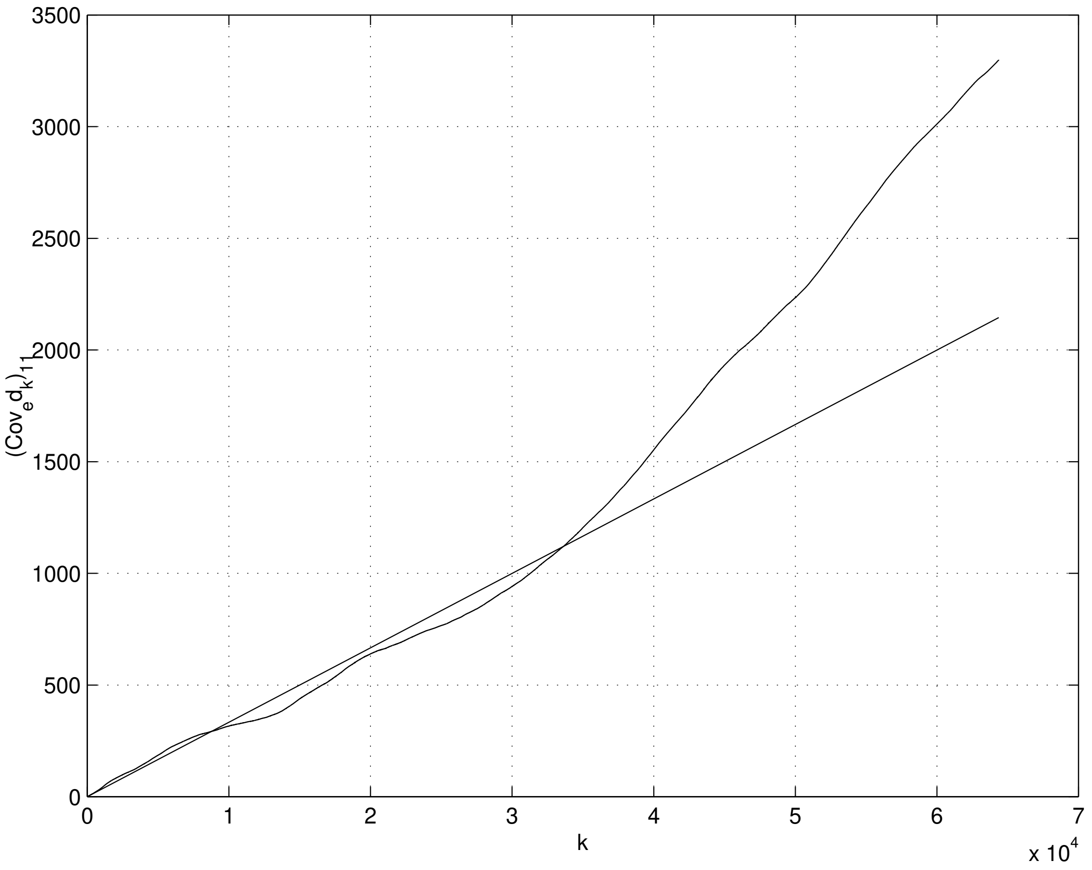


Figure 7: The $(1,1)$ entry of the empirical covariance matrices $\mathbf{Cov}_e d_k,\ \ 1 \leq k \leq T$, of the deviation maps for the cycle of the round-off map with initial condition $(10^4, 0)$, and period $T = 64366$, in the dyadic case $q/p^n = 1/2$ (see section 4.4). The straight lines correspond to the asymptotically linear evolution of the covariances computed in Proposition 4.2 under the Bernoulli hypothesis for the coding sequence.