Ergod. Th. & Dynam. Sys. (1998), **18**, 321–330
Printed in the United Kingdom © *1998 Cambridge University Press*

The ghosts of the cat

EHRHARD BEHRENDS
I. Mathematisches Institut, Arnimallee 2–6, D-14195 Berlin, Germany

(*Received* 15 *February* 1996)

Abstract. Let $A \in SL(2,\mathbb{Z})$ be given and $n \in \mathbb{N}$. A induces a map A_n on $\mathbb{Z}_n^2$ by $(x, y) \mapsto (a_{11}x + a_{12}y, a_{21}x + a_{22}y)$ mod n. A_n can be thought of as a discrete approximation of the similarly defined map on the unit square. It is known that the A_n have a surprisingly small period: there always is an $r \leq 3n$ such that A_n^r is the identity on $\mathbb{Z}_n^2$.

One can visualize the properties of the iterates of A_n by considering the sets $P, A_nP, A_n^2P, \ldots$ for a fixed subset P of $\mathbb{Z}_n^2$. (Here the cat comes into play: P has often been chosen to be the digitalized picture of a cat, in particular when treating the special case of the Anosov map $A = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.) It turns out that in the sequence $(A_n^k P)_k$ mostly 'chaotic' pictures occur as one would expect. However, some kind of regular behaviour can also be observed for certain powers A_n^k before the end of the period.

It is the aim of this paper to describe these phenomena and to explain why and how they occur. In order to quantify the chaotic behaviour of the maps on $\mathbb{Z}_n^2$ under consideration, we introduce suitable functions.

Our methods are elementary. Only basic results from the geometry of numbers will be used.

1. *Introduction*

The Anosov map $(x, y) \mapsto (2x + y, x + y)$ mod 1, defined on the unit square, plays an important role in the theory of dynamical systems. The discrete variant $(x, y) \mapsto (2x + y, x + y)$ mod n on $\mathbb{Z}_n^2$ can be thought of as an approximation; it corresponds to the restriction of the Anosov map to the subset of pairs of rational numbers with denominator n.

It was observed in [**3**] that in the discrete case the periods are surprisingly small which is in marked contrast to the fact that on the square the map is ergodic. A new proof of this fact as well as the discussion of the corresponding case for arbitrary matrices in $SL(m, \mathbb{Z})$ can be found in [**1**]. The reader who is interested in more detailed information on the Anosov map and some literature concerning the importance of its discrete approximation to quantum chaos is referred to this paper.

Here we are interested in what happens before the end of the period. To illustrate the phenomena we are going to describe we will sketch the images of certain digitalized pictures with respect to the iterations of the map under consideration (all these sketches can be found in the Appendix). We will restrict ourselves to three pictures:

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

(1) a 'square' Sqr_n (the set of $(i, j) \in \mathbb{Z}_n^2$ such that $3 \leq i,\ j \leq [n/2]$);
(2) a 'cat' Cat_n (a sketch in a 16×18 rectangle);
(3) a cross Cro_n consisting of the (i, j) in $\mathbb{Z}_n^2$ such that either $i = j$ or $i + j = (n-1)$ mod n.

These can be found in Figure A1 of the Appendix for the case $n = 30$.

In Figure A2 we sketch P, $A_n P$, $A_n^2 P$, ... for the case of the Anosov map, $n = 29$, and $P = Cat_{29}$. The choice $n = 29$ is motivated by the fact that the period here is very small. One might expect that what can be seen in this case is typical in that the iterates produce patterns which tend to be more and more 'chaotic' until, after the middle of the period, they in turn become more and more 'regular' leading finally to the original pattern.

However, this is far from being true. Investigating various other examples, one finds that before the end of the period pictures occur which are by no means chaotic. It turns out that one has to distinguish two cases.

Patterns of type I. One starts with a picture like Sqr_n or Cat_n built up essentially from 'blocks' $\{(i, j) \mid i_0 \leq i \leq i_0 + r,\ j_0 \leq j \leq j_0 + r\}$, where the numbers r are not too small compared with n.

Patterns of type II. The relevant information is given by certain lines as in Cro_n.

(For simplicity we will not consider mixtures of these two cases.)

Here are the phenomena we are going to investigate.

1.1. *Phenomena in case I.* We will concentrate on the following.

1.1.1. *The clusters.* Consider, for example, the fifth iteration of Sqr_{28} with respect to the Anosov map which we will denote by $A_{28}^5(Sqr_{28})$ (Figure A3). It is not 'chaotic' but consists of a number of clusters. There are 29 of them (here and in similar cases one has to take into account the fact that we are calculating mod n so that, for example, $(i, 0)$ is adjacent to $(i, n-1)$). $A_{28}^5(Cat_{28})$ looks quite similar (Figure A4): it has the same number of clusters, and whereas the individual ones look different the pattern is the same.

Thus it is apparent that the phenomenon is caused essentially by the particular form of the map and that the initial picture is of less importance. Note, however, that $A_{28}^5(Cro_{28})$ shows no similar behaviour (Figure A5) which indicates that the distinction between case I and case II is reasonable.

The relevant map here is induced by the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)^5 \bmod 28 = \left(\begin{smallmatrix} 5 & 27 \\ 27 & 6 \end{smallmatrix}\right) =: A_{28,5}$, acting on $\mathbb{Z}_{28}^2$. We will explain in §2 why and how the particular entries of $A_{28,5}$ give rise to precisely the clusters observed.

1.1.2. *The ghosts.* This is a little bit more spectacular. As an example we have chosen the 12th iterate in the case $n = 45$. Figure A6 provides $A_{45}^{12}(Sqr_{45})$, $A_{45}^{12}(Cat_{45})$, and $A_{45}^{12}(Cro_{45})$, respectively. Whereas the first two undoubtedly are some kind of 'ghosts' of the original pattern, nothing similar can be said of the third. Therefore, as in 1.1.1

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

it only seems to be of importance whether case I applies or not. The number of ghosts (five in this example) and how they are placed is seemingly an invariant only depending on the entries of $A_{45,12} = \binom{2\ 1}{1\ 1}^{12} \bmod 45 = \binom{10\ 18}{18\ 37}$.

See §3 for a discussion.

1.2. *Phenomena in case II.* In this case very different degrees of chaotic behaviour are apparent. As an example, consider $A_{31}^{8}(Cro_{31})$ and $A_{31}^{10}(Cro_{31})$ in Figure A7. How this phenomenon can be concluded from the matrices $A_{31,8} = \binom{16\ 26}{26\ 21}$ and $A_{31,10} = \binom{3\ 7}{7\ 27}$ will be discussed in §4.

Clusters, ghosts and lines showing different degrees of chaotic behaviour were first observed in the course of computer simulations. These experiments also gave rise to various observations which now—having understood how the different patterns arise—can be explained. Here is a sample.

- If one starts with a fixed pattern P, then it is likely that in the sequence $P, AP, \ldots$ clusters (or ghosts) can be observed in a number of consecutive steps; i.e. if $A^k P$ shows clusters then $A^{k+1}P$ often does also.
- The number of clusters, if there are any, is always $\pm 1 \bmod n$.
- It is much more likely that one observes ghosts in the case of composed numbers n than in the case of prime numbers.

Whereas our illustrations always use the Anosov matrix $\binom{2\ 1}{1\ 1}$ our results apply to arbitrary $A \in SL(2, \mathbb{Z})$. §§2–4 contain, as already mentioned, mainly the necessary facts to explain the phenomena 1.1.1, 1.1.2 and 1.2 and the discussion of some consequences. Also in §5, we introduce two functions in order to have a measure of how 'chaotic' the mappings under consideration are.

2. *Clusters*

To begin with we remind the reader of an elementary fact concerning *lattices* in $\mathbb{Z}^2$. Let $x_1 = \binom{x_{11}}{x_{12}}$, $x_2 = \binom{x_{21}}{x_{22}} \in \mathbb{Z}^2$ be linearly independent and $L := \{ax_1 + bx_2 \mid a, b \in \mathbb{Z}\}$. L is called the *lattice* generated by x_1 and x_2. Crucial for that which follows will be the fact that the quotient $\mathbb{Z}^2/L$ has precisely $|\det(x_1, x_2)| = |x_{11}x_{22} - x_{21}x_{12}|$ elements. This is proved, for example, in [**2**] or [**7**].

Now let $B = \binom{b_{11}\ b_{12}}{b_{21}\ b_{22}} \in SL(2, \mathbb{Z})$ be arbitrary and suppose that there is a given pattern P in $\mathbb{Z}^2$ of type I. Suppose further that $x_1 := B^{-1}\binom{1}{0}$, $x_2 := B^{-1}\binom{0}{1}$ are small compared with P.

If x_0 and $x_0 + x_1$ are in P then, since $Bx_1 = \binom{1}{0}$, these points are mapped by B to adjacent points. The same happens with x_0 and $x_0 + x_2$, with $x_0 + x_1$ and $x_0 + x_1 + x_2$, and so on. In other words, $P \cap (x_0 + L)$ is mapped under B to a set which is a cluster as observed in phenomena 1.1.1. It is easy, but not necessary here to give this fact a more rigorous form; the necessary definitions (e.g. connectedness) for subsets of $\mathbb{Z}^2$ are provided by a theory called digital topology (see [**4**] or [**6**]).

If x_0 and $\hat{x}_0$ are such that $x_0 + L$ and $\hat{x}_0 + L$ are disjoint then B might map $P \cap (x_0 + L)$ and $P \cap (\hat{x}_0 + L)$ to sets which are not adjacent. By the result mentioned at the beginning of this section, the maximal number of points x_0 one can choose such that the associated

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

sets $x_0 + L$ are pairwise disjoint is precisely $|\det(x_0, \hat{x}_0)|$. Therefore *this* is the number of clusters in $B(P)$.

Let us now turn from $\mathbb{Z}^2$ to $\mathbb{Z}_n^2$. The idea is to apply a local version of what has been done before to the new situation. To be more precise, let $x_0 = \binom{x_{01}}{x_{02}} \in \mathbb{Z}_n^2$ be given such that $0 < x_{01}, x_{02} < n-1$. Furthermore, suppose that there are vectors $x_1 = \binom{x_{11}}{x_{12}}$, $x_2 \in \binom{x_{21}}{x_{22}} \in \mathbb{Z}^2$, such that $Bx_1 = \binom{1}{0} \bmod n$, $Bx_2 = \binom{0}{1} \bmod n$ are such that the $|x_{ij}|$, $i, j = 1, 2$, are small compared with n. Then what has been done before can now be repeated for $\{x_0 + ax_1 + bx_2 \mid a, b \in \mathbb{Z}, 0 \le x_{0i} + ax_{1i} + bx_{2i} \le n-1 \text{ for } i = 1, 2\}$. x_1 and x_2, being the inverse images under B of the unit vectors, have as components precisely the entries of the matrix B^{-1}. Since B has determinant 1 this means that, modulo n, $x_1 = \binom{b_{22}}{-b_{21}}$, $x_2 = \binom{-b_{12}}{b_{11}}$.

However, for us it is important whether in the equivalence classes of x_1 and x_2 are representatives of absolute value, small relative to n. Therefore, we introduce the following notation. For $n \in \mathbb{N}$ fixed and $x \in \mathbb{Z}$ let x^* be that number in $x + n\mathbb{Z}$ which has the smallest possible absolute value. To put it another way, x^* is the unique number in C_n such that $x = x^* \bmod n$; here

$$C_n := -\frac{n-1}{2} + \{0, \dots, n-1\} \quad \left(\text{respectively, } -\frac{n-2}{2} + \{0, \dots, n-1\}\right)$$

if n is odd (respectively, even).

(The definition depends on n, but no confusion should arise since we will never consider different n at the same time. Examples for $n = 30$ are $5^* = 5$, $28^* = -2$, $15^* = -15$.)

Summing up we arrive at the following.

PROPOSITION 1. *Let $B = \binom{b_{11}\ b_{12}}{b_{21}\ b_{22}} \in SL(2, \mathbb{Z})$ and $n \in \mathbb{Z}$ be given. Then the map $x \mapsto Bx$ mod n on $\mathbb{Z}_n^2$ maps patterns of type I to clusters if and only if the absolute values of the numbers $(b_{ij})^*$, $i, j = 1, 2$, are small compared with n. In this case there are precisely $|b_{22}^* b_{11}^* - b_{21}^* b_{12}^*|$ clusters.*

Example. Let $n = 28$ and $B = \binom{2\ 1}{1\ 1}^5$. Modulo n this is the matrix $\binom{5\ 27}{27\ 6}$ which we met in §1. We have $5^* = 5$, $6^* = 6$, $27^* = -1$ so that $|6 \cdot 5 - (-1)(-1)| = 29$ should be the number of clusters, and this is precisely what has been observed in the computer simulation.

Even more can be said. In order to describe where the clusters are located it suffices to consider vectors $y_1, \dots, y_r \in \mathbb{Z}^2$ such that any $x \in \mathbb{Z}^2$ is equivalent mod L to some y_ρ; then the clusters will be close to the points $By_1, \dots, By_r$. It is convenient to choose the y's such that they are of the form (a, b) with a, b nonnegative and small compared with n. It follows that the 'centers' of the clusters are just the $a\binom{b_{11}}{b_{21}} + b\binom{b_{21}}{b_{22}}$ for these a, b. However, b_{ij}^* are small in the case under consideration, and this means that the $a\binom{b_{11}}{b_{21}} + b\binom{b_{21}}{b_{22}}$ in $\mathbb{Z}_n^2$ generate the same pattern as the $a\binom{b_{11}^*}{b_{21}^*} + b\binom{b_{21}^*}{b_{22}^*}$ in $\mathbb{Z}^2$. This explains, for example, that in the above example (Figures A3 and A4) the clusters are lined up in such a way that the respective slopes are $-1/5$ and -6.

With our proposition at hand we are also able to explain the observations described in §1. Since $b_{ij}^* = b_{ij} \bmod n$ for every n and $\det B = 1$, we have $b_{11}^* b_{22}^* - b_{21}^* b_{12}^* = 1$

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

mod n and hence $|b_{11}^* b_{22}^* - b_{21}^* b_{12}^*|$, the number of clusters, necessarily is $+1$ or -1 mod n.

Also, if iterations $A_n, A_n^2, \ldots$ are under consideration and $B = A_n^k$ produces clusters for a particular k, then $(a_{ij}^k)^*$ are small compared with n for $i, j = 1, 2$ ($(a_{ij}^k) =$ the components of A^k). Suppose now that the components of A are small, as, for example, the case for the Anosov map. Then $(a_{ij}^{k+1})^*$ are not much larger necessarily than $(a_{ij}^k)^*$ and, since $\det A = 1$, the determinants of $((a^k)^*)_{ij}$ and $((a_{ij}^{k+1})^*)$ coincide. This explains why in the course of the iterations of a pattern clusters usually do not occur only once between more chaotic sections and why the number of clusters on these occasions remains the same.

Note, however, that the clusters associated with A^{k+1} might be more 'distorted' than those for A^k, and after further iterations these 'very distorted' clusters provide a chaotic picture.

3. *Ghosts*

Again we fix $B \in SL(2, \mathbb{Z})$ and $n \in \mathbb{N}$, and as in the previous section we at first study the map induced by B in $\mathbb{Z}^2$.

Given any pattern P, suppose that there exist linearly independent $x_1, x_2 \in \mathbb{Z}^2$ such that x_1, x_2, Bx_1, Bx_2 are all small with respect to the size of P. Let L be the lattice generated by x_1, x_2. Then, for any $x_0 \in P$, the intersection of P with $x_0 + L$ is some kind of coarse version of P. Under B this is mapped to a similar pattern, the distortion solely depends on how x_1, x_2 transform to Bx_1, Bx_2. As in the previous sections there are $|\det(x_1, x_2)|$ many sets of the form $x_0 + L$, and therefore B produces precisely this number of ghosts. The step from $\mathbb{Z}^2$ to $\mathbb{Z}_n^2$ is as in the previous section, we only state the final result.

PROPOSITION 2. *Let B and n be as above. Then $x \mapsto Bx$ mod n can produce ghosts if and only if there are linearly independent $x_1 = \binom{x_{11}}{x_{12}}$ and $x_1 = \binom{x_{21}}{x_{22}}$ in $\mathbb{Z}^2$ such that $|x_{ij}^*|$ $(i, j = 1, 2)$ as well as $|(b_{11}x_{i1} + b_{12}x_{i2})^*|$, $|(b_{21}x_{i1} + b_{22}x_{i2})^*|$ $(i = 1, 2)$ are small compared with n. In this case the number of ghosts is $|x_{11}^* x_{22}^* - x_{12}^* x_{21}^*|$.*

Note. One might have difficulties regarding $B(P \cap (x_0 + L))$ as ghosts in the special case when Bx_1, Bx_2 are modulo n vectors of the form $\binom{\varepsilon}{\delta}$, $|\varepsilon|, |\delta| \leq 1$; if, for example, Bx_1, Bx_2 modulo n are the vectors $\binom{1}{0}$ and $\binom{0}{1}$, respectively, then this corresponds to the clusters of §2. In order not to complicate the formulation of our result we prefer to think of the clusters as a degenerate case of ghosts.

Example. Consider $B = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)^{12}$ and $n = 45$ as in the introduction. We have B mod $45 = \left(\begin{smallmatrix} 10 & 18 \\ 18 & 37 \end{smallmatrix}\right)$. We investigate, for $a, b \in \mathbb{Z}$ with $|a|$, $|b|$ small, in what cases $\binom{a}{b}$ is mapped to a vector for which the *-version of the components is small. One finds that the best choice is as follows. $\binom{1}{2}$ and $\binom{2}{-1}$ are mapped under B to itself. Therefore, we choose $x_1 = \binom{1}{2}$, $x_2 = \binom{2}{-1}$, and it follows that there are $|2 \cdot 2 - 1(-1)| = 5$ ghosts as observed.

The further discussion mainly parallels that of the case of clusters. We only summarize the results.

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

- The 'pixels' by which the ghosts are sketched sit on (a translate of) the lattice generated by Bx_1, Bx_2; in the example they lie on lines with slope 2 and $-1/2$ (cf. Figure A6).
- The fact that B mod n has two fixed points with small coordinates as in the example has as a consequence that the ghosts are very similar to the original. We note that this can happen (unless B is, mod n, the identity) only if n is a composed number. For prime numbers the ghosts necessarily are a 'distorted' version of the original pattern. To illustrate this, consider as a further example the 12th iterate of the Anosov map in the case $n = 73$; $A_{73}^{12}(Cat_{73})$ can be found in Figure A8. We have $A^{12} \bmod 73 = \binom{54\ 13}{13\ 41}$, and a similar calculation as before this time leads to the choice $x_1 = \binom{2}{3}$ and $x_2 = \binom{3}{-1}$ which are mapped to $\binom{1}{3}$ and $\binom{3}{-2}$, respectively.
- Let B be the form A_n^k for a matrix A with small entries like, for example, in the Anosov case and suppose that there are x_1, x_2 for B as in Proposition 2. Then x_1, x_2 and A_n^{k+1} also satisfy the assumptions of Proposition 2. This means that there should be the same numbers of ghosts, but those associated with A_n^{k+1} can be more distorted than those produced by A_n^k.

4. *Lines*

Let n be fixed and $x \in \mathbb{Z}_n^2$, $x \neq 0$. By the *line generated by* x we mean the subset $L_x := \{mx \mid m \in \mathbb{Z}_n\} \subset \mathbb{Z}_n^2$. The collection of all L_x will be denoted by $\mathbb{L}$. If n is prime, then every L_x will have n elements, and for simplicity we will restrict our discussion to this case.

The L_x look quite different. Some are discrete approximations of ordinary lines in $\mathbb{R}^2$, others are more or less regular patterns rather than lines. In order to quantify this behaviour we introduce the following definition: $\gamma(L_x)$ is the norm of the smallest y which generates L_x, i.e. $\min\{\sqrt{y_1^{*2} + y_2^{*2}} \mid y = (y_1, y_2) \in \mathbb{Z}_n^2, L_x = L_y\}$. Then L_x looks like a line which can be used in a discrete picture, say, only if $\gamma(L_x)$ is small.

Now let $B = \binom{b_{11}\ b_{12}}{b_{21}\ b_{22}}$ be a matrix with $b_{ij} \in \mathbb{Z}_n$ and $\det B = 1$. As usual B induces a linear map on $\mathbb{Z}_n^2$ and thus on $\mathbb{L}$. Furthermore, let $P \subset \mathbb{Z}_n^2$ be a pattern of type II. Since P is built up from (translates of) lines L_x with small $\gamma(L_x)$, the image $B(P)$ will be a pattern of type II again only if the $\gamma(B(L_x))$ are also small. It is thus natural to count the $L_x \in \mathbb{L}$ with small $\gamma(L_x)$ for which $\gamma(B(L_x))$ is small too, to measure how regular or chaotic B treats type II patterns. To make this more rigorous we define, for $r \leq n$, $\chi_B(r)$ to be the cardinality of $\{L_x \mid L_x \in \mathbb{L}, \gamma(L_x) \leq \sqrt{r}, \gamma(B(L_x)) \leq \sqrt{r}\}$.

Now we are able to understand the phenomena in case II. Chaotic pictures $B(P)$ correspond to the case where for $B := A_n^k$ the function χ_B is slowly increasing (and even zero for small r) whereas more or less regular ones occur if χ_B increases faster. To illustrate this, consider the χ_B functions for the patterns of Figure A7:

- $n = 31$, $B = A_{31,8} = \binom{16\ 26}{26\ 21}$: $(\chi_B(r))_r = (0, 0, 0, 0, 4, 4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, \ldots)$
- $n = 31$, $B = A_{31,10} = \binom{3\ 7}{7\ 27}$: $(\chi_B(r))_r = (0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 8, 8, 8, 8, \ldots)$.

5. *Measures of chaotic behaviour for a map on* $\mathbb{Z}_n^2$

In view of the discussion of the previous sections, the following problems arise.

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

(1) Let $n \in \mathbb{N}$ and a matrix $B = \binom{b_{11}\ b_{12}}{b_{21}\ b_{22}}$ with $b_{ij} \in \mathbb{Z}_n$, $\det B = 1$ be given. What properties of the b_{ij} are responsible for a 'chaotic' behaviour of the mapping induced by B on $\mathbb{Z}_n^2$, i.e. under what circumstances are the $B(P)$ 'chaotic' for 'regular' pictures $P \subset \mathbb{Z}_n^2$?

(2) If $n \in \mathbb{N}$ and $A \in SL(2, \mathbb{Z})$ are given, how can one deduce from the entries of A whether in the sequence $A_n, A_n^2, A_n^3, \ldots$ there will be 'chaotic' matrices (where 'chaotic' is measured with respect to a suitable definition according to (1))?

We have no idea how to treat (2), here we will propose only some definitions concerning (1). *One possibility* has been mentioned already in §4: the function χ_B. Whereas it describes the observations properly the calculation of its values is rather cumbersome and an explicit description in terms of the b_{ij} would be useful.

Our *second definition* has patterns of type I as a starting point. We can regard B as more or less 'chaotic' if for such patterns P the image $B(P)$ fails to have or has little recognizable structure. Since the only observed 'structures' are the ghosts (and, in the degenerate case, the clusters), we can quantify the chaotic behaviour of B by calculating to what extent the assumptions of Proposition 2 in §3 are satisfied. To this end, we first introduce the *-norm $\|x_0\|_*$ of a vector $x_0 \in \mathbb{Z}_n^2$. This number is defined as $\|(x, y)\|_* := \sqrt{|x^*|^2 + |y^*|^2}$, i.e. it is the ℓ^2-Norm of the smallest vector y_0 in $\mathbb{Z}^2$ such that $x_0 = y_0 \bmod n$. In order to observe ghosts one should find linearly independent x_1, x_2 with small $\|x_1\|_*$, $\|x_2\|_*$, $\|Bx_1\|_*$, $\|Bx_2\|_*$. This will *not* happen if for all x_0 such that $\|x_0\|_* \leq r$, ($r \in \mathbb{N}$, r small compared with n) the vector Bx_0 has a large *-norm. This motivates the following definition. For $r \in \mathbb{N}$, let $\varphi_B(r) := \min\{\|B(x_0)\|_* \mid 0 < \|x_0\|_* \leq r\}$. Clearly φ_B is a decreasing function, and the chaotic behaviour of B can be seen from φ_B as follows: B will be chaotic iff φ_B attains small values only for fairly large values of r. As an example, consider the sixth, eighth and 12th iteration of the cat in the case $n = 35$ in Figure A9 which show a chaotic behaviour, ghosts and clusters, respectively.

The corresponding φ_B functions are as follows:

$$B = \binom{1\ 2}{1\ 1}^6, n = 35;$$
$$(\varphi_B(r)) = (15.03, 5.39, 5.39, 5.39, 5.39, 2.00, 2.00, 2.00, 2.00, 2.00, \ldots)$$
$$B = \binom{1\ 2}{1\ 1}^8, n = 35;$$
$$(\varphi_B(r)) = (14.76, 14.32, 2.24, 2.24, 2.24, 2.24, 2.24, 2.24, 2.24, 2.24, \ldots)$$
$$B = \binom{1\ 2}{1\ 1}^{11}, n = 35;$$
$$(\varphi_B(r)) = (8.06, 8.06, 8.06, 4.12, 4.00, 4.00, 4.00, 4.00, 1.00, 1.00, \ldots).$$

As one would expect, in the case of ghosts (respectively, clusters) $\varphi_B(r)$ attains small values (respectively, even the value one) for small r.

In contrast to χ_B the function φ_B is easy to calculate. x_0 with $0 \leq \|x_0\|_* \leq r$ can be represented as $x_0 = (a, b)$ with $a, b \in \mathbb{Z}$, $0 \leq \sqrt{|a|^2 + |b|^2} \leq r$. Thus

$$\varphi_B(r) = \min\{\sqrt{|(ab_{11} + bb_{12})^*|^2 + |(ab_{21} + bb_{22})^*|^2} \mid 0 < \sqrt{|a|^2 + |b|^2} < r\}.$$

It should be stressed that these definitions are only the very first steps towards an understanding of the chaotic behaviour of matrices $B \in SL(2, \mathbb{Z})$ mod n (or, more

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

generally, $B \in SL(m, \mathbb{Z})$ mod n).

Quantifications should be functions as in our examples or—even better—numbers which describe what is seen when treating concrete patterns P. It would then be very interesting to derive techniques to find—given n—matrices B in $SL(2, \mathbb{Z})$ such that B behaves 'as chaotic as possible' on $\mathbb{Z}_n^2$. Applications could be, for example, the cryptography of discrete pictures or the simple generation of uniformly distributed pseudorandom numbers in the unit square, i.e. sequences with a small discrepancy (in the sense of [**5**]) which are important for fast numerical integration.

Appendix

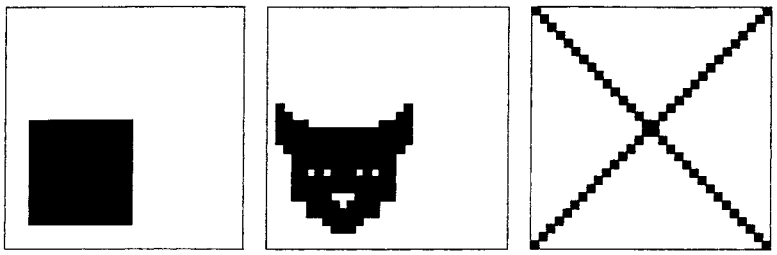


FIGURE A1. (a) Sqr_{30}, (b) Cat_{30}, (c) Cro_{30}.

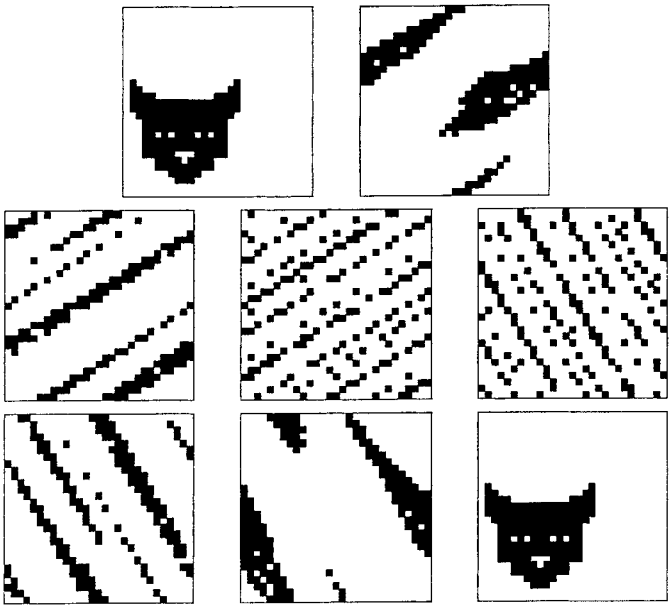


FIGURE A2. $A_{29}^k(Cat_{29}), k = 0, \ldots, 7$.

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

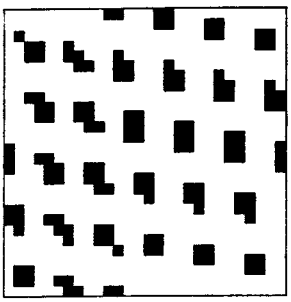


FIGURE A3. $A_{28}^{5}(Sqr_{28})$.

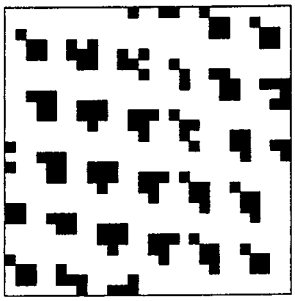


FIGURE A4. $A_{28}^{5}(Cat_{28})$.

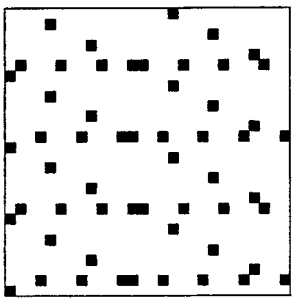


FIGURE A5. $A_{28}^{5}(Cro_{28})$.

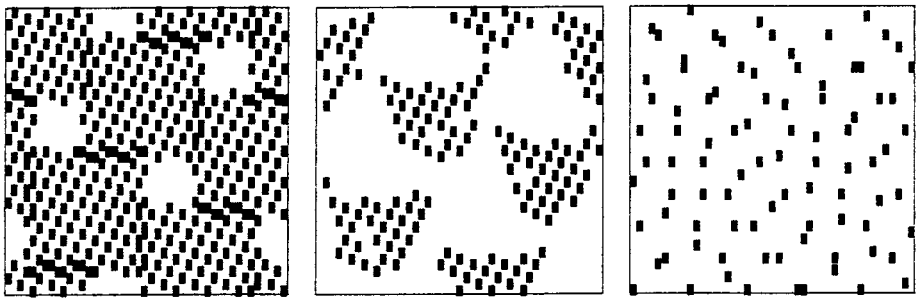


FIGURE A6. (a) $A_{45}^{12}(Sqr_{45})$, (b) $A_{45}^{12}(Cat_{45})$, (c) $A_{45}^{12}(Cro_{45})$.

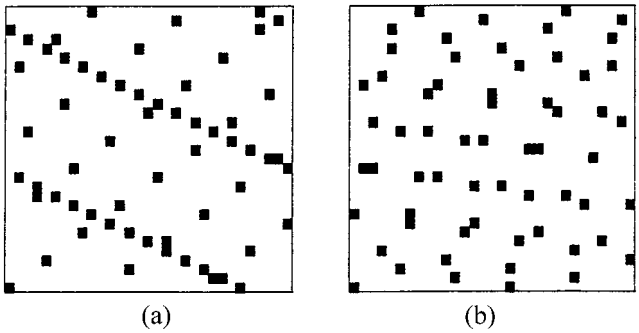


FIGURE A7. (a) $A_{31}^{8}(Cro_{31})$, (b) $A_{31}^{10}(Cro_{31})$.

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press

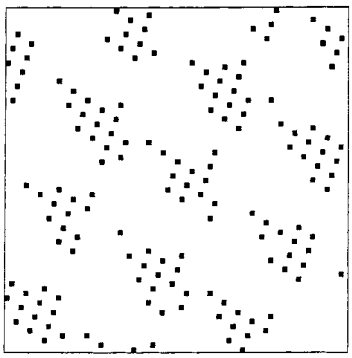


FIGURE A8. $A_{73}^{12}(Cat_{73})$.

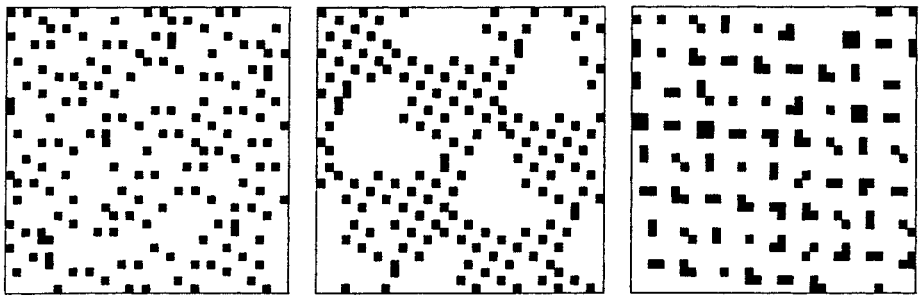


FIGURE A9. (a) $A_{35}^{6}(Cat_{35})$, (b) $A_{35}^{8}(Cat_{35})$, $A_{35}^{11}(Cat_{35})$.

REFERENCES

[1] E. Behrends and B. Fiedler. Periods of discretized linear Anosov maps. *Ergod. Th. & Dynam. Sys.* **18** (1998), 331–341.
[2] J. W. Cassels. *An Introduction to the Geometry of Numbers.* Springer, 1971.
[3] F. J. Dyson and H. Talk. Period of a discrete cat mapping. *Amer. Math. Monthly* **99** (1992), 603–614.
[4] T. Y. Kong, R. Kopperman and P. R. Meyer. A topological approach to digital topology. *Amer. Math. Monthly* **98** (1991), 901–917.
[5] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences.* Wiley, 1974.
[6] A. Rosenfeld and R. A. Melter. Digital geometry. *The Math. Intelligencer* **11**(3) (1989), 69–72.
[7] K. L. Siegel. *Lectures on the Geometry of Numbers.* Springer, 1989.

https://doi.org/10.1017/S0143385798100378 Published online by Cambridge University Press