p-adic Chaos and Random Number Generation

Christopher F. Woodcock and Nigel P. Smart

CONTENTS

We discuss the properties of p-adic analogues of the logistic and Smale horseshoe maps, and adapt them to form possible practical pseudo-random number generators. The properties of these practical modifications are studied in detail in the case p = 2.

Many people have considered chaotic maps to be a source of randomness; however, from a computational viewpoint the classical chaotic maps are not particularly suited for machine computation. Computers live in the discrete world whilst classical chaotic maps are usually defined on real manifolds. In this paper we present a possible remedy to this problem, namely a theory of chaos over the p-adic numbers.

Consider the thought experiment of performing an infinite sequence of independent throws of an unbiased die with p faces, (p a prime, most notably $p = 2$). The space of all possible outcomes, C, clearly identifies with the direct product of a countable number of copies of a discrete set with p elements. The set C carries with it a natural topology, under which it is a Cantor set. In addition C has an invariant probability measure, μ, under the shift operator $T : C \to C$ where $(T(x))_i = x_{i+1}$. More precisely, $\mu(T^{-1}(E)) = \mu(E)$ for all measurable subsets E of C (see [Taylor 1973, Chapter 7, p. 187]; note that T is not one-one).

Thus if we wish to construct an "idealised" random number generator with seed-space K, we must define an isomorphism

$$\Theta : K \to C,$$

which parametrises the outcomes of the experiment. Clearly Θ induces a mapping

Keywords: p-adic numbers, chaos theory, random numbers

1058-6458/1998 $0.50 per page

$$V : K \to K$$

corresponding to $T : C \to C$. Therefore we must construct an appropriate discrete dynamical system (K, V) equivalent to (C, T), and the dynamical system (K, V) must exhibit chaotic behaviour in that it should be sensitive to initial conditions. Clearly for ease of implementation, analysis etc. it would be helpful if V were given by a simple formula and this would be facilitated if K had some arithmetic structure and V was say a polynomial function.

The set K, like C, will be a Cantor set and so in particular it will be totally disconnected. Therefore we cannot base the arithmetic structure on $\mathbb{R}$ or $\mathbb{C}$. However, we can take K to be $\mathbb{Z}_p$, the ring of p-adic integers, or even $\mathbb{Z}_p \times \mathbb{Z}_p$ etc. Now in practice only a small selection of seeds from K, those having short descriptions in some sense, could be used. Clearly, with the above choices for K, the natural approach would be to select seeds from $\mathbb{N}$, or $\mathbb{N} \times \mathbb{N}$. Thus we must also ensure that such choices provide us with seeds in K that are generic with respect to V or pseudo random in some strong sense. In particular the seeds should not have eventually periodic orbits under V. If the resulting sequence of bits was to be used in a stream cipher we would require the additional property that it should be hard to recover the seed from knowledge of a large portion of the sequence, (at least not without the use of a considerable amount of computing power).

1. p-ADIC CHAOS

It is well known that quite simple polynomial mappings $f : \mathbb{R}^n \to \mathbb{R}^n$ in one or several real variables can give rise, via iteration, to discrete dynamical systems that exhibit chaotic behaviour in the sense that they have sensitive dependence on initial conditions and admit an invariant Cantor set, C. The action of f on C is sometimes "topologically equivalent" to the more transparent action of the usual shift operator on a space of sequences of symbols taken from a finite alphabet. This is called "symbolic dynamics"; see [Newhouse 1980], for example.

Entirely analogous behaviour can also be observed for certain p-adic polynomial mappings (for a prime p); see [Thiran et al. 1989], for example. However, there is now the unifying feature that the ring of p-adic integers, $\mathbb{Z}_p$, is both a p-adic analytic manifold and a Cantor set (unlike in the real case). This allows for a smoother transition from the analytic to the symbolic in the p-adic case.

In this paper we first introduce p-adic analogues of two of the best known "real" examples: the logistic map

$$x \to 4x(1-x)$$

and (a polynomial realisation of) the Smale horseshoe map

$$(x, y) \to (y,\ ax + by^2 + c)$$

for suitable a, b and c. The associated symbolic dynamics in each case is respectively a one-sided shift and a full shift on two symbols. This is also the case for the p-adic analogues below, except now there are p symbols rather than two.

The analogous chaotic p-adic logistic and Smale horseshoe maps will then be considered as "idealised" random number generators and "practical" modifications of them will then be analysed in some detail when $p = 2$. These practical implementations appear to display certain statistical strength and possess some interesting properties.

If p denotes a prime number, we define the p-adic logistic map to be

$$\begin{aligned} L : \mathbb{Z}_p &\to \mathbb{Z}_p \\ x &\mapsto (x^p - x)/p\,. \end{aligned}$$

Note that $(x^p - x)/p \in \mathbb{Z}_p$ by Fermat's Small Theorem and when $p = 2$ we obtain a map reminiscent of the "standard" logistic map $x \to cx(1-x)$, where c is some constant.

Firstly we note that L is sensitive to initial conditions in the sense that if $x, y \in \mathbb{Z}_p$ with $v_p(x - y) =$

$n \geq 1$ then $v_p(L(x) - L(y)) = n - 1$. To see this note that

$$\frac{x^p - y^p}{x - y} = x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \in p\mathbb{Z}_p$$

as $v_p(x - y) \geq 1$. Now

$$L(x) - L(y) = \frac{x - y}{p}\left(\frac{x^p - y^p}{x - y} - 1\right),$$

and hence $v_p(L(x) - L(y)) = n - 1$.

We next determine the symbolic dynamics of the discrete dynamical system $(\mathbb{Z}_p, L)$. Denote the reduction modulo p of $x \in \mathbb{Z}_p$ by $\bar{x} \in \mathbb{F}_p$, and set

$$X = \prod_{i \geq 0} (\mathbb{F}_p)_i$$

by which we mean the direct product of a countable sequence of copies of $\mathbb{F}_p$, each with the discrete topology. On X we define the continuous shift operator, $T : X \to X$, by $(T(x))_i = x_{i+1}$ for all $x = (x_i) \in X$. This is the crucial result:

Theorem 1. *There is a homeomorphism $\Phi : \mathbb{Z}_p \to X$ such that $T \circ \Phi = \Phi \circ L$.*

Proof. We define Φ by $(\Phi(z))_i = \overline{L^i(z)}$ for all $z \in \mathbb{Z}_p$ so that clearly Φ is continuous and $T \circ \Phi = \Phi \circ L$. Since $\mathbb{Z}_p$ and X are both compact Hausdorff spaces it now only remains to show that Φ is injective and has a dense image.

Let $N \geq 1$ and suppose that $x, y \in \mathbb{Z}_p$. Then $(\Phi(x))_i = (\Phi(y))_i$ for $0 \leq i \leq N - 1$ if and only if $v_p(L^i(x) - L^i(y)) \geq 1$ for $0 \leq i \leq N - 1$. But this last statement holds if and only if $v_p(x - y) \geq N$ as L is sensitive to initial conditions in the sense described above. Therefore Φ is injective and naturally induces an injective mapping

$$\Phi_N : \mathbb{Z}_p/p^N\mathbb{Z}_p \to \prod_{i=0}^{N-1} (\mathbb{F}_p)_i.$$

This mapping is surjective for each $N \geq 1$ as both sides have order p^N and so Φ has a dense image in X. $\square$

A more constructive proof of the surjectivity of Φ can be obtained using Hensel's Lemma; however, we will not make use of this construction.

From the above theorem we see that the dynamical systems $(\mathbb{Z}_p, L)$ and (X, T) are topologically conjugate, which means that many properties of $(\mathbb{Z}_p, L)$ can be read off directly from the more transparent (but equivalent) symbolic representation (X, T). In particular:

(i) The periodic (or eventually periodic) points under L form a countable dense set in $\mathbb{Z}_p$. For each $N \geq 1$ there are precisely p^N points of period dividing N. These periodic points are repulsive and comprise a complete set of coset representatives for $p^N\mathbb{Z}_p$ in $\mathbb{Z}_p$.

(ii) The non-periodic (or not eventually periodic) points form an uncountable dense subset of $\mathbb{Z}_p$ and indeed there exists a dense orbit.

(iii) For each $N \geq 1$ and $x \in \mathbb{Z}_p$, the set $\{L^{-N}(x)\}$ consists of a complete set of coset representatives for $p^N\mathbb{Z}_p$ in $\mathbb{Z}_p$.

(iv) The map L preserves the Haar measure on $\mathbb{Z}_p$ (in the sense that $m(L^{-1}(E)) = m(E)$ for all measurable subsets E of $\mathbb{Z}_p$; note that from the proof of Theorem 1 above Φ induces the bijection Φ_N and so carries the Haar measure m on $\mathbb{Z}_p$ into the standard shift invariant probability measure μ on X.)

(v) Each $x \in \mathbb{N}^{>3}$ is not eventually periodic.

As the map L is then a chaotic map from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ we could use it as a theoretical way of generating "random" elements of $\mathbb{F}_p$. We start with an initial random seed $x_0 \in \mathbb{N}^{>3}$, compute $x_i = L^i(x_0)$ and then the "random" elements of $\mathbb{F}_p$ can be chosen to be $\overline{x_i}$. This seems to be an idea worth investigating due to the repulsive nature of the periodic points and the fact that elements of $\mathbb{N}^{>3}$ give rise to sequences that are not eventually periodic.

We now define the p-adic Smale horseshoe map to be

$$\begin{array}{rcl} S : \mathbb{Z}_p^2 & \to & \mathbb{Z}_p^2 \\ (x, y) & \mapsto & (y, x + L(y)); \end{array}$$

see [Newhouse 1980, pp. 17–18] for the analogous construction over the real numbers. Analogues of the Smale horseshoe map in the p-adic numbers have been considered before in [Arrowsmith and Vivaldi 1993]; however, the above is a more suitable analogue in this context.

We first observe that S is a homeomorphism with inverse $S^{-1}(x,y) = (y - L(x), x)$. Note that what we have here is a "kneading map" [Lagarias 1990]. That the Smale horseshoe map is a kneading map could lead one to consider its use possibly in Feistel type ciphers given the dual nature of S and S^{-1}. We shall not pursue this line of enquiry further in this paper.

If $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ and $m \in \mathbb{Z}$ then we put

$$(x_m, y_m) = S^m(x,y).$$

The map S is hyperbolic in the sense that the almost constant Jacobian matrix of S at each point has eigenvalues, $\lambda_1, \lambda_2 \in \mathbb{Q}_p$, with $\lambda_1\lambda_2 = -1$ and $v_p(\lambda_1) = -1$, $v_p(\lambda_2) = 1$. More concretely, suppose that $(x,y), (x^*, y^*) \in \mathbb{Z}_p \times \mathbb{Z}_p$ with $v_p(x - x^*) = m \geq 1$ and $v_p(y - y^*) = n \geq 1$, (we allow for the possibility that m or n is infinity). Then, using that L is sensitive to initial conditions, we easily obtain that S, S^{-1} are sensitive to initial conditions:

(i) $v_p(x_1 - x_1^*) = n$ and $v_p(y_1 - y_1^*) \geq \min(m, n-1)$ with equality if $m \geq n$.
(ii) $v_p(y_{-1} - y_{-1}^*) = m$ and $v_p(x_{-1} - x_{-1}^*) \geq \min(m-1, n)$ with equality if $m \leq n$.

Thus by recursion it follows that if $m \geq n$ then $v_p(y_n - y_n^*) = 0$ while if $m \leq n$ then $v_p(x_{-m} - x_{-m}^*) = 0$ and so in any case $(x,y), (x^*, y^*)$ can be separated modulo p on applying a suitable S^r (for some integer r).

We next determine the symbolic dynamics of the discrete dynamical system $(\mathbb{Z}_p \times \mathbb{Z}_p, S)$. Put

$$Y = \prod_{i \in \mathbb{Z}} (\mathbb{F}_p)_i$$

and define the shift operator $T : Y \to Y$ by putting $(T(x))_i = x_{i+1}$ for all $x = (x_i) \in Y$. With this definition we note that T is a homeomorphism. Then we will show below (in Theorem 2) that $(\mathbb{Z}_p \times \mathbb{Z}_p, S)$ is topologically conjugate to (Y, T), in other words there is a homeomorphism $\Psi : \mathbb{Z}_p \times \mathbb{Z}_p \to Y$ such that $\Psi \circ S = T \circ \Psi$.

As in the case of the p-adic logistic map we will thus be able to read off the main properties about $(\mathbb{Z}_p \times \mathbb{Z}_p, S)$ directly from its symbolic representation, (Y, T), which is now a full p-shift rather than a one-sided p-shift.

(i) Just as in the case of the logistic map, the periodic points of S form a countable dense set of points in $\mathbb{Z}_p \times \mathbb{Z}_p$. For each $N \geq 1$ there are precisely p^N points of period dividing N. In this case the periodic points are not repulsive but exhibit expansive and contracting features in different directions.
(ii) The non-periodic points form an uncountable dense subset of $\mathbb{Z}_p \times \mathbb{Z}_p$. In addition there exists a dense orbit.
(iii) The map S preserves the Haar measure on the space $\mathbb{Z}_p \times \mathbb{Z}_p$. (Note that from the proof of Theorem 2 below Ψ induces the bijection Ψ_N and so carries the Haar measure $m(x) \times m(y)$ on $\mathbb{Z}_p \times \mathbb{Z}_p$ to the standard shift invariant measure μ on Y. Alternatively this can be seen directly from the definition of S since the Haar measure $m(x) \times m(y)$ is invariant under interchange of variables x, y and the Haar measure $m(x)$ on the first factor $\mathbb{Z}_p$ is translation invariant.)
(iv) Every element $(x,y) \in \mathbb{N}^{>0} \times \mathbb{N}^{>0} \setminus \{(1,1)\}$ is non-periodic.

Now all that remains is to prove that $(\mathbb{Z}_p \times \mathbb{Z}_p, S)$ and (Y, T) are topologically conjugate.

Theorem 2. *There is a homeomorphism* $\Psi : \mathbb{Z}_p \times \mathbb{Z}_p \to Y$ *such that* $\Psi \circ S = T \circ \Psi$.

Proof. We set

$$(\Psi(x,y))_i = \bar{x}_i$$

for all $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ so that clearly Ψ is continuous and $\Psi \circ S = T \circ \Psi$. Just as in the previous case of the logistic map all that is left is to show that Ψ is injective and has a dense image.

Let $N \geq 1$ and suppose that $(x,y),(x^*,y^*) \in \mathbb{Z}_p \times \mathbb{Z}_p$. Then as S, S^{-1} are sensitive to the initial conditions we deduce that

$$(\Psi(x,y))_i = (\Psi(x^*,y^*))_i \quad \text{for } -N+1 \leq i \leq N$$

if and only if

$$v_p(x-x^*) \geq N \quad \text{and} \quad v_p(y-y^*) \geq N.$$

Therefore Ψ is injective and naturally induces an injective mapping

$$\Psi_N : \mathbb{Z}_p/p^N\mathbb{Z}_p \times \mathbb{Z}_p/p^N\mathbb{Z}_p \to \prod_{i=-N+1}^{N} (\mathbb{F}_p)_i.$$

The domain and codomain of this map both have order p^{2N} and so Ψ_N is surjective. This then implies that Ψ has a dense image in Y as required. $\square$

2. A FINITE APPROXIMATION

Clearly if we wish to compute the chaotic sequences

$$x_i = L(x_{i-1}) \text{ or } (x_i, y_i) = S(x_{i-1}, y_{i-1})$$

in a computer then the initial starting points, x_0 or (x_0, y_0), would have to be chosen in $\mathbb{Z}_p \cap \mathbb{Z} = \mathbb{Z}$, as a computer cannot represent a general p-adic integer to arbitrary accuracy. This should not present a problem for our sequence of elements of $\mathbb{F}_p$, $b_i = \overline{x_i}$. If the initial starting point is truly a random element of $\mathbb{Z}$, (resp. $\mathbb{Z}^2$), then the resulting sequence of elements of $\mathbb{F}_p$ should behave chaotically and would then look "random" to an observer.

However, the size of the integers involved increases with every step we take along our sequence. In general it will take p-times as long to compute the next element of $\mathbb{F}_p$ as it did the current one. One way to overcome this is to work to some fixed level of p-adic precision, rather like one does in the real case, for example

$$x'_i = L(x'_{i-1}) \pmod{p^e} \text{ and } b'_i = \overline{x'_i},$$

or respectively

$$(x'_i, y'_i) = S(x'_{i-1}, y'_{i-1}) \pmod{p^e} \text{ and } b'_i = \overline{x'_i}.$$

Unfortunately the resulting sequence will no longer be chaotic, indeed it is ultimately periodic. However, the first e elements of the sequence, (b'_i), will be the same as the first e elements of the sequence (b_i) and so if e is large enough this may be sufficient for our application.

For the rest of this section we shall concentrate on the logistic map in the case $p = 2$ and $e \geq 3$ (we would expect to obtain similar results to the ones below for the Smale horseshoe map). In this case we prove that the resulting logistic map has a remarkable structure, and is likely to possess a very large orbit. The first choice we have to make is for a set of coset representatives for $\mathbb{Z}/2^e\mathbb{Z}$. We shall choose as our set of coset representatives $X_e = \{1, 2, 3, \ldots, 2^e\}$ and then our logistic map becomes the map

$$\begin{array}{rcl} L_e : X_e & \to & X_e \\ x & \mapsto & (x(x-1)/2) \pmod{2^e}. \end{array}$$

Our first result is the following:

Lemma 3. *With the choice of coset representatives X_e above, the map L_e is a permutation of X_e.*

Proof. We clearly need only show that L_e is an injective map so suppose that $x, y \in X_e$ and $L_e(x) = L_e(y)$. Then we must have $(x-y)(x+y-1) \equiv 0 \pmod{2^{e+1}}$. If x and y have the same parity then $x - y \equiv 0 \pmod{2^{e+1}}$ and so $x = y$. If, however, x and y have opposite parity then $x + y - 1 \equiv 0 \pmod{2^{e+1}}$, which is clearly impossible if we choose $x, y \in X_e$. $\square$

We can also prove the following:

Theorem 4. *As a permutation of X_e the map L_e is even.*

Proof. Let ζ denote a primitive 2^e-th root of unity in $\mathbb{C}$, and let x^* denote the involution on X_e given by

$$x \to x^* = 2^e + 1 - x.$$

For all $x \in X_e$ we have $\zeta^{L_e(x)} = \zeta^{x(x-1)/2}$, $\zeta^{x^*} = \zeta^{1-x}$ and $\zeta^{L_e(x^*)} = -\zeta^{L_e(x)}$. The sign of L_e as a permutation is then given by

$$\sigma = \prod_{1\le i<j\le 2^e} \frac{\zeta^{L_e(i)} - \zeta^{L_e(j)}}{\zeta^i - \zeta^j}.$$

Using the above involution and some rather messy algebra one can then show that $\sigma = 1$. Due to space constraints we leave the details to the reader. □

It turns out that as e increases we obtain longer and longer cycles, as the next theorem demonstrates, in a very weak way.

Theorem 5. *Given $r \in \mathbb{N}$ and $\varepsilon > 0$ there exists an $N_0 \in \mathbb{N}$ such that for all $e \ge N_0$ the fraction of x in X_e lying in a cycle of length greater than r is greater than $1 - \varepsilon$.*

Proof. Let $1 \le r \le e-1$ and let $x \in X_e$ with $L_e^r(x) = x$. Suppose that $y \in X_e$ with $y \ne x$ and $2^r | x - y$. Then there is an s such that 2^s exactly divides $x - y$ with $r \le s \le e-1$. Hence 2^{s-1} divides $L_e(x) - L_e(y)$ and by recursion 2^{s-r} divides $L_e^r(x) - L_e^r(y) = x - L_e^r(y)$. Thus $L_e^r(y) \ne y$. Hence $\bigl|\{x \in X_e : L_e^r(x) = x\}\bigr| \le 2^r$, and so

$$\bigl|\{x\in X_e : L_e^m(x) = x \text{ for some } m \text{ with } 1\le m\le r\}\bigr| \le \sum_{m=1}^{r} 2^m < 2^{r+1}.$$

Therefore

$$\frac{\bigl|\{x \in X_e : x \text{ lies in a cycle of length} > r\}\bigr|}{|X_e|} > (2^e - 2^{r+1})/2^e = 1 - 2^{r+1-e}.$$

The result follows on choosing $N_0 = r + 1 - \log_2(\varepsilon)$. □

We computed for various values of e the maximum period and the expected period for the map L_e. For values of $e \le 19$ these were computed accurately; however, for $e \ge 20$ the values were determined using a Monte-Carlo simulation method of computing the cycle lengths generated from a random seed pulled out of X_e. The values of the expected and maximum cycle lengths were then normalized by dividing the result by 2^e. Our results are summarized in Table 1.

e	exp.	max.	e	exp.	max.
3	0.8203	0.8750	15	0.3918	0.5579
4	0.3303	0.3750	16	0.5337	0.7044
5	0.4016	0.5312	17	0.3453	0.4723
6	0.4806	0.6406	18	0.6372	0.7875
7	0.3943	0.4531	19	0.7874	0.8857
8	0.4933	0.5664	20	0.58	0.7379
9	0.3320	0.5351	21	0.33	0.4380
10	0.2269	0.2754	22	0.36	0.4216
11	0.4103	0.5839	23	0.47	0.6395
12	0.3523	0.4497	24	0.53	0.7258
13	0.4604	0.6399	25	0.94	0.9712
14	0.5622	0.7268	26	0.59	0.7380

TABLE 1. Normalized cycle lengths for the finite logistic map (exp. = expected, max. = maximum).

As the table demonstrates, we have a good chance of obtaining a large cycle for a randomly chosen seed. Thus our theorem above appears to be far too pessimistic and it would be nice to obtain a more accurate result. In the next section we detail a heuristic reason why we believe one to exist.

It is interesting to note that Golomb [1964] empirically discovered that the normalised expected maximum cycle length of a random permutation on n-symbols tended to $0.62432\ldots$ as n tended to infinity, a result proved by Shepp and Lloyd [1966]. Hence our normalized expected cycle lengths appear to be quite good when compared to what one would expect from a random permutation on X_e.

3. PERIODIC POINTS FOR L_e

For each $x \in \mathbb{Z}_2$ we let $\mathrm{red}_e(x)$ denote the unique element of X_e such that $x \equiv \mathrm{red}_e(x) \pmod{2^e}$. In what follows a periodic point of X_e will mean a point periodic with respect to the map L_e, whilst a periodic point of $\mathbb{Z}_2$ will mean a point periodic with respect to the map L.

Condition ($\dagger_e$)

An element $x \in \mathbb{Z}_2$ is said to satisfy condition ($\dagger_e$) if

$$\mathrm{red}_{e+1}(x) = \mathrm{red}_e(x).$$

Thus the set

$$Z = \{x \in \mathbb{Z}_2 : x \text{ satisfies condition } (\dagger_e)\}$$

has Haar measure $\frac{1}{2}$ and is the union of 2^e of the 2^{e+1} cosets of $2^{e+1}\mathbb{Z}_2$ in $\mathbb{Z}_2$. The set Z is also "well distributed" in the sense that one coset of $2^{e+1}\mathbb{Z}_2$ in Z is contained in each of the cosets of $2^e\mathbb{Z}_2$ in $\mathbb{Z}_2$. Our main result of this section links the periodic points of L_e to the periodic points of the map $L : \mathbb{Z}_2 \to \mathbb{Z}_2$.

Theorem 6. *There is a one to one correspondence between the points $y \in X_e$ of exact period k, for $1 \le k \le 2^e$, and the periodic points $x \in \mathbb{Z}_2$ of exact period k such that if $0 \le i \le k-1$ then*

1. *$L^i(x)$ satisfies condition ($\dagger_e$) and*
2. *if $L^i(x) \equiv x \pmod{2^e}$ then $i = 0$.*

Proof. Suppose that $y \in X_e$ has exact period k so that $L_e^k(y) = y$ and $L_e^l(y) \ne y$ for $1 \le l \le k-1$. Then by the symbolic dynamics for L there is a unique $x \in \mathbb{Z}_2$ with $L^m(x) \equiv L_e^m(y) \pmod 2$ for all $m \ge 0$. Now since L is sensitive to initial conditions we obtain successively

$$L^r(L_e^m(y)) \equiv L_e^r(L_e^m(y)) \pmod{2^{e-r+1}}$$

for $0 \le r \le e$. Therefore

$$\begin{aligned} L^r(L^m(x)) = L^{r+m}(x) &\equiv L_e^{r+m}(y) \\ &\equiv L_e^r(L_e^m(y)) \equiv L^r(L_e^m(y)) \pmod 2 \end{aligned}$$

for $0 \le r \le e$ and so

$$L^m(x) \equiv L_e^m(y) \pmod{2^{e+1}}$$

for all $m \ge 0$. Hence x is clearly a periodic point of exact period k satisfying the conditions of the theorem and $\mathrm{red}_e(x) = y$.

Conversely, suppose that $x \in \mathbb{Z}_2$ is a periodic point of exact period k satisfying the conditions of the theorem. Put $y = \mathrm{red}_e(x) \in X_e$. Then $L^k(x) = x$, $L^l(x) \not\equiv x \pmod{2^e}$ for $1 \le l \le k-1$ and $\mathrm{red}_{e+1}(L^m(x)) = \mathrm{red}_e(L^m(x)) \in X_e$ for all $m \ge 0$. Hence

$$\begin{aligned} L_e(\mathrm{red}_e(L^m(x))) &= L_e(\mathrm{red}_{e+1}(L^m(x))) \\ &\equiv L(\mathrm{red}_{e+1}(L^m(x)) \\ &\equiv L(L^m(x)) \equiv L^{m+1}(x) \\ &\equiv \mathrm{red}_e(L^{m+1}(x)) \pmod{2^e}. \end{aligned}$$

Therefore $L_e(\mathrm{red}_e(L^m(x)) = \mathrm{red}_e(L^{m+1}(x))$ and so $L_e^m(y) = \mathrm{red}_e(L^m(x))$ for all $m \ge 0$. Hence $y = \mathrm{red}_e(x) \in X_e$ is a periodic point of exact period k. Further $L^m(x) \equiv \mathrm{red}_e(L^m(x)) \equiv L_e^m(y) \pmod 2$ for all $m \ge 0$ and so the required one to one correspondence follows. □

Now let β_e denote the number of cycles in the cycle decomposition of L_e. Then clearly for each $R \ge 1$ the proportion of elements of X_e lying in cycles of length greater than R is at least $1 - R\beta_e/2^e$. In particular if β_e is $O(e^h)$ for some $h \ge 1$ then for each $\varepsilon \in (0,1)$ the proportion of elements of X_e lying in cycles of length greater than $2^{(1-\varepsilon)e}$ tends to one as $e \to \infty$. If we can prove that $\beta_e = O(e^h)$ then we would have greatly strengthened Theorem 5. Our numerical evidence above seems to support this assumption, as does the following heuristic argument:

Conjecture. $\beta_e = O(e)$.

Heuristic Reasoning. We first make the plausible assumption that the periodic points of $\mathbb{Z}_2$ of exact period k, with $1 \le k \le 2^e$ (which are in general solutions of polynomial equations of high degree), are "well distributed" with respect to condition ($\dagger_e$). Therefore we expect that the statement

"x satisfies the conditions of Theorem 6"

should hold with "probability" at most 2^{-k}, in some very ill defined sense. For each $k \ge 1$ there are precisely

$$A_k = \sum_{d|k} \mu(d) 2^{k/d}$$

periodic points of L of exact period k, so that $A_k \leq 2^k$. Thus the "expected" number of cycles of length k in X_e should be at most $A_k 2^{-k}/k \leq 1/k$ and the expected total number β_e of cycles for L_e will then be at most

$$\sum_{k=1}^{2^e} 1/k \leq \log(2^e) + 1 = O(e).$$

A random permutation also exhibits the property that the expected number of cycles is of the order of the logarithm of the length of the permutation; see [Goncharov 1944]. In addition our numerical investigation seemed to support the claim that $\beta_e = O(e)$.

Note for the "chaotic" map L on $\mathbb{Z}_2$ there are many periodic orbits but they have total measure zero in $\mathbb{Z}_2$. The permutation L_e of the finite set X_e may be thought of as an approximation to L in some sense, even though now of course every orbit is periodic. The mechanism described above would ensure that there are "few" cycles in the cycle decomposition of L_e and so a low proportion of elements of X_e would lie in short cycles.

Lemma 7. *The only value of e for which the cycle decomposition of X_e can contain a transposition is $e = 1$.*

Proof. There are two periodic points of L in $\mathbb{Z}_2$ of exact period 2, namely the roots of $x^2 + x + 2 = 0$. Suppose that $e \geq 1$ and x_1, x_2 are the two periodic points of exact order 2 and assume they both satisfy condition $(\dagger_e)$. Let $y_1, y_2 \in X_e$ be such that $x_i \equiv y_i \pmod{2^{e+1}}$, then

$$y_1 + y_2 = 2^{e+1} - 1$$

and so $y_1 = 2^e$ and $y_2 = 2^e - 1$, while also $y_1 y_2 \equiv 2 \pmod{2^{e+1}}$ and so $2^e \equiv 2 \pmod{2^{e+1}}$. The only way this can happen is when $e = 1$. □

4. KICKING AWAY THE SMALL ORBITS

Returning to our application to a random number generator we see that even with these large cycles existing there is the chance that the cycle obtained, from any given seed, will have a small length. It is this problem that we try to overcome in this section. One way we can overcome the small cycle problem is to periodically reseed the generator using some other map. We call this reseeding "kicking" and we shall describe the details below in the context of the Smale horseshoe map. A similar discussion could be given for the logistic map as well.

We assume we are working to a fixed modulus 2^e so our resulting stream of bits "shadows" the true chaotic stream of bits for only $2e$ of the bits. More explicitly if we know $b'_{n-e+1}, \dots, b'_{e+n}$ then we can recover (x'_n, y'_n). But the value of b'_{e+1+n} will be dependent on the noise accumulated by working modulo 2^e and may not be the output had we worked to infinite 2-adic precision.

However, one could hope that even the resulting stream, (b'_i), will be random enough. After all we could consider that after every e bits the "noise" accumulated from our rounding operation produces a "random" new initial state and so on.

Alas this is not the case. As the map S is now from X_e^2 to X_e^2, the sequence (x'_i) cannot help being eventually periodic. One way to describe what is happening is that the sequence (x'_i) "shadows" the 2-adically chaotic sequence (x_i), but with less and less accuracy due to the build up of noise. The sequence (x_i) will, with probability zero, be periodic as the periodic points of S have measure zero in $\mathbb{Z}_p \times \mathbb{Z}_p$; however, the sequence (x'_i) cannot help being periodic.

We need to occasionally perturb our map slightly so it does not fall into a small period. We do this by taking

$$\begin{aligned} S_e : X_e \times X_e &\rightarrow X_e \times X_e \\ (x, y) &\mapsto (y,\, x + L_e(y) + L_e(z)), \end{aligned}$$

where z is some random input; the point of passing z through L_e is to hide any linearity in the generator that produces z. For most of the time we set $L_e(z) = 0$, and then at random points in time we take z to come from a uniform distribution on X_e.

As we have mentioned before if the resulting stream is to be used for cryptography we not only need that the stream behaves as a random sequence but that knowledge of a long portion of the sequence does not provide knowledge of the rest of the sequence (at least without expending a huge computing effort). For our original theoretical p-adic random number generator this was no problem but for the practical version above this is a problem. Without the kicking mechanism the complete sequence could be obtained with only the knowledge of $2e$ consecutive bits of output. Hence the kicking mechanism not only reduces the chances of our bit stream falling into a period but it also makes the recovery of the seed a much harder problem.

However, an attack could perhaps use the probability of whether a kick occurs at a certain bit to deduce information about the seed. We therefore need to determine a mechanism that describes when the kicks occur and that gives negligible probabilistic information to an attacker.

After some thought we decided on the following scheme. A linear feedback shift register (LFSR) of maximal period is used to output bits that are added onto a counter. Once the counter has reached a certain threshold, T, a kick is applied and the counter reset to zero. If one is not so worried about someone recovering the seed and one only wants to avoid the problem of falling into a small period then the threshold level can be chosen to be quite high as our numerical experiments on the logistic map suggest.

If we assume the LFSR outputs bits with a uniform distribution, then the probability of a kick occurring at the n^{th} bit is given by

$$p(n) = q(n) + \sum_{i=T}^{n-T} p(i)\, q(n-i),$$

where

$$q(n) = \frac{1}{2^n}\left(\binom{n}{T} - \binom{n-1}{T}\right).$$

The expected length of time between kicks then comes out at around $2T$ and the chance of going $4T$ bits without a kick occurring is negligible.

If you graph the function $p(n)$ for some choice of T then you notice that it oscillates around $\approx 1/(2T)$ with a period of $2T$ bits. However, the amplitudes decrease over time so after a while the function appears to behave as a constant function. Hence if the output from the bit stream is used from this point onwards it appears as if no statistical properties of when the kick occurs can be used in any cryptanalysis.

In practice we decided to take $e = 32$, then all arithmetic can be done in 64 bits, which just happened to be the length of the data-type unsigned long long for our C++ compiler. We used the standard C command rand() to produce the random kicks z; however, any non-constant function seemed to be able to be used here, with no degradation of statistical properties.

This meant the key-size (or size of data needed to start the bit stream) was $(2^{32})^4 = 2^{128}$. This consisted of two 32-bit integers for (x_0, y_0), one 32-bit integer for the seed for the random number generator and one to initialise the 32-bit LFSR. In our experiments we decided to take $T = 16 = e/2$.

The resulting code produced around 150,000 bits per second on a Silicon Graphics R5000 workstation. The resulting stream of bits was tested for statistical randomness using the Frequency, Autocorrelation, Serial, Runs and Linear Complexity tests. In addition we tested the resulting streams against Maurer's Test [Maurer 1992]. Sequences of various lengths and various subsequences were tested. For every sequence and test applied the tests accepted the null hypothesis, that the sequences were indeed random, at a confidence level of ninety five percent.

REFERENCES

[Arrowsmith and Vivaldi 1993] D. K. Arrowsmith and F. Vivaldi, "Some p-adic representations of the Smale horseshoe", *Phys. Lett. A* **176**:5 (1993), 292–294.

[Golomb 1964] S. W. Golomb, "Random permutations", *Bull. Amer. Math. Soc.* **70** (1964), 747.

[Goncharov 1944] V. Goncharov, "From the domain of combinatorial analysis", *Bull. Acad. Sci. URSS, Ser. Math.* **8** (1944), 3–48. In Russian; translation in *Amer. Math. Soc. Transl.* (2) **19** (1962), 1–46.

[Lagarias 1990] J. C. Lagarias, "Pseudorandom number generators in cryptography and number theory", pp. 115–143 in *Cryptology and computational number theory* (Boulder, CO, 1989), edited by C. Pomerance, Proc. Sympos. Appl. Math. **42**, Amer. Math. Soc., Providence, RI, 1990.

[Maurer 1992] U. M. Maurer, "A universal statistical test for random bit generators", *J. Cryptology* **5**:2 (1992), 89–105.

[Newhouse 1980] S. E. Newhouse, "Lectures on dynamical systems", pp. 1–114 in *Dynamical systems* (Bressanone, 1978), edited by J. Coates and S. Helgason, Progr. Math. **8**, Birkhäuser, Boston, 1980.

[Shepp and Lloyd 1966] L. A. Shepp and S. P. Lloyd, "Ordered cycle lengths in a random permutation", *Trans. Amer. Math. Soc.* **121** (1966), 340–357.

[Taylor 1973] S. J. Taylor, *Introduction to measure and integration*, Cambridge U. Press, 1973.

[Thiran et al. 1989] E. Thiran, D. Verstegen, and J. Weyers, "p-adic dynamics", *J. Statist. Phys.* **54**:3-4 (1989), 893–913.

Christopher F. Woodcock, Institute of Mathematics and Statistics, University of Kent, Canterbury, Kent, CT2 7NF, United Kingdom (C.F.Woodcock@ukc.ac.uk)

Nigel P. Smart, Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, United Kingdom (nsma@hplb.hpl.hp.com)

Received June 9, 1997; accepted in revised form February 23, 1998