The Hasse-Weil Bound and Integrability Detection in Rational Maps

John A G ROBERTS †, *Danesh JOGIA* † *and Franco VIVALDI* ‡

† *School of Mathematics, The University of New South Wales, Sydney NSW 2052, Australia*
E-mail: jagr@maths.unsw.edu.au, daneshj@maths.unsw.edu.au

‡ *School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, United Kingdom*
E-mail: f.vivaldi@qmul.ac.uk

This paper is part of the Proceedings of **SIDE V***;*
Giens, June 21-26, 2002

Abstract

We reduce planar measure-preserving rational maps over finite fields, and study their discrete dynamics. We show that application to the orbit analysis over these fields of the Hasse-Weil bound for the number of points on an algebraic curve gives a strong indication of the existence of an integral for the map. Moreover, the method is ideally suited to separating near-integrability from genuine integrability.

1 Introduction

Suppose a rational symplectic map of the plane has a rational integral. Can we infer the existence of such an integral by studying (a reduction of) this map over a *finite* phase space? If the map depends on parameters, can we identify from such finite measurements the parameter values at which the integral occurs? This is the topic of this paper (see also [14]).

Various criteria for integrability are available for maps (for background on integrable mappings, see [4, 17]). The most prominent are singularity confinement [5, 7, 9] (a discrete-time version of the Painlevé criterion for differential equations) and the algebraic entropy test [3, 7, 16, 18]. There are other methods as well [1, 12].

Phase spaces are real or complex manifolds, and hence the underlying number systems are the real or complex fields. In this paper we take an arithmetical perspective, and replace the latter with *finite fields,* via an algebraically natural discretization process that does not require rounding-off. With this device the phase space becomes finite, and endowed with a rich arithmetical structure. In the presence of an integral of the motion, the points in the orbits are roughly *equidistributed* among the level sets of the integral. This phenomenon is a consequence of an important result in arithmetic geometry, the so-called *Hasse-Weil bound* for the number of points on algebraic curves over finite fields.

The implication of this theorem to the question of integrability is the main theme of this paper. We will show that in an integrable map, the maximal orbit length is much shorter than in the non-integrable case, and we will construct effective algorithms that turn measurements on finitely many orbits into an integrability test. A unique feature of this approach is the complete absence of the concept of 'near integrability'. Due to a singular change in topology, parameter values converging to an integrable value in $\mathbf{C}$ typically do not converge in $\mathbf{F}_p$ at all, and consequently the value of an observable will not converge to its integrable value.

In the next section we introduce the main ideas through the analysis of a specific example. The Hasse-Weil theorem is presented in Section 3, together with some basic constructions. The statistics of orbit lengths in the integrable and non-integrable case are compared in Section 4, where we also describe some numerical techniques. Finally, in Section 5 we briefly discuss the sieve algorithm that allows one to recover integrable parameter values from measurements over several finite fields. We also discuss the lack of the concept of near-integrability over finite fields. Although we confine ourselves to maps of the plane, we are hopeful that aspects of the ideas described will also work in higher dimensions (this is currently being investigated).

2 Integrable rational maps over finite fields: a motivating example

Consider the following rational planar map L

$$x' = -x - \frac{y+1}{y^2+1}\,, \qquad y' = -y - \frac{x'-1}{(x')^2+1}. \tag{2.1}$$

This map is area-preserving. It is also integrable, being a special case of a QRT map [11], [13, Appendix A]. We have

$$I(x',y') = I(x,y), \qquad I(x,y) = x^2y^2 + x^2 + y^2 + xy + x - y. \tag{2.2}$$

Furthermore, L is *reversible* [13] meaning it has the time-reversal property:

$$L^{-1} = G \circ L \circ G^{-1}, \qquad G : x' = -y, \quad y' = -x. \tag{2.3}$$

The map G is an involution and reversibility is equivalent to saying that L can be written as the composition of two involutions. All QRT maps are reversible and reversibility is a ubiquitous property of integrable maps in any dimension.

Whilst we usually think of the action of (2.1) on $\mathbf{R}^2$ or $\mathbf{C}^2$, we could equally well think of it as a map on the 'rational plane' $\mathbf{Q}^2$, by restricting coordinates to rational values. (This is because the coefficients of the map are rational.) It is clear from (2.1) that if the initial point of an orbit is rational, so are all points in that orbit (in particular, the denominators never vanish). Here we are interested in letting (2.1) act on the *finite* phase space $\mathbf{F}_p^2$ (or its projective version, see below), where $\mathbf{F}_p$ – the set of integers modulo a prime p – is the simplest instance of a *finite field*. To reduce the map L from $\mathbf{Q}^2$ to $\mathbf{F}_p^2$, it suffices to reduce modulo p the result of the arithmetical operations involved in computing (2.1). This creates no difficulties, although we have to allow for the possibility that the denominators in (2.1) could now vanish.

Height	Cycle lengths	# points on level set
0	2,2,2,2	8
1	9,9	18
2	7,7	14
3	none	0
4	13	13
5	7,7	14
6	5,5	10
7	11	11
8	9	9
9	3,3,3,3	12
10	6,6	12

Table 1. Cycle length data for the rational map (2.1) modulo 11, organized by level set height of its integral (2.2).

With a finite phase space, all the dynamics induced by L can be charted (albeit at the expense of a total loss of familiar topology). Importantly, the possession of the integral (2.2) is a purely algebraic property that can be studied over any field: it entails that iterates of an initial point (x_0, y_0) under L will lie on the integral level set $I(x, y) = I(x_0, y_0)$ (and, likewise, for iterates of (x_0, y_0) under L^{-1} when L is invertible). On the real plane, this leads to the signature integrable phase portrait of a foliation by curves (see, e.g., [11, 8] for many such phase portraits). When the phase space is finite, each level set of the integral is a finite set of points which can be decomposed into the orbits induced by the action of the rational map.

For illustration, we consider (2.1–2.2) when $p = 11$. Since $11 \equiv 3 \,(\mathrm{mod}\, 4)$, standard number theory [6, Theorem 82] tells us that the denominators in (2.1) do not vanish. It follows that (2.1) is invertible over $\mathbf{F}_{11}^2$, and induces a permutation of the 121 phase space points. In Table 1, we indicate the number of points in each level set of $I(x, y)$ together with the breakdown of those points into cycles (see also Figure 1). The longest cycle has length 13 and constitutes the level set $I(x, y) = 4$. The largest level set is the 18 points derived from $I(x, y) = 1$ which decompose into two 9-cycles. The actual points belonging to the level sets are organized by the reversibility property (2.3). Since G, as well as L and I, reduces well modulo p, we deduce from (2.3) the standard property that a point $\mathbf{x}$ and its image $G\mathbf{x}$ have the same period. They belong to one *symmetric* cycle invariant under G or belong in an *asymmetric* pair of cycles interchanged by G (as illustrated in Figure 1). Moreover, we observe that the integral $I(x, y)$ is invariant under G so that $\mathbf{x}$ and $G\mathbf{x}$ always belong to the same level set. We observe that the cardinality of the level sets of $I(x, y)$ is always bounded by

$$HW(11) = 11 + 2\sqrt{11} + 1 = 18.63\ldots. \tag{2.4}$$

Here $HW(p)$ is the so-called *Hasse-Weil bound* for the number of points on an irreducible algebraic curve of genus one defined over the finite field $\mathbf{F}_p$. We will explain its origin and significance in the next section.

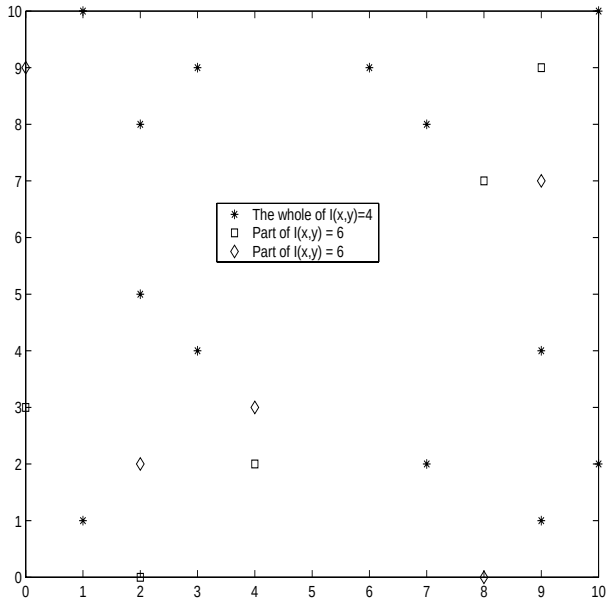

Figure 1. Some orbits of the map (2.1) on the finite phase space $\mathbf{F}_{11}^2$. Shown is the 13-cycle which constitutes the level set of height 4 of the integral (2.2), and the two 5-cycles which make up the level set $I(x, y) = 6$. The former is symmetric with respect to the reversing symmetry G of (2.3), whereas the latter form an asymmetric pair with respect to G.

In general, studying rational maps like (2.1) exclusively over $\mathbf{F}_p^2$, the *affine plane*, is inadequate due to the presence of singularities when the denominators vanish, which occurs in (2.1) when $p \equiv 1 \,(\mathrm{mod}\, 4)$. The standard algebraic-geometric device is to work with the *projective plane* $\mathbf{P}(\mathbf{F}_p^2)$ with homogeneous coordinates (X, Y, Z). It comprises $p^2 + p + 1$ points: the affine plane $(X, Y, 1)$ (p^2 points) together with the *line at infinity* $(X, 1, 0) \cup (1, 0, 0)$ ($p + 1$ points). To obtain the projective version of a given rational map of the affine plane, we introduce $x = X/Z$, $y = Y/Z$ and then define Z' so as to (minimally) clear the denominators in X' and Y' [1]. Applied to (2.1), this procedure yields the projective map $\tilde{L}$ (with all operations performed modulo p):

$$\begin{aligned} X' &= N(D^2 + N^2) \\ Y' &= -(Y^2 + Z^2)(YN^2 + YD^2 + DNZ - D^2Z) \\ Z' &= D(D^2 + N^2) \end{aligned} \tag{2.5}$$

where

$$N = -(XY^2 + XZ^2 + YZ^2 + Z^3), \qquad D = Z(Y^2 + Z^2). \tag{2.6}$$

An immediate consequence of (2.2) is that $\tilde{L}$ inherits an integral, $\tilde{I}(X', Y', Z') = \tilde{I}(X, Y, Z)$ with

$$\tilde{I}(X, Y, Z) = \frac{X^2Y^2 + Z^2(X^2 + Y^2 + XY) + Z^3(X - Y)}{Z^4}. \tag{2.7}$$

[1]Of course, writing a rational map in projective coordinates is also the starting point for performing the singularity confinement test. However, the discrete topology here makes it impossible to resolve the singularity by introducing a measure ϵ of proximity to the singularity and letting $\epsilon \to 0$.

We see from (2.5–2.6) that whenever a point $(X, Y, 1)$ in the affine plane is a singularity for the map by satisfying: (i) $Y^2 + Z^2 = Y^2 + 1 \equiv 0 \,(\mathrm{mod}\ p)$; or (ii) $N^2 + D^2 \equiv 0 \,(\mathrm{mod}\ p)$, then $Z' = 0$ and this is true of further iterates. The conditions (i) and (ii) correspond, respectively, to the vanishing of the denominators of x' and y' in the original non-projective map L. Furthermore, we see from (2.7) that on the line at infinity ($Z = 0$), $\tilde{I}$ is either *indeterminate* at the two points $(0, 1, 0)$ or $(1, 0, 0)$, or has (formal) value ∞ at the $p - 1$ points $(X, 1, 0)$, $X \neq 0$. The two points $(0, 1, 0)$ or $(1, 0, 0)$ are *base points* of the integral in that they can be considered to lie on every level set of $\tilde{I}$. Both points map under (2.5) to $(0, 0, 0)$, which is *not* part of the projective space so the orbit *terminates*. The preservation of $\tilde{I}$ by $\tilde{L}$ shows that singular points of the map satisfying (i), respectively (ii), map to $(1, 0, 0)$, respectively $(0, 1, 0)$ and hence to $(0, 0, 0)$.

When $p = 11$, or more generally $p \equiv 3 \,(\mathrm{mod}\ 4)$, the dynamics of $\tilde{L}$ on the affine plane and the line at infinity are disjoint. To supplement Table 1, we need to add the base points $(0, 1, 0)$ and $(1, 0, 0)$ to each level set of $\tilde{I}$. Also, the level set $\tilde{I} = \infty$ decomposes into an additional $p - 1$ fixed points of $\tilde{L}$. To illustrate the decomposition of points of $\mathbf{P}(\mathbf{F}_p^2)$ under the action of $\tilde{L}$ when orbits can move from the affine plane to the line at infinity, we set $p = 13$. Table 2 gives the corresponding breakdown. There are two types of orbit now: cycles and *terminating* orbits. The latter typically involve points in the affine plane, the first of which is a singular point of $\tilde{L}^{-1}$ (the projective version of L^{-1}) and the last of which is a singular point of $\tilde{L}$. These singular points are mapped, respectively, by $\tilde{L}^{-1}$ and $\tilde{L}$ to one of $(0, 1, 0)$ or $(1, 0, 0)$. We observe from Table 2 that, with the exception of $\tilde{I} = 4$, the number of points on each level set is bounded by $HW(13)$, where

$$HW(13) = 13 + 2\sqrt{13} + 1 = 21.21\ldots. \tag{2.8}$$

3 Some results from algebraic geometry and a necessary condition for existence of an integral

An *algebraic curve* in the affine plane is defined to be the solution set of $f(x, y) = 0$, where f is polynomial in two indeterminates, with coefficients in a given field K. An algebraic curve C in the projective plane (or a *projective curve*) is defined to be the solution set of the equation

$$C: \quad F(X, Y, Z) = 0 \tag{3.1}$$

where F is a homogeneous polynomial of positive degree. A curve is invariably specified with respect to a given field, which must necessarily contain the coefficient field K (lest it has no points on it). A *singular point* of the curve (3.1) is defined to be a (projective) solution of $\nabla F = (0, 0, 0)$. A curve is called *irreducible* over the appropriate coefficient field, if F does not factor into the product of two non-constant polynomials. When we consider (3.1) over $\mathbf{P}(\mathbf{F}_p^2)$, we have the following celebrated result [15, Theorem V.2.3]: [2]

[2] We are indebted to James Hirschfeld for some clarifying discussions on the Hasse-Weil bound.

Height	Cycle lengths	Terminating component lengths	# Points on level set
0	2,2,2,2,2,2	a1a,a1a,b1b,b1b	18
1	none	a1b,a1b,b2a,b2a	8
2	none	a1a,b1b,a5a,b5b	14
3	7	a1a,b1a,b1b	12
4	1,1	a2b,b3a,a7b,b8a	24
5	none	a1b,b2a,a4b,b5a	14
6	none	a2a,b2b,a3b,b4a	13
7	none	a2b,b3a,a5b,b6a	18
8	3,3	a2a,a2a,b2b,b2b	16
9	none	a3b,a3b,b4a,b4a	16
10	none	b1a,a4a,b4b	11
11	3,3,3	b1a,b1a	13
12	none	a4a,a4a,b4b,b4b	18
∞	1,1,1,1,1,1,1,1,1,1,1,1	a, b	14

Table 2. Orbit length data for the projective map (2.5) modulo 13, organized by level set height of its integral (2.7). In terminating orbits,'a' denotes the base point $(1,0,0)$ and 'b' the base point $(0,1,0)$. The notation 'a2b', for example, refers to an orbit of 2 affine points, where the second point maps under the map to b, whereas the first point maps under the inverse map to a (so that 4 points of the projective plane are in this orbit segment).

Theorem 1. *(Hasse-Weil) Let C be an irreducible projective curve of genus g defined over the finite field $\mathbf{F}_p$. Then $\#C$, the number of points on C with coordinates in $\mathbf{P}(\mathbf{F}_p^2)$, satisfies*

$$\#C \leq HW_g(p) + \#C_s, \tag{3.2}$$

where

$$HW_g(p) := p + 1 + 2g\sqrt{p} \tag{3.3}$$

and $\#C_s$ is the number of singular points on the curve. That is, $HW_g(p)$ is a bound for the number of non-singular points on C.

In (3.2), g is the *genus* of the curve (3.1), a non-negative integer characterizing the complexity of the curve, which remains invariant under birational coordinate transformations. If d is the degree of F, and if all singular points of the curve are *double* points, meaning the vector of second partial derivatives of F is non-vanishing at the points, then

$$g = \frac{1}{2}(d-1)(d-2) - \#C_s. \tag{3.4}$$

The Hasse-Weil upper bound (there is an analogous lower bound) gives a much stronger result than can be obtained by elementary methods (it is equivalent to the Riemann Hypothesis for algebraic function fields [15]). For example, induction can be used to show that the equation $F(X,Y,Z) = 0$, where F is homogeneous of degree $d \geq 1$, has at most

$d(p+1)$ solutions in $\mathbf{P}(\mathbf{F}_p^2)$ [10, Theorem 6.15]. The latter bound does not require any knowledge of singularities or reducibility of F.

Now consider a rational map L of the (real or complex) plane and suppose it has a rational integral I. By using projective coordinates, we can associate to L a projective map $\tilde{L}$ acting on $\mathbf{P}(\mathbf{C}^2)$ (as illustrated in the previous section). Furthermore, if $I(x,y) = n(x,y)/d(x,y)$, with $n(x,y)$ and $d(x,y)$ relatively prime polynomials, then

$$\tilde{I}(\tilde{L}\mathbf{X}) = \tilde{I}(\mathbf{X}), \qquad \tilde{I} = \frac{N(X,Y,Z)}{Z^\alpha\, D(X,Y,Z)}, \tag{3.5}$$

where $\mathbf{X} := (X,Y,Z)$, $\alpha = \deg n(x,y) - \deg d(x,y)$ and

$$N(X,Y,Z) = Z^{\deg n(x,y)}\; n\,(X/Z, Y/Z)$$
$$D(X,Y,Z) = Z^{\deg d(x,y)}\; d\,(X/Z, Y/Z).$$

The homogeneous polynomials $N(X,Y,Z)$ and $D(X,Y,Z)$ have the same degree as $n(x,y)$ and $d(x,y)$, respectively. The level set of $\tilde{I}$ of height h is an algebraic curve given by (cf. 3.1)

$$C_h: \quad F(X,Y,Z) = N(X,Y,Z) - h\, Z^\alpha\, D(X,Y,Z) = 0, \tag{3.6}$$

where the degree of the homogeneous polynomial F is the same as that of n. The level set $h = \infty$ can alternatively be viewed as the 0-level set of $\tilde{I}^{-1}$. If $\alpha \neq 0$, it is reducible. Points that simultaneously satisfy $N(X,Y,Z) = 0$ and $Z^\alpha\, D(X,Y,Z) = 0$ give $\tilde{I}$ an indeterminate value and are base points. Singularities of C_h are solutions of $\nabla\tilde{I} = (0,0,0)$, and solutions of $\nabla\tilde{I} = (0,0,0)$ on C_h yield its singularities.

We assume that our original map L has infinite order, otherwise it is dynamically not interesting. In this case, we can conclude that each level curve C_h has genus $g = 1$ or $g = 0$. We follow an argument given in [17, page 35]. Firstly, Hurwitz theorem tells us that the automorphism group of an algebraic curve with genus $g \geq 2$ is finite. Since all but a finite number of curves in the family $\{C_h\}$ will have the same genus, the map being of infinite order precludes this genus being 2 or higher. Consequently, generically, the genus of a typical curve of $\{C_h\}$ is $g = 1$. Curves on which additional singularities occur will have genus $g = 0$.

Suppose now that our map $\tilde{L}$ is representable modulo p, meaning the coefficients in the expressions for X', Y' and Z' reduce well modulo p (we will say more on reduction in Section 5). Suppose its integral $\tilde{I}$ also reduces well modulo p, to a non-constant rational function. Then (3.5) shows that the orbit of any chosen initial condition $\mathbf{X} \in \mathbf{P}(\mathbf{F}_p^2)$ will lie on the algebraic curve (3.6) of height $h = \tilde{I}(\mathbf{X})$. If this curve is irreducible, applying Theorem 1 with $g = 1$ now gives a bound on the number of points in this orbit:

Theorem 2. *Let L be a rational map which is representable over the finite field $\mathbf{F}_p$. Let $\mathcal{O}_p(\mathbf{X})$ denote the maximal (forward and backward) orbit of its projective version $\tilde{L}$ containing a given $\mathbf{X} \in \mathbf{P}(\mathbf{F}_p^2)$ (using L^{-1}, when it exists, to generate the pre-images of $\mathbf{X}$). If L has a rational integral that is representable over $\mathbf{F}_p$ and the level set containing $\mathbf{X}$ is irreducible, then*

$$\#\mathcal{O}_p(\mathbf{X}) \leq\; p + 1 + 2\sqrt{p} + \#C_s. \tag{3.7}$$

If $\mathcal{O}_p(\mathbf{X})$ is a cycle, its points are all singular points or all non-singular points on the level set. In the former case, $\#\mathcal{O}_p(\mathbf{X}) \leq \#C_s$, and in the latter case $\#\mathcal{O}_p(\mathbf{X}) \leq p + 1 + 2\sqrt{p}$.

The statement about cycles in Theorem 2 derives from some restrictions on how singular points of the curve can occur in orbits. Differentiating (3.5) gives

$$d\tilde{L}(\mathbf{X})^T \ \frac{\partial \tilde{I}}{\partial \mathbf{X}}(\tilde{L}\mathbf{X}) = \frac{\partial \tilde{I}}{\partial \mathbf{X}}(\mathbf{X}), \tag{3.8}$$

where superscript T denotes matrix transpose. From this (cf. [8, Appendix A]) we deduce that if $\tilde{L}\mathbf{X}$ is a solution of $\nabla \tilde{I} = (0,0,0)$, then so is $\mathbf{X}$. The converse is also true provided $\det d\tilde{L}(\mathbf{X}) \neq 0$. If $\tilde{L}$ and $\tilde{I}$ reduce modulo p, these conclusions are also true over $\mathbf{F}_p$ (the determinantal condition should be now taken modulo p). Cycles containing one singular point must contain only singular points.

Because we are principally interested with the Hasse-Weil bound (3.3) with $g = 1$, we will denote $HW_1(p)$ by simply $HW(p)$.

The results of Tables 1 and 2 of the previous section illustrate Theorems 1 and 2. Modulo 11, it can be checked that every level set of $\tilde{I}$ of (2.7) is irreducible and has no singular points in the affine plane $\mathbf{F}_{11}^2$, but that the base points $(1,0,0)$ and $(0,1,0)$ are singular points on every level set. In Table 1, the cycle of length 18 in the affine plane $\mathbf{F}_{11}^2$ achieves the maximum possible size given $HW(11)$ of (2.4). Modulo 13, the only level set of $\tilde{I}$ of (2.7) that is reducible is that with height 4 with

$$C_4 : (8xz + xy + 5yz - z^2)(5xz + xy + 8yz + 4z^2) = 0. \tag{3.9}$$

This accounts for the total number of points being 24. Each of the factors in (3.9) has genus 0 (is a *conic*) and no singular points. In this case, Hasse-Weil's result gives that each curve derived from the factors has *exactly* $p + 1 = 14$ points. There are 4 points common to both curves: $(2,9,1)$, $(4,11,1)$ and the base points $(1,0,0)$ and $(0,1,0)$.

It follows from Theorem 2 that if the orbit bounds are exceeded for an integrable map which reduces, together with its integral, modulo p, then the level set containing the orbit must be reducible. For example, the McMillan map:

$$x' = y\ , \qquad y' = -x - (1+2y)/(1+y^2) \tag{3.10}$$

has the integral $x^2y^2+x^2+y^2+2xy+x+y$ (see also [14]). When $p = 97$, the longest orbit has length 179, being the only orbit exceeding $HW(97) = 117.69\ldots$. It is found that the level set of height 24 containing this orbit factors: $(75y+86+(y+75)x)(22y+11+(y+22)x) = 0$. Each factor generates a conic with $p + 1 = 98$ points in projective space. The given orbit with 179 points achieves its length by moving between the two component conics.

4 Comparison of orbit statistics for integrable and non-integrable maps

In this section, we display evidence that Theorem 2 forms the basis of a strong negative criterion for integrability. That is, if a map does not have a (rational) integral, then it appears to have a significant proportion of orbits that exceed the bound based on Hasse-Weil. We also identify other quantities based on orbit statistics that act as reliable discriminators between integrability and non-integrability. For additional evidence on other maps, see [14].

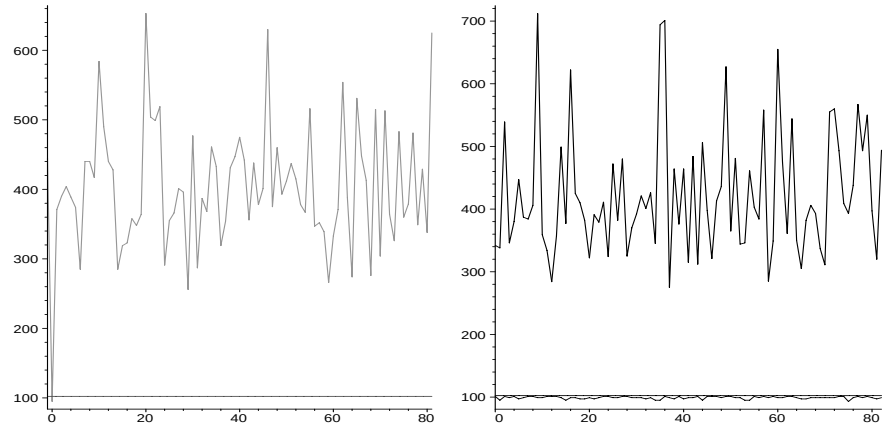

Figure 2. Left: Maximal orbit length versus δ for (4.1) when $(\epsilon, \xi, \lambda) = (1, 1, -1)$. Right: Maximal orbit length versus ϵ for (4.1) when $(\delta, \xi, \lambda) = (0, 1, -1)$ (bottom) and $(\delta, \xi, \lambda) = (3, 1, -1)$ (top). In each figure, $p = 83$ and the horizontal line represents the bound $HW(83)$.

We consider the 4-parameter family of rational area-preserving maps:

$$x' = -x - \frac{\delta y^2 + \epsilon y + \xi}{y^2 + 1}\,, \qquad y' = -y - \frac{\epsilon x' + \lambda}{(x')^2 + 1}. \tag{4.1}$$

When $\delta = 0$, each map is an asymmetric QRT map [13] with integral

$$I(x, y) = x^2y^2 + x^2 + y^2 + \epsilon xy + \xi x + \lambda y. \tag{4.2}$$

Observe that the integrable map (2.1) discussed previously corresponds to taking $\delta = 0$, $\epsilon = \xi = 1$, $\lambda = -1$.

We have made various numerical studies of the family (4.1) over finite fields. We first calculate the projective versions of these maps, as per the special case (2.5). We then calculate the orbit structure on the $p^2 + p + 1$ points of the projective space $\mathbf{P}(\mathbf{F}_p^2)$. The parameter space is *finite*, namely $\mathbf{F}_p^4$, and we sample various subsets of this space. Each selection of a parameter vector $(\delta, \epsilon, \xi, \lambda) \in \mathbf{F}_p^4$ corresponds to studying the reduction over the finite field of an *infinite equivalence class of maps*, e.g., those maps with rational parameters that reduce to the chosen vector. We return to this point below in Section 5.

As with (2.1), the dynamics of (4.1) depends on the nature of the prime p. When $p \equiv 3 \,(\mathrm{mod}\ 4)$, the map is invertible and all orbits are cycles. When $p \equiv 1 \,(\mathrm{mod}\ 4)$, cycles coexist with terminating orbits. Computationally, we find the orbits by constructing an *orbit graph* on the space $\mathbf{P}(\mathbf{F}_p^2)$, connecting two points with an oriented arc once one point is the image of the other under the map. Decomposing the graph into its connected subgraphs reveals the cycles and highlights (if any) those non-invertible points of the dynamics where many terminating orbits meet at a common vertex. Of course, this process of identifying orbits and counting the number of points they contain can be done in the absence of any knowledge of the existence of an integral for the map.

The left plot in Figure 2 shows that in a one-parameter subfamily of (4.1), parametrized by δ, the known integrable case $\delta = 0$ is distinguished by being the only parameter value for which the maximal orbit length lies below the appropriate Hasse-Weil value. The

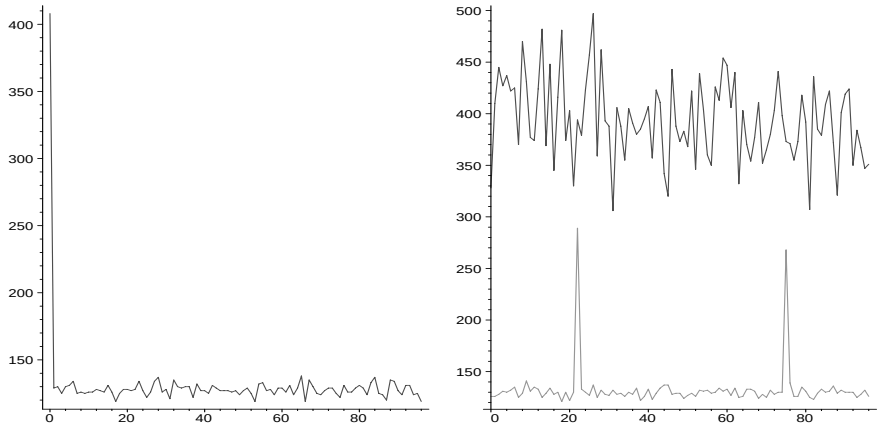

Figure 3. Left: Number of cycles versus δ for (4.1) when $(\epsilon, \xi, \lambda) = (1, 1, -1)$. Right: Number of cycles versus ϵ for (4.1) when $(\delta, \xi, \lambda) = (0, 1, -1)$ (top) and $(\delta, \xi, \lambda) = (3, 1, -1)$ (bottom). In each figure, $p = 97$.

right plot of Figure 2 combines the data for a one-parameter integrable subfamily of (4.1) (with $\delta = 0$) with another one-parameter subfamily (with $\delta = 3$) which is apparently not integrable. Our empirical experience is that using $HW(p)$ on the maximal orbit length as a method to isolate integrable parameter values is a useful selection method. It tends to overselect possible integrable parameter values for small primes ($\simeq 50$), but becomes increasingly discriminating for larger ones up to 100 (see Table 1 of [14] for an illustration). Of course, an integrable parameter value might not be selected at all using this criterion if the longest orbit derives from a reducible integral level curve (as occurs for (3.10) of the previous section). However, even allowing for this, the proportion of phase space occupied by orbits whose length is less than $HW(p)$ in a non-integrable map is significantly less than 1 (empirically, we find for $p > 50$, this proportion is already below 40 per cent). Thus, mean orbit length in an integrable map should effectively be bounded by $HW(p)$ but this is not true for a non-integrable map.

A consistently reliable selector of integrable parameter values, which does not appear to overselect, is illustrated in Figure 3. We consider only the orbits that are cycles in the projective space $\mathbf{P}(\mathbf{F}_p^2)$ and count their number. Integrable maps are distinguished by a markedly *larger* number of cycles than non-integrable maps. An explanation for this, and a statistical analysis of the envelope of the number of cycles data for integrable and non-integrable maps, is currently being investigated. Note in the righthand plot of Figure 3, the two spikes in the data for the non-integrable family occurring at $\epsilon = 22$ and $\epsilon = 75$. The data is alerting to the fact that for these two epsilon values and $\lambda = -1$, the map takes a different (non-integrable) form. This happens at these ϵ values because the numerator in the rational part of y' in (4.1) equals one of the factors in the denominator, allowing a cancellation (note: $(x')^2 + 1 \equiv (x' - 75)(x' - 22) \,(\mathrm{mod}\ 97)$).

Calculating the maximal orbit length or the number of cycles requires a complete orbit decomposition of the projective space $\mathbf{P}(\mathbf{F}_p^2)$. This becomes computationally laborious for primes p exceeding 100. An alternative approach which samples the dynamics for large primes is to take a randomly chosen initial condition and to calculate its orbit length modulo p as p increases. Suppose the conditions of Theorem 2 are satisfied for a sequence

of increasing primes $p_i \to \infty$ with corresponding initial conditions $\mathbf{X}_i$. From (3.7) it follows that if we *normalize* orbit lengths by $HW(p_i)$ and go to larger primes

$$\lim_{p_i \to \infty} o_{p_i}(\mathbf{X}_i) := \frac{\#\mathcal{O}_{p_i}(\mathbf{X}_i)}{HW(p_i)} \leq 1, \tag{4.3}$$

since, by assumption, any integral is assumed to have a finite number of singular points. A systematic choice of $\mathbf{X}_i$ is the reduction modulo p_i of the same $\mathbf{X} \in \mathbf{Q}^2$. This amounts to studying the image over various finite fields of the same rational orbit.

It is evident that for an integrable map L, the normalized orbit lengths $o_{p_i}(\mathbf{X}_i)$ should largely be confined to the interval (0,1). Heuristically, we find this to be the case on examples tested, see the left plot of Figure 4 (in both plots of Figure 4, $\mathcal{O}_{p_i}(\mathbf{X})$ is the maximal (forward and backward) orbit of the map containing $\mathbf{X}$). Exceptions might occur when the level set containing $\mathbf{X}_i$ is reducible modulo p_i. Indeed, for the map (3.10) discussed previously, $o_{p_i}(\mathbf{X})$ for the chosen $\mathbf{X}$ in Figure 4 exceeds 1 only at primes 37, 97 and 397, which are precisely the only primes in the range considered when the level set of the integral is reducible. Statistically, as we move through the primes, exceptional normalized lengths exceeding 1 in the integrable case because of reducibility of the level set appear to be rare.

In contrast, when we plot the normalized orbit lengths for a randomly chosen initial condition for a non-integrable map, we find values exceeding 1 are very common. We illustrate this in the right plot of Figure 4 with the map

$$x' = y, \qquad y' = -x + y + \frac{\epsilon}{y^2}. \tag{4.4}$$

This map satisfies singularity confinement, but is non-integrable for $\epsilon \neq 0$. This can be deduced from its non-zero algebraic entropy and confirmed by a phase portrait [7]. Other indications of its non-integrability have been given in [16, 9].

It is worth noting that a finer analysis of normalized orbit lengths obtained from reductions of rational maps (e.g., the cumulative distribution function for the normalized lengths) reveals some characteristic features that are different for the integrable and non-integrable case [14].

5 Reduction, sieving, and lack of near integrability

Each point in a finite field is congruent to infinitely many rational numbers, and indeed to a set of rationals which is *dense* on the real line. Therefore in reducing coordinates and parameters from the rational field to a finite field there is a dramatic loss of information.

The question arises as to how to recover a rational value (an integrable parameter value, in our case) when all the information we have about it is modulo p. This is indeed possible —in an asymptotic sense— using a sieve method based on continued fractions, which we briefly describe [14]. Fix a rational r/s, and a set of primes p_i coprime to s. Then there exist unique integers k_i, $0 \leq k_i < p_i$, such that $r/s \equiv k_i \,(\mathrm{mod}\ p_i)$. This set of congruences is in bi-unique correspondence with a single congruence $r/s \equiv A \,(\mathrm{mod}\ M)$, where $M = \prod p_i$, and $0 \leq A < M$. For all sufficiently large M, $r/s = Am - Ma$, for one convergent a/m in the continued fractions expansion of A/M, while the other convergents

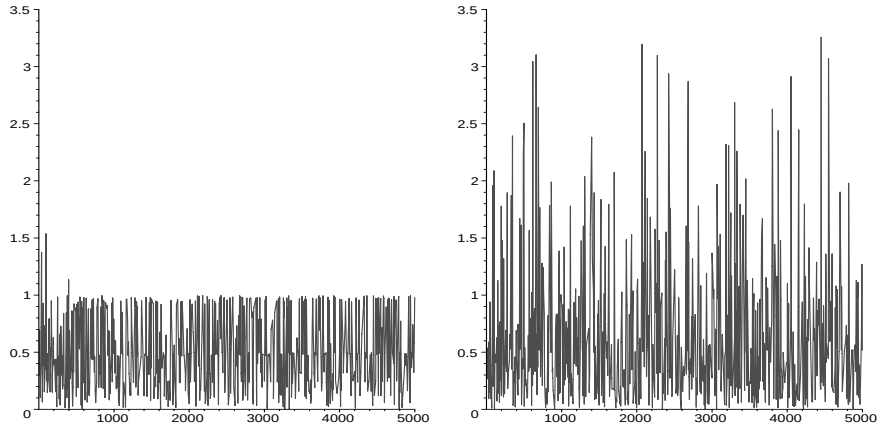

Figure 4. Normalized orbit lengths $o_{p_i}(\mathbf{X})$ plotted against primes p_i ($7 \leq p_i < 5000$) for: Left, the integrable map (3.10) and $\mathbf{X} = (42, 71, 1)$; and: Right, the non-integrable map (4.4) with $\epsilon = 7$ and $\mathbf{X} = (31/10, 31/10, 1)$.

give spurious solutions r'/s'. Defining the *height* h of a rational as $h(r/s) = |rs|$, we find that all spurious solutions have diverging height, and fluctuate erratically. This makes the identification of r/s possible.

For instance, the rational $r/s = -5/3$ is congruent to $k = 19, 23, 12, 27, 14$ modulo the primes $p = 31, 37, 41, 43, 47$, respectively. The three rationals of smallest height satisfying these congruences are: $-\frac{5}{3}$,$-\frac{1}{19008314}$, -31680524, which clearly illustrates the divergence of height.

One by-product of the reduction process is the disappearance of the concept of 'near integrability', which rests crucially on the topology of the real line. For dynamics on manifolds, the powerful KAM theory shows that near-integrable systems (in discrete or continuous time) retain some features of integrable ones. In the case of symplectic mappings, the KAM theory ensures that a set of positive measure of invariant curves of an integrable map are retained under a sufficiently small canonical perturbation, see [2, Chapter 6], [13, Section 5] for overviews. This is a form of continuity which enhances even further the significance of integrable systems. On the other hand, however, it also causes the convergence (albeit not necessarily uniform) of an observable to its integrable value as we approach the integrable regime, which makes integrability testing chronically difficult.

The study of phase portraits of a real mapping near an integrable regime is a telling example of such difficulties, requiring looking in the right place at the right magnification in order to locate stochasticity. Likewise, measuring entropy in parametrized families of real maps containing integrable cases so as to locate the latter is numerically very exacting.

Here, the reduction of phase space and parameter space modulo p destroys any notion of near-integrability because the topology is discrete. For a dramatic illustration, let $\epsilon = 0$ represent the integrable parameter value in a family of maps. Then, for any integer a and prime p, one can find a sequence of rational parameters $\epsilon_k \to 0$, which are congruent to a modulo p for every k, e.g., $\epsilon_k = a/(1 + kp)$. By the same token, one could construct a sequence $\epsilon_k \to \infty$ with the same congruence property. This means that, over the real/complex field, an orbit of a point in a nearly-integrable map and the orbit of the same point in a far-from-integrable map can reduce over the finite field to *one and the*

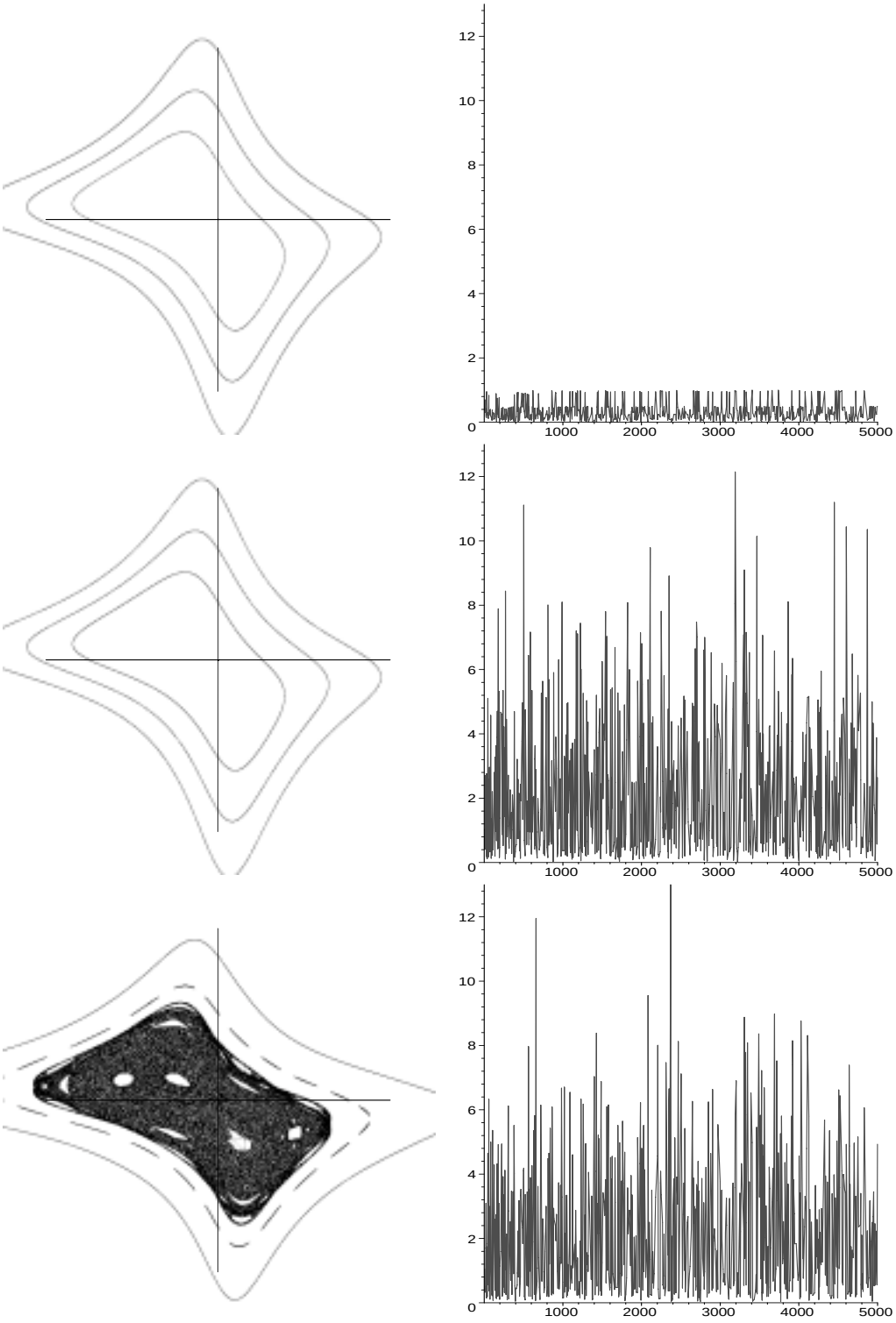

Figure 5. Each figure in the left column shows part of the real phase portrait of (4.1) with $(\epsilon, \xi, \lambda) = (1, 1, -1)$ and $\delta = 0$ (top), $\delta = 10^{-4}$ (middle), $\delta = 1$ (bottom). In each portrait, the orbits of initial conditions $(1, 0)$, $(1, 1)$ and $(1, 2)$ are plotted. In the right column, the normalized lengths of the orbit of $(1, 1, 1)$ in $\mathbf{P}(\mathbf{F}_p^2)$ are plotted as a function of p for the corresponding map parameter values.

same orbit for the *same* reduced map. Our methodology gives prominence to genuine integrability by causing near-integrable and far-from-integrable (as seen in a continuum of real/complex parameters) to attain the same status upon reduction. (The resolution of this apparent paradox is that merging measurements made over several finite fields shows that the height of the spurious rational parameter values diverges.)

Figure 5 illustrates this point. The same three initial conditions yield the top phase portrait for the integrable map and the middle phase portrait for the near-integrable perturbation of this map. Although the curves in corresponding portraits appear largely indistinguishable, reduction over finite fields of orbits lying on them reveals a great difference. The normalized orbit length plots for each initial condition in the near-integrable map, as illustrated for $(1, 1, 1)$, are similar to those found for the far-from-integrable map depicted at the bottom of the figure. One plausible explanation for this is that the KAM curves are *not* algebraic curves, as distinct from the level curves of the integral, so that the Hasse-Weil theory and bound are *not* applicable. Figure 5 further reinforces the usefulness of plotting orbit lengths normalized by $HW(p_i)$ against p_i as a decisive and computationally-efficient discriminator of (algebraic) integrability.

References

[1] Ablowitz M J, Halburd R and Herbst B, On the extension of the Painleve property to difference equations, *Nonlinearity* **13** (2000), 889–905.

[2] Arrowsmith D K and Place C M, An introduction to dynamical systems, Cambridge University Press, Cambridge, 1990.

[3] Bellon M P and Viallet C-M, Algebraic entropy, *Commun. Math. Phys.*, **204** (1999), 425–437.

[4] Grammaticos B, Nijhoff F W and Ramani A, Discrete Painleve equations, in The Painleve Property: One Century Later, Editor: Conte R, Springer, New York, 1999, 413–516.

[5] Grammaticos B, Ramani A, and Papageorgiou V, Do integrable mappings have the Painleve property?, *Phys. Rev. Lett.* **67** (1991), 1825–1828.

[6] Hardy G H and Wright E M, An introduction to the theory of numbers, Oxford University Press, Oxford, (1979).

[7] J. Hietarinta and C. Viallet, Singularity confinement and chaos in discrete systems, *Phys. Rev. Lett.* **81** (1998), 325–328.

[8] Iatrou A and Roberts J A G, Integrable mappings of the plane preserving biquadratic invariant curves II, *Nonlinearity* **15** (2002), 459–89.

[9] Lafortune S and Goriely A, Singularity confinement and algebraic integrability, preprint, University of Arizona at Tucson (2002).

[10] Lidl R and Niederreiter H, Finite fields, Addison-Wesley, Reading, (1983).

[11] Quispel G R W, Roberts J A G and Thompson C J, Integrable mappings and soliton equations, *Phys. Lett. A* **126** (1988), 419–421; Quispel G R W, Roberts J A G and Thompson C J, Integrable mappings and soliton equations II, *Physica D* **34** (1989), 183–192.

[12] Rerikh K V, Algebraic-geometry approach to integrability of birational plane mappings. Integrable birational quadratic reversible mappings. I, *J. of Geometry and Physics* **24** (1998), 265–290.

[13] Roberts J A G and Quispel G R W, Chaos and time-reversal symmetry. Order and chaos in reversible dynamical systems, *Phys. Rep.* **216** (1992), 63–177.

[14] Roberts J A G and Vivaldi F, Arithmetical method to detect integrability in maps, *Phys. Rev. Lett.* **90** (2003), 034102; also Publisher's Note, *Phys. Rev. Lett.* **90** (2003), 079902.

[15] Stichtenoth H, Algebraic function fields and codes, Springer-Verlag, New York, 1991.

[16] Takenawa T, Algebraic entropy and the space of initial values for discrete dynamical systems, *J. Phys. A: Math. Gen.* **34** (2001), 10533–10545.

[17] Veselov A P, Integrable maps, *Russian Mathematical Surveys* **46** (1991), 1–51.

[18] Viallet C-M, Complexity and integrability, in SIDE III, *CRM Proc. Lec. Notes* **25**, AMS, Providence, (2000), 439-444.