SIGNATURE OF TIME-REVERSAL SYMMETRY IN POLYNOMIAL AUTOMORPHISMS OVER FINITE FIELDS

JOHN A. G. ROBERTS AND FRANCO VIVALDI

Abstract. We investigate the reduction to finite fields of polynomial automorphisms of the plane, which lead to invertible dynamics (permutations) of a finite space. We provide evidence that, if the map of the plane is non-integrable, then the presence or absence of a type of time-reversal symmetry called R-reversibility produces a clear signature in the cycle statistics of the associated permutation. If there is such a time-reversal symmetry, the cycle statistics is conjectured to obey a universal distribution, whereas if no such time-reversal symmetry is present, the cycle statistics is consistent with that of a random permutation. These results furnish necessary conditions for R-reversibility to exist in rational maps of the plane, which can be checked via finite computation in a finite field. This translates into effective tests for the existence of R-reversibility, and a probabilistic algorithm for determining parameter values at which a map has such a property.

1. Introduction

An automorphism L of some space is said to be *reversible* or to have a *time-reversal (or reversing) symmetry*, if there exists an automorphism G satisfying

$$G \circ L \circ G^{-1} \;=\; L^{-1}\,. \tag{1}$$

Whenever G is an involution, the property (1) is equivalent to the map L being able to be written as a composition of two involutions, e.g., $LG := L \circ G$ and G. Devaney [7] made extensive studies of the properties of maps that were such compositions when, additionally, both G and LG fix a subspace with half the dimension of the phase space. He called such maps *R-reversible.* The R-reversible maps include, and are a natural generalization of, the symplectic maps that arise from taking surfaces of section of Hamiltonian flows with conventional time-reversal symmetry. Note, however, that R-reversible maps need not be symplectic or even volume-preserving.

For planar maps, particularly area-preserving ones, R-reversibility has been much studied and exploited, even dating back to pioneering studies by Birkhoff ([24, 22, 31] and references therein). In the planar context, R-reversibility equates to the map being the composition of two involutions that are each reflections across a non-intersecting curve in the plane (the so-called *symmetry lines*). The symmetry lines are particularly useful for finding *symmetric* periodic orbits, i.e., those invariant under G [8], and for studying phenomena involving symmetric periodic orbits like period-doubling [24, 31, 15]. For our purpose, via a result due to Finn [11], one can then use the following:

Definition 1. *A smooth map of the plane L is R-reversible if it is the composition of two involutions G and LG with $\det(dG) < 0$ and $\det(d(LG)) < 0$, where dG is the Jacobian of G.*

When the map L is *algebraic* —defined by rational functions with coefficients in some field K— the definitions of reversibility and R-reversibility can easily be adapted to an algebraic

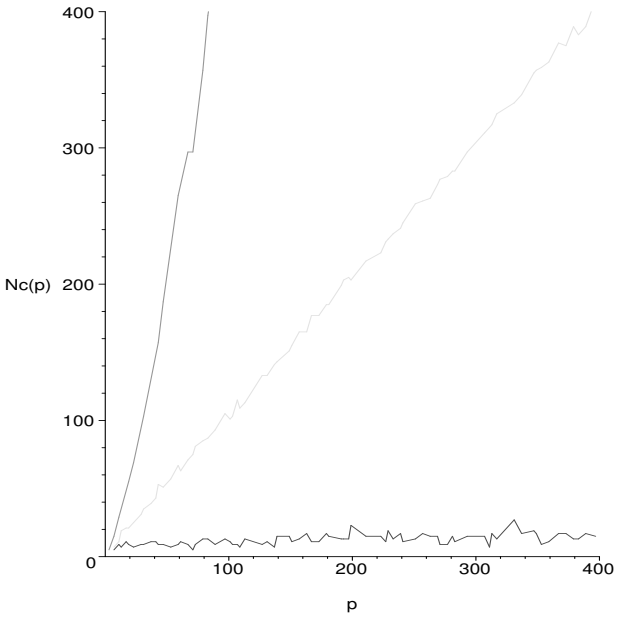

FIGURE 1. Maps over finite fields $\mathbb{F}_p$: growth of the number of cycles with prime p, for an integrable map (top curve), a non-integrable R-reversible map (middle), and a non-integrable non-R-reversible map (bottom). The curves are conjectured to be asymptotic to $p\log(p)$, p, and $2\log(p)$, respectively.

setting. In particular, if one requires that the map L be symplectic, then the condition $\det(dG) < 0$ (which makes sense only if the field K is ordered) becomes $\det(dG) = -1$, which is verifiable in any field.

The phase space of the map L need not be K^2, since K can be replaced by any field in which the coefficients of L can be represented, and this may include the case of *finite* fields. Thus, for instance, a rational map over $\mathbb{Q}$ is definable not only over fields containing $\mathbb{Q}$ (such as $\mathbb{R}$), but also over any finite field whose characteristic (the prime divisor of its cardinality) does not divide the denominator of the coefficients of L. The property of R-reversibility should be thought of as a *global* algebraic property of the map; the task then is to identify the signature of R-reversibility in the various finite representations of this map.

We will show that, over finite fields, R-reversibility manifests itself combinatorially, by constraining the cardinality of $Fix(G)$ —the set of fixed points of G— and $Fix(LG)$ and by inducing a tight organization of the periodic orbits. This is in turn reflected in an asymptotic (large fields) distribution of their periods. Strong evidence suggests that this distribution is universal, i.e., independent of the map (within the class of R-reversible maps with a single time-reversal symmetry), and that it is also markedly different from the period distribution of maps which are not R-reversible (see figures 2 and 7). This peculiar phenomenon results from the fact that the *symmetric orbits,* i.e., the orbits invariant under the involution G, dominate the statistics over the asymmetric ones, in sharp contrast with the case of maps with real or complex coordinates [24].

This distributional result, together with a companion result for integrable systems [32, 19], leads to simple and effective tests for detecting integrability and R-reversibility in algebraic mappings, or for spotting (algebraic) parameter values at which a parametric family has such

properties. The mere counting of cycles already provides a compelling test (figure 1).[1] A prominent feature of such tests is their sharpness, in the sense that a non-R-reversible map which is obtained by perturbing an R-reversible one will give the same reading irrespective of the size of the perturbation. By comparison, testing for R-reversibility in area-preserving maps, over the continuum of the real or complex plane, has proved quite mathematically subtle (see [21], [31, section 3.3], [30] for a fuller discussion and references therein).

This paper is organized as follows. In section 2 we study time-reversal symmetry for permutations. We find that, trivially, all permutations have such a property, because in a finite space time-reversal symmetries can be constructed on a cycle-by-cycle basis. However, the permutations that result from reducing to a finite field an R-reversible map have special features, which we use to introduce a non-trivial definition of finite R-reversibility (definition 2). We then consider R-reversible polynomial automorphisms over an algebraic number field [1]. Combining normal form techniques with the Cebotarev density theorem, we derive a lower bound for the number of cycles over the field $\mathbb{F}_{p^n}$ valid for a set of primes p having positive density (theorem 1). This result will form the basis for R-reversibility tests developed in section 5.

In section 3 we provide experimental evidence of the existence of a universal period distribution for R-reversible maps with a single family of time-reversal symmetries. The main result is a conjectured analytic form of this distribution (conjecture 1). We present a heuristic Galois-theoretic justification for the existence of a Poisson law for the frequency of cycles of small period, but also show some experimental evidence indicating a possible departure from such law for larger periods. In section 4 we consider maps which are not R-reversible, and conjecture that they instead behave like random permutations (conjecture 2).

The marked difference between these distributions leads to effective criteria for testing the presence of R-reversibility. We develop this idea in section 5, where we consider the problem of identifying parameter values for which a parametized family of maps is R-reversible. We show that, if the parameters being sought are algebraic, this can be done by merging results of measurements performed over different finite fields, together with a continued fraction algorithm, which is detailed in an appendix (see also [32]). Although this method is probabilistic, it does nonetheless provide crisp evidence of explicit algebraic relations. Finally, in section 6 we briefly discuss open problems and directions for future research.

2. Reversibility over a finite phase space

In this section we study reversibility from a combinatorial perspective, identifying the properties of the permutations obtained by reducing to finite fields R-reversible polynomial automorphisms of the plane. The main result of this section is a lower bound on the number of cycles (theorem 1). Due to the scarcity of asymmetric orbits (see figure 3), in practice this bound is quite sharp (see the middle curve in figure 1).

We recall from (1) that if G is a reversing symmetry of L, then so is any member of the family

$$L^i\, G = G\, L^{-i} \qquad i \in \mathbb{Z}. \tag{2}$$

[1]The fact that R-reversibility leads to more cycles, of average shorter length, as compared to non-R-reversible maps has been found in other settings, for example: (*i*) in a study of roundoff in a planar symplectic map, where the real map was replaced by an approximation on a finite lattice [28]; and (*ii*) in so-called time-reversible Boolean networks [5].

Orbits invariant under G —the symmetric orbits— are clearly invariant under any member of the family.

2.1. **Permutations and reversibility.** Let π be a permutation of $X = \{1, 2, \ldots, n\}$. The group of all such permutations is the symmetric group S_n of order $n!$. The permutation π partitions X into disjoint cycles. As we are interested only in the number and length of these cycles, we encode this partition as

$$\alpha(\pi) := (\alpha_1(\pi), \alpha_2(\pi), \ldots, \alpha_n(\pi)),$$

where $\alpha_i(\pi)$ is the number of i-cycles. Notice that

$$\sum_{i=1}^{n} i\,\alpha_i(\pi) = n, \qquad \sum_{i=1}^{n} \alpha_i(\pi) = \#Cycles(\pi),$$

where $\#Cycles(\pi)$ is the number of cycles of π.[2] The cycle decomposition of π represents an additive partition of the integer n into $\#Cycles(\pi)$ parts, and two permutations are conjugate in S_n precisely when they correspond to the same partition [33, Theorem 3.5].

It turns out that for every $\pi \in S_n$, it is possible to construct an involution γ such that equation (1) is satisfied with $L = \pi$ and $G = \gamma$. (In the presence of a reversing symmetry, we denote the set of symmetric cycles by $SymCycles(\pi)$, that of odd symmetric cycles by $SymOddCycles(\pi)$, etc.) This is because the permutation π^{-1} has the same cycle structure as π, with the cycles traversed in the opposite direction, and this allows the conjugating permutation to be chosen as an involution. This is detailed in the following

Proposition 1. *For every $\pi \in S_n$, there exists a reversing symmetry $\gamma \in S_n$ which is an involution. If the cycles of π have distinct lengths, then they are all symmetric with respect to γ. Otherwise, γ can be chosen so as to have, for each i such that $\alpha_i(\pi) > 1$, any number of pairs of asymmetric i-cycles, up to $\lfloor \alpha_i(\pi)/2 \rfloor$. Moreover, every reversing symmetry of a permutation π, whether involutory or not, acts as an involution on every cycle of π that it leaves invariant. Restricting to these symmetric cycles and using γ again to denote the ensuing involution, we have the property that*

$$\#Fix(\gamma) = \#SymOddCycles(\pi) + 2\,\#SymEvenCycles(\pi)_\gamma \tag{3}$$

$$\#Fix(\pi\gamma) = \#SymOddCycles(\pi) + 2\,\#SymEvenCycles(\pi)_{\pi\gamma} \tag{4}$$

and consequently

$$\#Fix(\gamma) + \#Fix(\pi\gamma) = 2\,\#SymCycles(\pi). \tag{5}$$

The subscript γ in equation (3) denotes the cycles that intersect $Fix(\gamma)$, etc. From this result it follows that a reversing symmetry on a finite space is necessarily an involution if there are no more than two cycles of any period. Furthermore, (3)–(5) may be vacuous statements (all entries are zero) if γ fixes no cycle of π (a necessary condition for this to occur is $\alpha_i(\pi) > 1$ for each cycle present).

Proof: We construct γ cycle-by cycle, matching the cycles of π with those of its inverse. Let $\mathcal{C}$ be a cycle of π of length $i > 0$. With a suitable re-labelling of its elements we can describe the action of π and of its inverse on $\mathcal{C}$ as

$$\pi_{\mathcal{C}}^{\pm 1}(x) \equiv x \pm 1 \,(\mathrm{mod}\ i). \tag{6}$$

[2] We use the symbol "#" to denote the cardinality of a finite set.

The map $\gamma_{\mathcal{C}}(x) \equiv -x \,(\mathrm{mod}\, i)$ defines an involution on $\mathcal{C}$, which conjugates the two cyclic permutations of $\mathcal{C}$ given by (6). Repeating the above procedure for all cycles of π, we obtain the required involution γ.

If all cycles of π have distinct lengths, then such γ necessarily leaves each cycle invariant, that is, each cycle is symmetric. If instead $\alpha_i(\pi) > 1$ for some i, then we can choose to compose the involution $\gamma_{\mathcal{C}}$ constructed above with any involution of the i-cycles; these will then decompose into m pairs of asymmetric i-cycles, with $0 \le m \le \lfloor \alpha_i(\pi)/2 \rfloor$, together with $\alpha_i - 2m$ symmetric i-cycles.

Consider now permutations π and δ such that $\pi^{-1} = \delta\pi\delta^{-1}$. Although the latter conjugacy necessarily forces δ to map cycles of π of the same length among themselves, this permutation of the cycles need not be involutory if $\alpha_i(\pi) > 2$ for some i.

Nevertheless, if $\mathcal{C}$ is an i-cycle of π which is left invariant by δ, we will ultimately show that δ acts as an involution on $\mathcal{C}$. So, without loss of generality, we denote δ by γ on $\mathcal{C}$, which is hence γ-symmetric. An easy induction from $\pi^{-1} = \gamma\pi\gamma^{-1}$ then gives

$$\gamma\pi^j = \pi^{-j}\gamma \qquad j \in \mathbb{Z}. \tag{7}$$

Then, for each $x \in \mathcal{C}$, we have that $\gamma(x) = \pi^k(x)$, for some $k = k(x)$, determined uniquely modulo i. If k is even, then (7) gives

$$\begin{aligned} \gamma(x) = \pi^{k/2}\pi^{k/2}(x) &\implies \pi^{-k/2}\gamma(x) = \pi^{k/2}(x) \\ &\implies \gamma\pi^{k/2}(x) = \pi^{k/2}(x) \end{aligned}$$

showing that $\pi^{k/2}(x) \in Fix(\gamma)$. Similarly, if k is odd

$$\begin{aligned} \gamma(x) = \pi^{-1}\pi^{(k+1)/2}\pi^{(k+1)/2}(x) &\implies \pi\pi^{-(k+1)/2}\gamma(x) = \pi^{(k+1)/2}(x) \\ &\implies \pi\gamma\pi^{(k+1)/2}(x) = \pi^{(k+1)/2}(x) \end{aligned}$$

showing that $\pi^{(k+1)/2}(x) \in Fix(\pi\gamma)$.

Now, if the period i is odd, the parity of k can be chosen arbitrarily, so an odd cycle has points in both $Fix(\gamma)$ and $Fix(\pi\gamma)$. Conversely, if $x, y \in \mathcal{C}$ with $x \in Fix(\gamma)$ and $y \in Fix(\pi\gamma)$, then $y = \pi^k(x)$ for some k, and we find

$$\pi^k(x) = \pi\gamma\pi^k(x) = \pi\pi^{-k}\gamma(x) = \pi^{-k+1}(x)$$

giving $\pi^{2k-1}(x) = x$, so the period is odd. Moreover, if $x \in \mathcal{C} \cap Fix(\gamma)$, then,

$$\gamma\pi^j(x) = \pi^{-j}\gamma(x) = \pi^{-j}(x) \qquad j \in \mathbb{Z}. \tag{8}$$

This equation shows that $\mathcal{C}$ is γ-symmetric. In addition, the fixed point condition $\pi^j(x) = \pi^{-j}(x)$ yields the congruence $2j \equiv 0 \,(\mathrm{mod}\, i)$, and consequently if the set $\mathcal{C} \cap Fix(\gamma)$ is non-empty, then it has one or two points, depending on whether i is odd or even, respectively. The case $x \in \mathcal{C} \cap Fix(\pi\gamma)$ is dealt with similarly.

We conclude that an i-cycle of π is γ-symmetric if and only if it has precisely one point in $Fix(\gamma)$ and one in $Fix(\pi\gamma)$ for odd i, and two points in $Fix(\gamma)$ and none in $Fix(\pi\gamma)$ (or vice-versa) if i is even. This establishes (3), and hence (4), by replacing γ with $\pi\gamma$. Adding the two results yields (5), since the above reasoning also shows that

$$\#SymEvenCycles(\pi) = \#SymEvenCycles(\pi)_{\gamma} + \#SymEvenCycles(\pi)_{\pi\gamma}.$$

Finally, equation (8) shows that $\gamma^2\pi^k(x) = \gamma\pi^{-k}(x) = \pi^k(x)$, so that γ acts as an involution on the γ-symmetric cycle, mapping forward iterates of x to their corresponding backward

iterates. (In fact, γ is conjugate to $\gamma_{\mathcal{C}}(x)$ that we constructed in the first part of the proof. This justifies our earlier replacement of δ by γ when restricted to $\mathcal{C}$.) □

Note that the second half of the above proof reproduces some ideas that date back to [8]. Our proof also shows that in the *a posteriori* cycle-by-cycle construction of the involution γ, once the permutation π is given, one can choose to distribute the symmetric even cycles as unevenly as desired, between $Fix(\gamma)$ and $Fix(\pi\gamma)$. It turns out that for permutations which represent the reduction to a finite field of an R-reversible polynomial automorphism, one instead has equipartition of symmetric even cycles between the two symmetry lines. This suggests the following (cf. definition (1))

Definition 2. *A permutation π of n^2 points is called R-reversible if it is the composition of two involutions γ and $\pi\gamma$ with $\#Fix(\gamma) = \#Fix(\pi\gamma) = n$.*

From proposition 1, we then obtain the the desired bound on the number of cycles, together with information on the arrangement of symmetric cycles.

Corollary 1. *If $\pi \in S_{n^2}$ is R-reversible, then $\#Cycles(\pi) \geq \#SymCycles(\pi) = n$. Each odd symmetric cycle has precisely one point on $Fix(\gamma)$ and one on $Fix(\pi\gamma)$, while every even symmetric cycle has two points on one fixed set, and none on the other. Furthermore, the number of even cycles intersecting $Fix(\gamma)$ and $Fix(\pi\gamma)$ is the same.*

2.2. **Polynomial automorphisms and reversibility.** We now show that a natural source of R-reversible permutations —in the sense of definition 2— derives from the group of planar polynomial automorphisms. This group, which we denote $GA_2(K)$, comprises maps of the form $x' = f(x, y)$, $y' = g(x, y)$, where f and g are polynomials over some field K, *and* there is an inverse that is also polynomial. This condition on the inverse ensures that the Jacobian determinant of the map is constant, a non-zero element of K.

Elements of $GA_2(K)$ therefore provide invertible maps of K^2 (indeed of $\bar{K}^2$, where $\bar{K}$ is the algebraic closure of K) and the iterated dynamics of examples with $K = \mathbb{R}, \mathbb{C}$ has received much attention. A famous example is the Hénon quadratic family

$$x' = y, \quad y' = -\delta x + y^2 + \epsilon, \tag{9}$$

with parameter ϵ and Jacobian determinant $\delta \neq 0$. The area-preserving case is $\delta = 1$ and the dissipative case is $0 < |\delta| < 1$. However, if we let $K = \mathbb{F}_q$, a finite field with $q = p^k$ elements, p a prime, the elements of $GA_2(K)$ correspond to permutations of q^2 points, i.e., to elements of S_{q^2}.

The group $GA_2(K)$ has the structure of an amalgamated free product (see [1, 10, 12, 13, 14, 29] and references therein), which can be exploited to investigate various dynamical properties of its elements. For example, a normal form is obtained following [12]. First define a *generalised Hénon transformation* by

$$H: \quad x' = y, \quad y' = -\delta x + h(y), \tag{10}$$

with h a polynomial satisfying $\deg h \geq 2$ and $\delta \neq 0$ the constant Jacobian determinant of H. Then one shows that any nonlinear element of $GA_2(K)$ which is dynamically non-trivial [3] is conjugate within the group to a composition

$$H_n \circ H_{n-1} \circ \cdots \circ H_2 \circ H_1, \tag{11}$$

[3]This means that the element is not conjugate in $GA_2(K)$ to an affine map, or to an *elementary* map. An elementary map is of the form $x' = \alpha x + h(y)$, $y' = \beta y + v$, with h a polynomial, $\alpha, \beta, v \in K$ and $\alpha\beta \neq 0$ [12]. Elementary maps send horizontal lines to horizontal lines.

Type	*Polynomial automorphism L*	*R-reversibility condition and reversor G*
L_1	$x' = y$ $y' = -\delta x + h(y)$	$\delta = 1$ $x' = y \quad y' = x$
L_2	$x' = -\delta_1 x + y^2 + 1$ $y' = -\delta_2 y + x'^2 + \epsilon$	$\delta_1 = \delta_2 = 1$ $x' = -x + y^2 + 1 \quad y' = y$
		$\delta_1\delta_2 = 1 \quad a^3 = \delta_2 \quad \epsilon = a^2$ $x' = ay \quad y' = a^{-1}x$
L_3	$x' = y + X^3 + \epsilon_3 X^2 + \epsilon_4 X + \epsilon_5$ $[X = -\epsilon_1 x + y^2 + \epsilon_2]$ $y' = -x + (y^2 + 2\epsilon_2 + x'^2)/\epsilon_1$	$\epsilon_3 = \epsilon_5 = 0$ $x' = y \quad y' = x$

TABLE 1. Examples of polynomial automorphisms L, together with conditions for L to be R-reversible in $GA_2(K)$, and the corresponding reversor G.

of n generalised Hénon transformations with H_i depending on the constant δ_i and the polynomials h_i. Depending on the field K, certain simplifications of h_i can be made. The degree of the composition (11) can be shown to be $\prod_i \deg h_i$.

The reversibility of the elements of $GA_2(K)$ has been studied in [1], while closely related work for the real and complex cases is contained in [13, 14, 29]. These papers investigate equation (1) when both L *and* G belong to $GA_2(K)$, providing necessary and sufficient conditions for L to be reversible. A straightforward necessary condition from (1) is that $\det(\mathrm{d}L) = \pm 1$ (because the Jacobian determinants of L and G are constant), while from above, it suffices to develop further conditions for reversibility on the normal forms (11) [13]. For $n \leq 3$ in equation (11), conditions for R-reversibility on some normal forms are presented in table 1. In particular, the area-preserving Hénon map, (9) with $\delta = 1$, is seen to be R-reversible.

The nature of the involutions in $GA_2(K)$ is described by the following result [1]

Proposition 2. *If K is a field with* $\mathrm{char}(K) \neq 2$*, all involutions in $GA_2(K)$ are conjugate to either $G_1 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ or $G_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.*

Consequently, if $L, G \in GA_2(K)$, with L reversible with involutory reversing symmetry G, then this constitutes R-reversibility if and only if G and LG are conjugate to G_2 (whence L is area-preserving), in which case $Fix(G)$ and $Fix(LG)$ are both images of the line $y = x$ under a polynomial automorphism. For $K = \mathbb{C}, \mathbb{R}$, this shows that $Fix(G)$ and $Fix(LG)$ are actually curves of genus 0.

We now turn to the problem of the reduction to a finite field of an R-reversible map. The simplest case is that of a map L with rational coefficients a_i/b_i, to be reduced to a map $\overline{L}$ on the finite field $\mathbb{F}_p$ —the set of integers modulo a prime number p. The reduction is performed coefficientwise, and the only non-trivial step is the computation of the modular inverse b_i^{-1} of b_i using Euclid's algorithm. Clearly, we must exclude the primes p which divide the denominators b_i, but some additional care is required, for the following reason. We start with $L, G \in GA_2(\mathbb{Q})$, with G and LG conjugate to G_2 (cf. proposition 2), and we must ensure that $\overline{L}, \overline{G} \in GA_2(\mathbb{F}_p)$. When this is the case, the reduced map is also R-reversible, the fixed sets of the involutions have cardinality equal to q, and we shall speak of *good reduction.* We remark that good reduction is achieved for all but finitely many primes p.

The general case involves polynomials L, G whose coefficients are algebraic numbers α_i. Letting $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots)$, we now assume that $L, G \in GA_2(K)$. Then we choose an algebraic number α such that $K = \mathbb{Q}(\alpha)$, and this can be done so that α is an algebraic integer, namely a root of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$, of degree k. We write

$$\alpha_i = c_0^{(i)} + c_1^{(i)}\alpha + \cdots + c_{k-1}^{(i)}\alpha^{k-1} \qquad c_j^{(i)} = \frac{a_j^{(i)}}{b_j^{(i)}}. \tag{12}$$

We reduce L to the finite field $\mathbb{F}_q$ with $q = p^n$, p a prime (for background reference, see, e.g., [18]). The primes to be excluded now are the divisors of the denominators $b_j^{(i)}$. With this proviso, the coefficients α_i of L, G will be simultaneously representable in the finite field $\mathbb{F}_q$ precisely when the polynomial f has a root $\overline{\alpha}$ in $\mathbb{F}_q$. The polynomial f has k roots in $\mathbb{F}_{p^n}$ if $n \geq k$. For $n < k$, f has roots in $\mathbb{F}_{p^n}$ for a set of primes p having positive density (infinite, in particular), from the Cebotarev density theorem [27, page 129]. Each root corresponds to a reduction of L to $\mathbb{F}_q$, according to (12). For the actual computation of the roots there are standard algorithms [23, chapter 4].

As for $K = \mathbb{Q}$, the primes of good reduction are those for which the reduced system has involutions conjugate to the map G_2 of proposition 2, in which case the fixed sets of the involutions have cardinality equal to q.

Structurally, the process of reduction works as follows. For given p, the set of linear combinations

$$R = \left\{ \sum_{j=1}^{k-1} \frac{a_j}{b_j}\alpha^j \ : \ p \not| b_j \right\}$$

is a ring, which serves as the phase space of our dynamical system L. If $\overline{\alpha}$ is a root of f in $\mathbb{F}_{p^n}$, then the substitution $\alpha \mapsto \overline{\alpha}$, together with the reduction of a_j/b_j modulo p, define a ring homomorphism $\phi : R \to \mathbb{F}_{p^n}$. Its kernel is a maximal ideal P in R which divides pR. After extending ϕ to R^2 in the obvious way, we have the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{L} & R \\ \downarrow\phi & & \downarrow\phi \\ \mathbb{F}_q & \xrightarrow{\overline{L}} & \mathbb{F}_q \end{array}$$

and similarly for G.

We collect some of the above considerations in the following

Theorem 1. *Let K be an algebraic number field, and let L be an R-reversible map in $GA_2(K)$. Then for all positive integers n, there exists a set of primes p having positive density, for which L reduces to an R-reversible map $\overline{L} \in GA_2(\mathbb{F}_q)$, $q = p^n$, and hence to an R-reversible permutation of q^2 points in the sense of definition 2. Consequently, the cycles of $\overline{L}$ follow the prescriptions of corollary 1, with, in particular, $\#Cycles(\overline{L}) \geq q$.*

The bound $\#Cycles(\overline{L}) \geq q$ on the number of cycles is the best possible one: for instance the reduction to $\mathbb{F}_3$ of the area-preserving Hénon map (equation (9) with $\delta = 1$) has precisely 3 cycles for all values of the parameter ϵ. The infinite set of primes of good reduction prescribed by this result will form the basis for the asymptotic study of section 3.

Theorem 1 shows that R-reversible permutations are naturally constructed by reducing R-reversible polynomial automorphisms of the real or complex plane, provided their coefficients

are algebraic numbers. Likewise, the combinatorial consequences of a permutation being R-reversible can be used to infer whether or not a given polynomial automorphism of $\mathbb{C}^2$ or $\mathbb{R}^2$ is R-reversible.

As a simple example of such inference, consider the following area-preserving map L and its reduction to $\mathbb{F}_3$

$$\begin{aligned} x' &= x - \frac{1}{5}y^2 + 1 \equiv x + y^2 + 1 \,(\text{mod } 3) \\ y' &= y + x'^2 + \frac{2}{13} \equiv y + x'^2 + 2 \,(\text{mod } 3). \end{aligned}$$

One verifies that on $\mathbb{F}_3^2$ the reduced map $\overline{L}$ has a single 9-cycle, and therefore the map L is not R-reversible, from theorem 1. Note that L is reversible, according to (1), but the reversors G ($x' = -x + \frac{1}{5}y^2 - 1$, $y' = -y$) and LG are orientation-preserving, so conjugate to the map G_1 of proposition 2 (see [29, case R3 of table 3]). Each reversor fixes one point of the phase space, consistent with the single symmetric cycle of $\overline{L}$ and equation (5). We shall consider the problem of inference again in section 5.

3. R-reversible period distribution

For simplicity, in what follows we restrict consideration to reduction to the finite fields $\mathbb{F}_p$, p prime. Let L be an R-reversible polynomial automorphism of the plane, with coefficients in some algebraic number field. Furthermore, we assume throughout that L has the single family of reversing symmetries (2). This is equivalent to saying that L does not have non-trivial maps with which it commutes (i.e., maps different from powers of L).

From theorem 1, for a set of primes p having positive density, the maps L and G can be represented over $\mathbb{F}_p$, and hence the phase space $\mathbb{F}_p^2$ decomposes into the union of at least p cycles. Let $T(z)$ be the period of the point $z \in \mathbb{F}_p^2$ under L. We define

$$\mathcal{R}_p(x) := \frac{1}{p^2} \#\{z : T(z) \leq px\} \tag{13}$$

which represents the probability that a point chosen at random in $\mathbb{F}_p^2$ belongs to a cycle of length not exceeding px. We also denote by $\mathcal{R}'_p$ the analogous density computed using *symmetric* orbits only.

Experimental evidence (see figure 2) supports the following

Conjecture 1. *For every R-reversible polynomial automorphism with a single family of reversing symmetries, the limit*

$$\mathcal{R}(x) := \lim_{p\to\infty} \mathcal{R}_p(x) = \lim_{p\to\infty} \mathcal{R}'_p(x) = 1 - e^{-x}(1 + x) \tag{14}$$

exists, and is independent of the map.

We have formulated this conjecture in terms of distributions rather than the associated densities (cf. equation (15)), because the former are much easier to compute than the latter. From equation (14) it follows that, near zero, $\mathcal{R}(x) = x^2/2 + O(x^3)$, which itself suffices to differentiate the R-reversible from the non R-reversible behaviour (where with the same scaling $\mathcal{R}(x)$ is zero —see section 4), and the integrable behaviour, where $\mathcal{R}(x)$ is conjectured to grow linearly [19]. (For the reader's convenience, we summarize the essence of the behaviour of the distribution function (14) for algebraically integrable systems [32, 19]. The level sets of the integrals are algebraic curves of genus at most one; the motion on such curves is conjugate

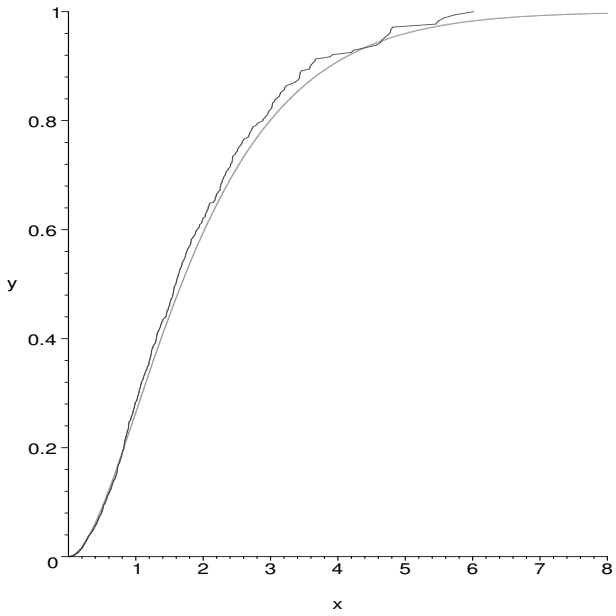

FIGURE 2. Comparison between conjectured and actual period distributions for an R-reversible map. The experimental data is for the Hénon map (9) with $\delta = 1$ at the prime $p = 997$. Three curves are plotted: the distribution (13) for $\epsilon = 1$ (the irregular curve), its average over all ϵ-values, and the theoretical distribution (14) (the smooth curves). At this resolution, the last two curves are indistinguishable. For a more accurate analysis, see figure 4.

to a translation with respect to an abelian group —the analogue of rotation on a circle. It then follows that, over a finite field, all orbits on the same curve necessarily have the same period, whereas the total number of points on a curve is of order p, due to the Hasse-Weil bound. As a result, the limiting distribution function is a step function, with steps at the reciprocals of the natural integers. The existence of the limit (14) is found to be related to the validity of a variant of the so-called elliptic analogue of Artin's conjecture on primitive roots.)

We now examine more closely the numerical evidence supporting conjecture 1. First of all, we note that the asymmetric orbits play no role in the asymptotics, in marked contrast with the real or complex case, where asymmetric orbits dominate the statistics [24]. In figure 3 we show that the fraction of the phase space occupied by asymmetric orbits appears to decay algebraically as $1/2p$.

In figure 4, we plot the ratio between the theoretical and numerical period distributions, using the same data as in figure 2. The data for the prime $p = 499$ is added for comparison. For $p = 997$, the relative error is within 1% for a substantial range of values of x: $0.1 \leq x \leq 4$. Furthermore, comparison with $p = 499$ indicates that this range increases with p, suggesting a nonuniform convergence to the limiting distribution (14). The large relative error in the vicinity of the origin results from the anomalous behaviour of orbits of very low period (see below). The large relative fluctuations for large x are attributable to poor statistics (note that at $x = 7$, $1 - \mathcal{R}(x) < 10^{-2}$).

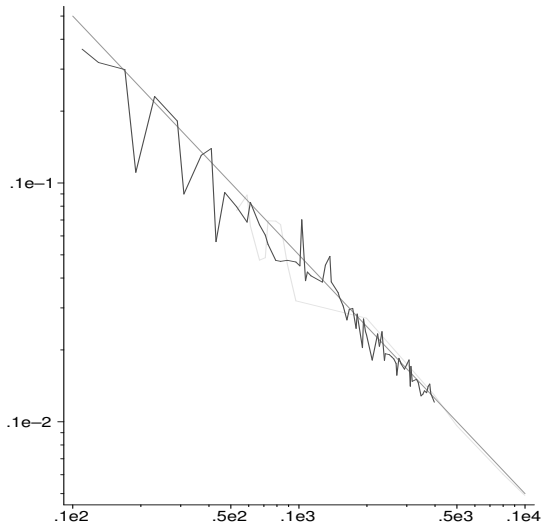

FIGURE 3. Log-log plot of the fraction of the phase space occupied by asymmetric orbits for the area-preserving Hénon map (9), and an R-reversible map of type L_2 of table 1 at a sequence of primes p in the range $10 < p < 1000$. The function $p \mapsto 1/2p$ is plotted for comparison.

We have obtained data consistent with the above quantitative picture from a variety of R-reversible polynomial maps, as given in table I. In fact conjecture 1 also appears to hold for R-reversible rational maps (where one works over projective space and uses periodic orbits only [32, figure 4]). The same distribution was also found when the parametric average is replaced by averaging over different primes, the parameter being fixed. This provides additional evidence of the robustness of this phenomenon.

A distinguished feature of the limit (14) is the scaling of the periods by p (cf. equation (13)). The density

$$\frac{d}{dx}\mathcal{R}(x) = xe^{-x} \tag{15}$$

represents the limiting probability that a point chosen at random in $\mathbb{F}_p^2$ belongs to a cycle of length $T = px$. Let $R_p(x,k)$ be the probability that a cycle of length $T = px$ will appear k times, and let $R(x,k)$ be the corresponding limiting distribution. Then equation (15) implies that

$$\sum_{k\geq 0} kR(x,k) = e^{-x}. \tag{16}$$

Assuming that the k-dependence is modelled by a Poisson distribution with parameter e^{-x} (see below), we have

$$R(x,k) = e^{-\lambda}\frac{\lambda^k}{k!} \qquad \lambda = e^{-x}. \tag{17}$$

The numerical functions $R_p(x,k)$, which represent the probability of k occurrences of the period $T = xp$, feature large fluctuations, in spite of the fact that the data have been averaged over all parameter values (see figure 5, for $k = 0$). To suppress fluctuations we consider the

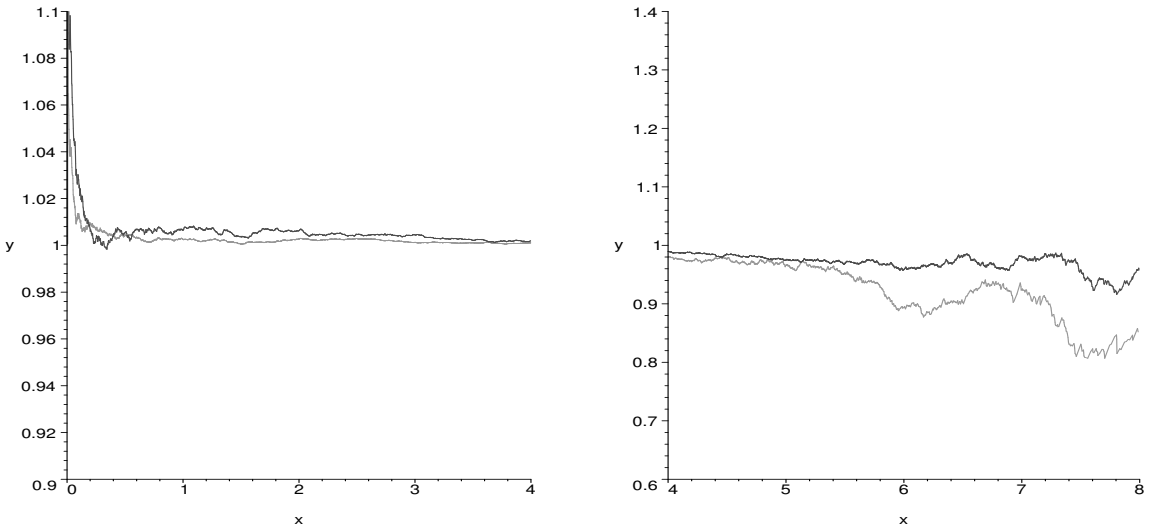

FIGURE 4. Left: the ratio $\mathcal{R}'_p(x)/\mathcal{R}(x)$ between the period distribution (13) of the area-preserving Hénon map, and its conjectured asymptotic form (14), for $p = 499$ and $p = 997$ (the darker curve). The convergence of $\mathcal{R}'_p(x)$ to $\mathcal{R}$ appears to be non-uniform near zero (small periods). Right: the ratio $(1 - \mathcal{R}'_p(x))/(1 - \mathcal{R}(x))$, for the same map. The fluctuations for large x (large periods) are attributable to poor statistics in a regime where the function $1 - \mathcal{R}$ approaches zero.

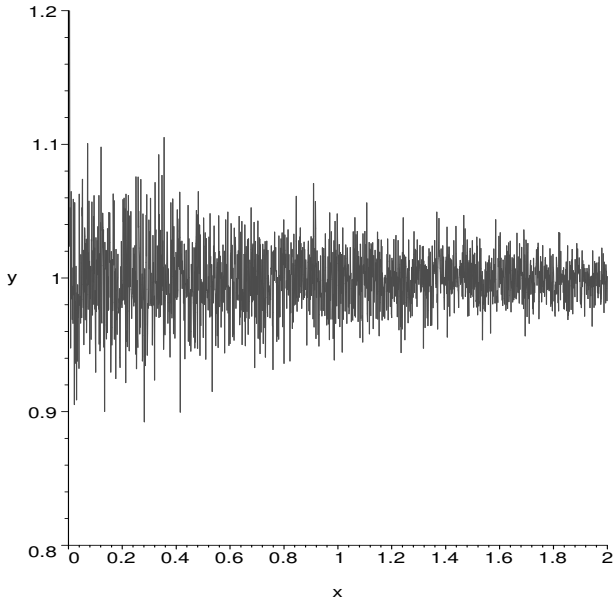

FIGURE 5. The ratio $R_p(x, 0)/R(x, 0)$ for the area-preserving Hénon map at $p = 997$. The data represent the average over all parameter values.

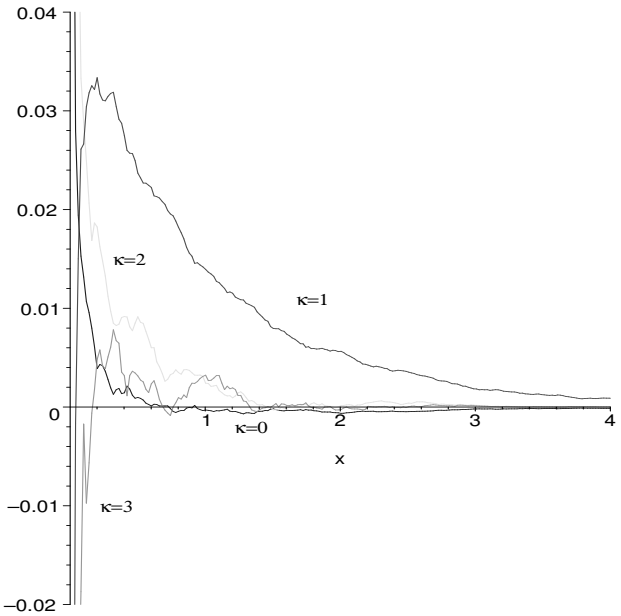

FIGURE 6. Testing the Poisson distribution (17) for the area-preserving Hénon map at $p = 997$, averaged over all parameter values. We compare the Riemann sums (18) of the numerical densities $R_p(x, k)$ with the corresponding integrals (19) for $k = 0, 1, 2, 3$, displaying the normalized relative error. The largest discrepancy occurs for $k = 1$.

Riemann sums

$$S_p(x,k) = \frac{1}{p}\sum_{t=1}^{\lfloor px \rfloor} R_p(t/p,k) \tag{18}$$

and we compare them with the integrals

(19)

$$S(x,0) = \int R(x,0)dx = \mathrm{Ei}(e^{-x}) \qquad S(x,k) = \int R(x,k)dx = \frac{1}{k}\sum_{n=0}^{k-1} R(x,n) \qquad k \geq 1$$

where Ei is the exponential integral.

A test of the validity of the Poisson distribution (17) is presented in figure 6, where we plot for various values of k the relative error in approximating S by S_p. The data are normalized so that such error vanishes as $x \to \infty$. Because the functions $R(x, k)$ are monotonic in x, the truncation error is bounded by $1/p \sim 10^{-3}$, which is negligible on the scale shown. The agreement is satisfactory, although the 3% relative error for $k = 1$ may not entirely be explained by inadequate statistics, and it allows for the possibility that the Poisson model may only be approximate.

Whilst a rigorous justification of these probabilistic phenomena seems very difficult, we now provide a heuristic explanation of the Poisson scaling law (17) valid in the in the limit of small periods. Every symmetric orbit of an R-reversible map intersects $\mathrm{Fix}(G)$ or $\mathrm{Fix}(LG)$, and these intersections are roots of a univariate polynomial $\Phi_T(x)$ over $\mathbb{Z}$ (T is the period). It is reasonable to assume that, typically, such a polynomial is irreducible over $\mathbb{Q}$, and that its Galois group $\mathrm{Gal}(\Phi_T)$ is the largest possible one. When T is odd, this group is the

symmetric group S_m. When T is even, the roots of Φ_T come in pairs, and the largest Galois group consistent with this constraint is the wreath product $\mathrm{Gal}(\Phi_T) \sim C_2 \wr S_{m/2}$. These assumptions on the Galois group are quite natural, and analogous results have been proved in the context of polynomial dynamical systems in one dimension [26, 2, 25]. The group $\mathrm{Gal}(\Phi_T)$ can be computed explicitly provided T is not too large [6].

Now, a map over $\mathbb{F}_p$ has k symmetric T-cycles precisely when the polynomial $\Phi_T(x)$ has k linear factors modulo p ($2k$, if T is even). From Cebotarev's density theorem, the probability of this event at a randomly chosen prime p is given by the probability that a random element in $\mathrm{Gal}(\Phi_T)$ has k ($2k$) fixed points. Because the degree m of $\Phi_T(X)$ increases exponentially with T, for large T, this probability is equal to $e^{-1}/k!$, independent of m, and hence of the period T [3, section 6.7]. From equation (17), this probability is precisely equal to $R(0,k)$. The above argument requires $m \to \infty$ (hence $T \to \infty$, logarithmically in m), and $T/p \to 0$. For fixed p and T, the range of k-values is limited by $kT \le p^2$. In addition, for fixed T, one has to exclude the finitely many primes which divide the discriminant of Φ_T, for which the factorization of Φ_T is anomalous (multiple roots), but these primes do not affect the asymptotics.

4. Lack of R-reversibility and random permutations

The simplest probabilistic model for an invertible map which is non integrable, non R-reversible, and has no other symmetry, is a *random* permutation [20]. Let π be a random permutation of $X = \{1, 2, \dots, n\}$. The probability that a point of X belongs to a t-cycle is equal to $1/n$, for all $t \le n$.[4] Letting $n = p^2$, this would give for a system which is not R-reversible $\mathcal{R}_p(x) \approx x/p \to 0$ as $p \to \infty$ (cf. equation (13)). In order to get a non-trivial limit, we scale the period differently and define

$$\mathcal{I}_p(x) := \frac{1}{p^2} \#\{z : T(z) \le p^2 x\} \tag{20}$$

which represents the probability that a point chosen at random in $\mathbb{F}_p^2$ belongs to a cycle of length not exceeding $p^2 x$. As p becomes large, the function $\mathcal{I}_p(x)$ cannot be expected to converge, due to the typical occurrence of very long cycles (of order p^2 —see below). Some averaging is therefore necessary. Let $\mathcal{P}_p = \mathcal{P}_p(L)$ be the set of primes not exceeding p at which the map L can be reduced. We define the average order of $\mathcal{I}$ as follows

$$\langle \mathcal{I} \rangle_p(x) = \frac{1}{\#\mathcal{P}_p} \sum_{p' \in \mathcal{P}_p} \mathcal{I}_{p'}(x). \tag{21}$$

Experimental evidence (see figure 7) supports the following

Conjecture 2. *For every (non-integrable) map, which is not R-reversible and has no other symmetry, the limit*

$$\mathcal{I}(x) := \lim_{p \to \infty} \langle \mathcal{I} \rangle_p(x) = x \tag{22}$$

exists and is independent of the map.

[4] This probability is derived as the product of $t-1$ terms of the form $(n-j)/(n-j+1)$, $j = 1, \dots, t-1$, being the probabilities of not returning to the point for the first $t-1$ steps, together with the term $1/(n-t+1)$, being the probability of returning to the point on the t-th step.

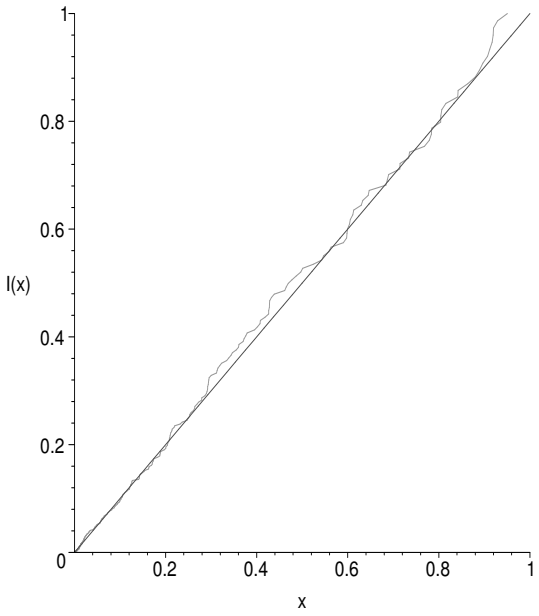

FIGURE 7. Conjectured and actual period distributions for a non R-reversible map, given by equations (22) and (21), respectively. The numerical distribution is for a map of the form L_3 of table 1 with $\epsilon_3 \neq 0$ (hence non R-reversible), which is computed averaging over the first 70 primes of good reduction. Parametric averages at a fixed prime give similar results.

Indeed experiments suggest that modelling cycle statistics by a random permutation may extend beyond period distribution. For instance, the expected maximum cycle length of a random permutation of p^2 points is equal to $p^2 \times 0.6243\ldots$, while the expected number of cycles is $2\log(p) + \gamma$, where γ is Euler's constant [34]. We have verified these statistics experimentally for various non R-reversible maps, see e.g., figure 8.

5. Detecting R-reversibility

The difference that exists in the distributions of cycle lengths, depending on the presence or absence of R-reversibility, and the ensuing effects on observables, suggest an effective procedure for identifying parameter values at which a given parametric family of algebraic mappings becomes R-reversible. This approach, based on theorem 1, should be seen as the analogue of the integrability criterion developed in [32], based on the Hasse-Weil bound.

Before we proceed, we note that tests of this kind are parametrically 'sharp', in the sense that the notion of near R-reversibility (or near integrability) familiar from perturbation theories in parametrized families, is plainly inapplicable here. If a non-R-reversible real or complex map is made to converge to an R-reversible one by adjusting a parameter, convergence is lost over a finite field. This is due to the fact that the process of reduction to a finite field for both phase space and parameter space is everywhere discontinuous, and moreover the pre-image of any finite field element is a set *dense* in the original coordinate space.

Consider thus a parametric family of maps L_ϵ which becomes R-reversible at unknown parameter value(s) $\epsilon = \epsilon^*$. We assume that ϵ^* is an algebraic number, that is, $f(\epsilon^*) = 0$, where f is a monic polynomial with rational coefficients which we wish to determine.

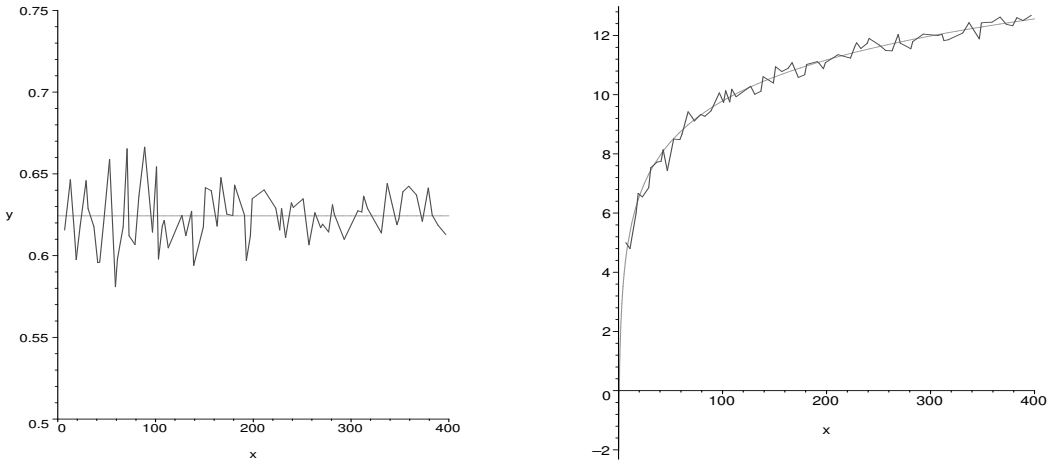

FIGURE 8. Left: Maximum cycle length for primes p up to 397 for a one-parameter family of non R-reversible maps of the type L_3 of table 1. For each prime, the maximum cycle length is an average over all parameter values and is scaled by p^2. The horizontal line corresponds to the theoretical maximum cycle length $p^2 \times 0.6243\ldots$ of a random permutation of p^2 elements. Right: Number of cycles for primes p up to 397 for the dissipative Hénon map (9) with $\delta = -3/10$, which is not R-reversible. (The prime $p = 13$ is excluded, for at that prime the map is area-preserving and R-reversible.) For each prime, the number of cycles is an average over all values of the parameter ϵ. The smooth curve corresponds to $2\log(p) + \gamma$, where γ is Euler's constant.

We now develop a probabilistic method for determining f. We select a finite sequence of primes $p_1, p_2, \ldots$, and for every p_i we compute the total number of cycles of the reduced map $\overline{L}_\epsilon$ for all reduced parameter values $\epsilon \equiv 0, \ldots, p_i - 1 \,(\mathrm{mod}\ p_i)$. In accordance with theorem 1, we then select the parameter values (if any) for which the number of cycles is at least p_i: for sufficiently large p this measurement will be quite unambiguous (figure 9). In this way one identifies a sequence of congruence classes representing the unknown parameter modulo various primes, and the task is to recover the latter from the former. Every value of $\overline{\epsilon}$ selected in this way is a root of f modulo p, and hence it corresponds to a linear factor in the factorization of f over $\mathbb{F}_p$

$$f(x) \equiv (x - \overline{\epsilon}) g(x) \,(\mathrm{mod}\ p).$$

The $\overline{\epsilon}$ sequence is non-empty. Indeed, from Cebotarev's theorem, we have that for every polynomial f over $\mathbb{Q}$, there exists a set $\mathcal{S}$ of primes having *positive density,* such that f decomposes completely as a product of distinct linear factors modulo p

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \equiv \prod_{k=1}^{d} (x - \overline{\epsilon}_k) \,(\mathrm{mod}\ p) \tag{23}$$

precisely when $p \in \mathcal{S}$. Such primes are called the *split primes* of f. If f is irreducible, the density of $\mathcal{S}$ is equal to $1/\#\mathrm{Gal}(f)$, where $\mathrm{Gal}(f)$ is the Galois group of f.[5] The existence of such a density is a very valuable probabilistic result, because, in the absence of special assumptions on the polynomial f, the process of factorization of f modulo a prime should be

[5]more precisely, the Galois group of the smallest normal extension of $\mathbb{Q}$ generated by the roots of f.

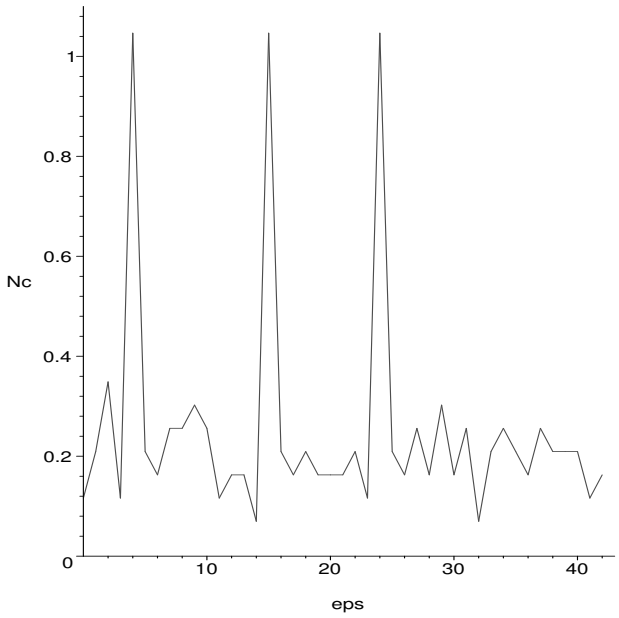

FIGURE 9. Normalized number N_c/p of cycles of the map L_2 of table 1 over $\mathbb{F}_p$ with $p = 43$, $\delta_1 = 5/3$, $\delta_2 = 1/\delta_1$, as a function of ϵ. The number of cycles exceeds p for the three parameter values $\epsilon = 4, 15, 24$, giving strong indication of R-reversibility.

p	$(\overline{\delta}_1, \overline{\epsilon})$		δ_1	
2	$(1, [0, 1])$			
7	$(4, 5)$	$(2, 4)$		
11	$(9, 9)$	$(4, 1)$		
17	$(13, 16)$	$(4, 1)$		
19	$(\mathbf{8}, [5, 16, 17])$		$-3/2$	$-1/7$
23	$(\mathbf{17}, 9)$		$5/3$	$1/88$
29	$(\mathbf{21}, 22)$		$5/3$	$-1/2534$
37	$(\mathbf{14}, [3, 4, 30])$		$5/3$	156302
41	$(\mathbf{29}, 5)$		$5/3$	-6408312
43	$(\mathbf{16}, [4, 15, 24])$		$5/3$	$-1/165334492$

TABLE 2. Reduced values of the parameter pairs (δ_1, ϵ) for which the map of the type L_2 of table 1 with $\delta_2 = 3/5$, has at least p cycles modulo p, for $p \leq 43$. If the same value of $\overline{\delta}_1$ corresponds to several values of $\overline{\epsilon}$, the latter are given in square brackets. For $p \geq 19$, the rightmost two columns give the two rationals number r/s of smallest height $|rs|$, which are congruent to the sequence of $\overline{\delta}_1$ values indicated in boldface, from $p = 19$ to the current prime.

expected to be quite random, subject only to the weak constraint of Stickelberger's theorem [4, p 198]. The aforementioned Cebotarev density gives the probability that, at a randomly selected prime, our parametric search yields the maximal number $\#\epsilon = d$ of reduced ϵ-values, where d is the degree of f. In fact, our strategy is precisely to identify the unknown degree of f by computing $\#\epsilon$ for a sufficient number of primes. One should be aware that the

identification of split primes is subject to two types of uncertainties. First, our R-reversibility criterion is only *necessary,* and one should expect false readings for small primes. Second, the process of reduction may generate spurious algebraic relations at finitely many primes, which alter the nature of the reduced map. An example of the latter will be given below. While these processes do not affect asymptotics, they are relevant to computations.

If f is irreducible of degree d, the probability of occurrence of the factorization (23) is bounded from below by $1/d!$. The minimum value occurs if $\mathrm{Gal}(f)$ is the symmetric group of order d, and this probability determines the applicability of our algorithm, which in practice works well for $d < 5$, say. In this context, we note that an efficient algorithm to recover an algebraic number from congruences has been developed recently, based on lattice reduction, with cryptographic applications [35]. However, our algorithm is simpler and well suited for our purpose.

Once the reduced roots $\overline{\epsilon}$ of f are known, we compute its reduced coefficients $\overline{a}_i$ as elementary symmetric functions of the roots. We must now recover the *rational* coefficients a_i of f from the knowledge of their value modulo different primes. This amounts to identifying a rational number from a sequence of congruences. To do so we use an algorithm based on the Chinese Remainder Theorem and continued fractions [9, 16] (our version of which is described in the appendix). It allows one to arrange the rationals r/s satisfying a sequence of congruences in order of increasing value of their 'height' $|rs|$, which is a measure of complexity. As the number of congruences increases, the rational of minimal height will eventually become r/s, while all other rationals will diverge in height and fluctuate wildly.

We illustrate our method by carrying out a blind search for the R-reversibility conditions $\delta_1\delta_2 = 1$ and $\epsilon^3 = \delta_2^2$ for maps of the type L_2 (see table 1). We fix $\delta_2 = 3/5$ (chosen so as to have a recognizable identity, but otherwise arbitrarily), and for a suitable number of primes p, $p \neq 5$, we search for all reduced pairs $(\overline{\delta}_1, \overline{\epsilon})$, $\overline{\epsilon} \neq 0$, for which the map L_2 reduced to $\mathbb{F}_p$ has at least p cycles. The data are displayed in table 2. We first consider the number $\#\delta_1$ of distinct values of δ_1 that occur at p. We find $\#\delta_1 = 0$ for $p = 3, 5, 13$, $\#\delta_1 = 1$ for $p = 2, p > 17$, and $\#\delta_1 = 2$ for $p = 7, 11, 17$.

Even though the maximal value of $\#\delta_1$ is 2, the inference that the minimal polynomial f_{δ_1} of δ_1 is quadratic is problematic, due to the persistent occurrence of $\#\delta_1 = 1$ for $p > 17$. If f_{δ_1} were quadratic, a single $\overline{\delta}_1$ value would correspond to a double root of f_{δ_1} modulo p, and hence all these primes would have to divide the discriminant of f_{δ_1}. So δ_1 is more likely to be rational, and we attempt to compute it from its residues modulo p, for $p > 17$ (the boldface data in table 2). Monitoring the rational of smallest height which satisfies such congruences, we arrive at the unequivocal inference $\delta_1 = 5/3$. The rational of next to minimal height is also displayed, for comparison. A few experiments varying δ_2 will persuade all but the most sceptical that area-preservation ($\delta_1\delta_2 = 1$) is necessary for R-reversibility.

Turning now to the parameter ϵ, our data give $\#\epsilon = 3$ as the maximum number of values. To gather further evidence, we fix $\delta_1 = 5/3$, $\delta_2 = 3/5$, and proceed to a one-dimensional parametric search on the remaining primes up to $p < 100$, again selecting the values of $\overline{\epsilon}$ (if any) for which the number of cycles of $\overline{L}_\epsilon$ is at least p. These are displayed in table 3.

The repeated occurrence of $\#\epsilon = 3$ strongly suggests that the minimal polynomial f_ϵ of ϵ is cubic (indeed the value $\#\epsilon = 1$ indicates that its Galois group is S_3). At the corresponding split primes p we have a factorization of the type (23) with $d = 3$

$$f_\epsilon(x) = x^3 + a_2x^2 + a_1x + a_0 \equiv (x - \overline{\epsilon}_1)(x - \overline{\epsilon}_2)(x - \overline{\epsilon}_3) \,(\mathrm{mod}\ p).$$

p	$\overline{\epsilon}$			$\overline{a}_0$	$\overline{a}_1$	$\overline{a}_2$	a_0	a_1	a_2
2	0	1							
7	5								
11	9								
17	16								
19	5	16	17	8	0	0	$-3/2$	0	0
23	9								
29	22								
37	3	4	30	10	0	0	84	0	0
41	5								
43	4	15	24	22	0	0	$-9/25$	0	0
47	24								
53	42								
59	21								
67	10	22	35	5	0	0	$-9/25$	0	0
71	38								
83	40								
89	79								
97	18	31	48	85	0	0	$-9/25$	0	0

TABLE 3. Reduced parameter values $\overline{\epsilon}$ for which the area-preserving map of type L_2 (cf. table 1) with $\delta_1 = 5/3$ and $\delta_2 = 3/5$, has at least p cycles modulo p, for all primes $p < 100$. The missing primes correspond to $\#\epsilon = 0$ (which include $p = 3, 5$, for which there is no reduction). For the split primes ($\#\epsilon = 3$) we also display the reduced coefficients $\overline{a}_k$ of the unknown polynomial f_ϵ. The quantity a_k on the same row is the rational number r_k/s_k of minimal height $|r_k s_k|$, which is congruent to $\overline{a}_k$ modulo p for all split primes up to the current one. Asymptotically, these values converge in height to the coefficients of f_ϵ (see appendix).

The reduced coefficients $\overline{a}_i$ are symmetric functions of the roots: they are displayed in table 3. Applying our sieve algorithm to the candidate split primes for ϵ ($p = 19, 37, 43, 67, 97$), we obtain the corresponding rationals of minimal height as $a_2 = a_1 = 0$ and $a_0 = -(3/5)^2$. We conclude that $f_\epsilon(x) = x^3 - (3/5)^2$, in agreement with the second R-reversibility condition for L_2 of table 1.

In closing we note that, from table 1, if $\delta_1 = r/s$ then at all primes p dividing $r - s$ ($p = 2$, in the above data), we have that $\overline{\delta}_1 = \overline{\delta}_2 = 1$, and the system becomes R-reversible for all values of ϵ. Thus if $r - s$ is divisible by a prime $p \geq 3$, this phenomenon will generate spurious data concerning split primes.

6. Discussion

In this paper, we give evidence that R-reversibility produces a universal signature on reduction to finite fields. Our examples have been polynomial automorphisms, though we note from [32] that R-reversible rational maps appear to achieve the same distribution when only periodic orbits are used. The mechanism driving this signature distribution is the fact that the cardinality of both symmetry lines is equal to p. We have restricted ourselves to the case of a single family of reversing symmetries. We expect that when there are multiple families

of reversing symmetries, we enter new (universal?) regimes for the periodic orbit distribution of the reduced map. On the other hand, in the absence of R-reversibility, evidence has been presented that the periodic orbit distribution is consistent with a random permutation.

The research presented here is still in an embryonic state; in closing, we isolate a few among many open questions.

Do the distribution functions $\mathcal{R}(x)$ and $\mathcal{I}(x)$ defined in sections 3 and 4 also describe the statistics of periods associated with the reductions of a *single* rational orbit? More precisely, let $z \in \mathbb{Q}^2$ be such that the L-orbit through z is infinite. If p is a prime of good reduction for L (i.e., such that L can be reduced modulo p), then the orbit of $\overline{L}$ modulo p is periodic; we let $T_p(z)$ be its period. As p varies, the normalized periods $T_p(z)/p$ (if L is R-reversible) and $T_p(z)/p^2$ (if L is not R-reversible), generate an infinite set of rational numbers. Are these numbers distributed according to $\mathcal{R}(x)$ and $\mathcal{I}(x)$, respectively? This statement is almost certainly false if we are allowed to choose the primes p, for in this case it would be easy to bias the sample. However, we have evidence that this statement is true if p runs through all primes of good reduction.

The above assumption leads to an alternative approach to R-reversibility tests, in the spirit of a Monte Carlo simulation, which offers considerable computational advantages with respect to a full orbit decomposition of the phase space. Specifically, for a fixed initial condition z, we scale the reduced period $T_p(z)$ by $(p^2+1)/2$, the expected value for the non-reversible case[6]. However, from equation (15) it follows that —assuming that asymmetric orbits are negligible— the expected R-reversible cycle length is of order p. As a result, the average order of these lengths is expected to converge to zero if the map is R-reversible, and to one if it is not, thereby providing a 0–1 statistical test for R-reversibility.

What constitutes an appropriate probabilistic model for the distribution (14)? If one neglects asymmetric orbits, then the cycles of an R-reversible map represent an additive partition of the integer p^2 into p parts, and hence a cycle decomposition can be viewed as an instance of such a partition. It is possible to show that the average number of repetitions of a t-cycle among all such partitions is given by

$$\frac{1}{s(p^2,p)} \sum_{m\geq 0} s(p^2-(p-m)t, m)$$

where $s(n,k)$ is the number of partitions of n into exactly k parts [36]. Our investigation indicates that this formula, suitably scaled, does not yield the exponential value (16), and neither does the related model of permutations of order p^2 with p cycles, obtained from the above by introducing suitable weights.

Acknowledgements

It is a pleasure to thank Herbert Wilf for a helpful interaction on partitions. J.R. would like to thank the School of Mathematical Sciences at Queen Mary for their hospitality during the periods November 2003 – February 2004, and July 2004, where a substantial part of this work was done. Financial support by the Australian Academy of Science (under the "Travel Grants to Europe" Scheme) and the EPSRC (under Grant GR/S62802/01) are gratefully acknowledged.

[6]The expected cycle length of a random n-permutation is $\sum_{t=1}^{n} t\,\mathrm{Prob}(t\text{-cycle}) = 1/n \sum_{t=1}^{n} = (n+1)/2$.

APPENDIX: A SIEVE ALGORITHM

We develop an algorithm for identifying a rational number from congruences.

Let $r = n/d$, with n and d coprime, and d positive, and define the *height* h of r as

$$h(r) = h\left(\frac{n}{d}\right) = |n|d. \tag{24}$$

(This is not the standard definition of height.) Let p_i, $i = 1, 2, \ldots$ be a sequence of distinct primes which do not divide d (or, indeed, a sequence of pairwise coprime positive integers, which are coprime to d). Further, let a_i be such that $r \equiv a_i \,(\mathrm{mod}\ p_i)$, and define the sequence

$$m^{(l)} = \prod_{i=1}^{l} p_i \qquad\qquad l \geq 1.$$

Then, from the Chinese remainder theorem ([17], Theorem 121), there exists a unique integer $a^{(l)}$, $0 \leq a^{(l)} < m^{(l)}$, such that $n \equiv a^{(l)} d \,(\mathrm{mod}\ m^{(l)})$. This means

$$n = a^{(l)} d - m^{(l)} s^{(l)} \tag{25}$$

for some integer $s^{(l)}$. If r is a non-negative integer, then $s^{(l)} = 0$ and $n = a^{(l)}$. Otherwise $s^{(l)} \neq 0$ (lest d divides n, contrary to our assumption, unless $d = 1$ and $n < 0$, in which case $s^{(l)} \neq 0$ because $a^{(l)} d \geq 0$). Hence the sequence $a^{(l)}$ is unbounded. From (25), we obtain

$$\frac{a^{(l)}}{m^{(l)}} - \frac{s^{(l)}}{d} = \frac{n}{d m^{(l)}} \tag{26}$$

and since, as l increases, the right-hand side tends monotonically to zero, so does the left-hand side. Let $\alpha^{(l)} = a^{(l)}/m^{(l)}$. From (24) and (26), we find that

$$m^{(l)} > 2h(r) \qquad \Longrightarrow \qquad \left|\alpha^{(l)} - \frac{s^{(l)}}{d}\right| < \frac{1}{2d^2}. \tag{27}$$

It follows that if $m^{(l)} > 2h(r)$, then $s^{(l)}/d$ is a convergent of $\alpha^{(l)}$ ([17], theorem 184); indeed, a convergent of even order if $r > 0$, and of odd order if $r < 0$.

Clearly $m^{(l)}$ will exceed twice the height or r for all sufficiently large l. We now assume that l is in this range, and drop all superscripts, for ease of notation. Let p_i/q_i, $i = 1, \ldots, k$ be the convergents of α. Then $a = g p_k$ and $m = g q_k$, where $g = \gcd(a, m)$ is bounded, being a divisor of n (cf. (25)). The conditions

$$n_i = a q_i - m p_i \qquad d_i = q_i \qquad \gcd(q_i, m) = 1 \qquad 2h(n_i/d_i) < m \tag{28}$$

define a set of reduced rationals n_i/d_i as well as a set $I \subseteq \{0, \ldots, k-1\}$ of values of i. From (25), there exists a unique integer $i^* \in I$, depending on l, such that $n_{i^*}/d_{i^*} = n/d$.

We wish to develop an asymptotic ($m \to \infty$) characterization of i^*, which does not rely on knowledge of n/d. We let $h_i = h(n_i/d_i)$. From the approximation theorem for continued fractions

$$\frac{1}{2 q_i q_{i+1}} < \left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{q_i q_{i+1}}, \qquad\qquad \frac{p_i}{q_i} \neq \alpha$$

we obtain the height estimate

$$\frac{m\, q_i}{2 q_{i+1}} < h_i < \frac{m\, q_i}{q_{i+1}}$$

which, for $i = i^*$, gives

$$q_{i^*} = d \qquad \frac{m}{2|n|} < q_{i^*+1} < \frac{m}{|n|}. \tag{29}$$

We estimate h_i for $i \neq i^*$. First let $i = i^* + j$, with $j > 0$, (in which case hence $i \leq k$, from the rightmost inequality in (28)). We have

$$h_i > \frac{m}{2} \cdot \frac{q_{i^*+j}}{q_{i^*+j+1}} \geq \frac{m}{2} \cdot \frac{q_{i^*+1}}{m} > \frac{m}{4|n|}.$$

Similarly, for $i = i^* - j$, we find

$$h_i > \frac{m}{2} \cdot \frac{q_{i^*-j}}{q_{i^*-j+1}} \geq \frac{m}{2} \cdot \frac{1}{d}.$$

Putting all together

$$h\left(\frac{n_i}{d_i}\right) \geq \frac{m}{4\max(d, |n|)}, \qquad \frac{n_i}{d_i} \neq \frac{n}{d}. \tag{30}$$

From the recursion formula

$$q_{-1} = 0 \qquad q_0 = 1 \qquad q_{i+1} = c_{i+1}q_i + q_{i-1}, \qquad i \geq 0 \tag{31}$$

(the c_i are the continued fraction coefficients of α), and (29), one obtains

$$\frac{q_{i^*+1}}{q_{i^*}} = c_{i^*+1} + \frac{q_{i^*-1}}{q_{i^*}} > \frac{m}{2|n|d}$$

and so, as $m \to \infty$, the continued fraction expansion of α will feature a diverging coefficient. This is the root cause of the divergence of the height.

We now consider the converse problem, namely that of recovering $\epsilon^* = n/d$ from two integer sequences $a^{(l)}, m^{(l)}$, with $0 \leq a^{(l)} < m^{(l)}$, and such that $m^{(l)}$ divides $m^{(l+1)}$. For each l, compute the convergents of $a^{(l)}/m^{(l)}$, and from those, the rationals n_i/d_i, according to (28). As l increases, these sets will feature a common element of minimal height, while all other rationals will have increasing height, according to the estimate (30).

References

[1] M. Baake and J. A. G. Roberts, *Symmetries and reversing symmetries of polynomial automorphisms of the plane*, *Nonlinearity* **18** (2005) 791–816.

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

[3] P. Cameron, *Permutation groups,* London Mathematical Society Student Texts 45, Cambridge University Press, Cambridge (1999).

[4] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin (1993).

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

[6] J. H. Davenport and G. C. Smith, *Fast recognition of alternating and symmetric Galois groups,* Journal of Pure and Applied Algebra **153** (2000) 17–25.

[7] R. L. Devaney, *Reversible diffeomorphisms and flows*, Trans. Am. Math. Soc. **218** (1976) 89-113.

[8] R. De Vogelaere, *On the structure of symmetric periodic solutions of conservative systems, with applications,* in: *Contributions to the Theory of Nonlinear Oscillations, Vol. 4*, ed. S. Lefschetz, Princeton University Press, Princeton (1958), pp. 53-84.

[9] C. Ding, D. Pei and A. Salomaa, *Chinese Remainder Theorem: applications in computing, coding, cryptography,* World Scientific, Singapore (1996).

[10] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Birkhäuser, Basel (2000).
[11] J. M. Finn, PhD Thesis, University of Maryland (1974).
[12] S. Friedland and J. Milnor, *Dynamical properties of plane polynomial automorphisms*, Ergod. Th. & Dynam. Sys. **9** (1989) 67–99.
[13] A. Gómez and J. D. Meiss, *Reversible polynomial automorphisms of the plane: the involutory case*, Phys. Lett. **A 312** (2003) 49–58; nlin.CD/0209055.
[14] A. Gómez and J. D. Meiss, *Reversors and symmetries for polynomial automorphisms of the complex plane*, Nonlinearity **17** (2004) 975-1000; nlin.CD/0304035 v2.
[15] J. M. Greene, R. S. MacKay, F. Vivaldi and M. J. Feigenbaum, *Universal behaviour in families of area-preserving maps*, Physica D **3** (1981) 468-486.
[16] R. T. Gregory and E. V. Krishnamurthy, *Methods and applications of error-free computation,* Springer-Verlag, Berlin (1984).
[17] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford (1979).
[18] H. Hasse, *Number theory*, Springer-Verlag, Berlin (1980).
[19] D. Jogia, J. A. G. Roberts, and F. Vivaldi, An algebraic geometric approach to integrable maps of the plane, preprint, University of New South Wales (2005).
[20] V. F. Kolchin, *Random Mappings* Optimization Software, New York (1986).
[21] J. S. W. Lamb, *Area-preserving dynamics that is not reversible*, Physica A **228** (1996) 344–365.
[22] J. S. W. Lamb and J. A. G. Roberts, *Time-reversal symmetry in dynamical systems: A survey*, Physica **D 112** (1998) 1–39.
[23] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Math. and its Appl., vol. 20, Addison-Wesley, Reading, Mass. (1983).
[24] R.S. MacKay, *Renormalisation in Area-Preserving Maps*, World Scientific, Singapore, 1993.
[25] P. Morton, *Galois groups of periodic points*, J. of Algebra **201** (1998) 401–428.
[26] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. **51** (1985) 385–414.
[27] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, Cambridge (1990).
[28] F. Rannou, *Numerical study of discrete plane area-preserving mappings*, Astron. & Astrophys. **31** (1974) 289–301.
[29] J. A. G. Roberts and M. Baake, *Symmetries and reversing symmetries of area-preserving polynomial mappings in generalised standard form*, Physica **A 317** (2003) 95–112; math.DS/0206096.
[30] J. A. G. Roberts and H. W. Capel, *Area preserving mappings that are not reversible*, Phys. Lett. A **162** (1992) 243–248.
[31] J. A. G. Roberts and G. R. W. Quispel, *Chaos and time-reversal symmetry — order and chaos in reversible dynamical systems*, Phys. Rep. **216** (1992) 63–177.
[32] J. A. G. Roberts and F. Vivaldi, *Arithmetical method to detect integrability in maps*, Phys. Rev. Lett **90** 3 (2003) [034102].
[33] J. J. Rotman, *An introduction to the theory of groups,* 4th ed., Springer, New York (1995).
[34] L. A. Shepp and S. P. Lloyd, *Ordered cycle lengths in a random permutation*, Trans. Amer. Math. Soc. **121** (1996) 340–357.
[35] I. E. Shparlinski and R. Steinfeld, in: *Algebraic number theory*, (Proc. 5th Int. Symp, ANTS-V, Sydney (2002)) eds. C. Fieker and D. R. Kohel, Springer Verlag, New York (2002) pp. 349–356.
[36] H. Wilf, private communication.

School of Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: jag.roberts@unsw.edu.au
URL: http://www.maths.unsw.edu.au/~jagr

School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, UK
E-mail address: f.vivaldi@maths.qmul.ac.uk
URL: http://www.maths.qmul.ac.uk/~fv