An algebraic geometric approach to integrable maps of the plane

2006 J. Phys. A: Math. Gen. 39 1133

(http://iopscience.iop.org/0305-4470/39/5/008)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **39** (2006) 1133–1149 doi:10.1088/0305-4470/39/5/008

An algebraic geometric approach to integrable maps of the plane

Danesh Jogia[1], **John A G Roberts**[1,3] **and Franco Vivaldi**[2,4]

[1] School of Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
[2] School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, United Kingdom

E-mail: daneshj@maths.unsw.edu.au, jag.roberts@unsw.edu.au and f.vivaldi@maths.qmul.ac.uk

Received 19 September 2005, in final form 2 December 2005
Published 18 January 2006
Online at stacks.iop.org/JPhysA/39/1133

Abstract

We show that the dynamics of a birational map on an elliptic curve over a field is, typically, conjugate to addition by a point (under the associated group law). When the field is taken to be the function field of rational complex functions of one variable, this amounts to an algebraic geometric version of the Arnold–Liouville integrability theorem for planar integrable maps. By-products of this approach are that birational maps preserving foliations are necessarily the composition of two involutions, and that relationships between birational maps preserving the same foliation can be described in terms of the respective points they add on the corresponding Weierstrass curves. When the result is applied to finite fields, it helps explain some universal features of the periodic orbit distribution function for the reductions of integrable maps.

PACS numbers: 02.10.−v, 02.30.Ik, 02.40.−k

1. Introduction

In recent years there has been a growing interest in the study of time-discrete integrable systems (integrable maps); see [31] and the excellent review [4] and references therein. In particular, planar integrable maps have received much attention. Traditionally, a planar integrable map L has been taken to be a rational map of the (real or complex) plane that is measure-preserving[5]

[3] www.maths.unsw.edu.au/~jagr.
[4] www.maths.qmul.ac.uk/~fv.
[5] Recall [22, chapter 2.2] that $L : \boldsymbol{x} \mapsto \boldsymbol{x}'$ with $\boldsymbol{x} \in \mathbb{R}^2$ is (anti) measure-preserving with density $m(\boldsymbol{x})$ if the Jacobian determinant $J(\boldsymbol{x}) := \det \mathrm{d}L(\boldsymbol{x})$ can be written $J(\boldsymbol{x}) = (-)\frac{m(\boldsymbol{x})}{m(\boldsymbol{x}')}$. The latter is equivalent to $\int_V m(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x} = (-)\int_{L(V)} m(\boldsymbol{x}')\,\mathrm{d}\boldsymbol{x}'$ for any region V in $\mathbb{R}^2$ (anti measure-preservation corresponds to L being measure-preserving and orientation-reversing).

and possesses one rational integral $I(x, y) = n(x, y)/d(x, y)$, with $n(x, y)$ and $d(x, y)$ coprime polynomials, satisfying

$$I(x', y') = \frac{n(x', y')}{d(x', y')} = \frac{n(x, y)}{d(x, y)} = I(x, y), \tag{1}$$

where primes denote application of the map L. The invariance of $I(x, y)$ implies that the dynamics of L is confined to the level sets of I, i.e., the one-parameter family of curves

$$n(x, y) - td(x, y) = 0. \tag{2}$$

In (2), the height t of I parametrizes the family. A choice of initial condition (x_0, y_0) in the plane fixes $t = t^* = I(x_0, y_0)$ and thereafter the dynamical interest is to understand the motion induced by L on the invariant curve $n(x, y) - t^* d(x, y) = 0$. As an example, we mention the asymmetric case of the widely-studied QRT family of integrable planar maps [19, 20]. In this case, L takes the form

$$x' = \frac{f_1(y) - xf_2(y)}{f_2(y) - xf_3(y)} \qquad y' = \frac{g_1(x') - yg_2(x')}{g_2(x') - yg_3(x')}, \tag{3}$$

where f_i and g_i are particular quartic polynomials. Letting

$$X := \begin{pmatrix} x^2 \\ x \\ 1 \end{pmatrix} \qquad Y := \begin{pmatrix} y^2 \\ y \\ 1 \end{pmatrix}, \tag{4}$$

and letting A_0 and A_1 be constant 3×3 matrices, then the polynomials f_i can be neatly expressed as components of cross products:

$$(f_1, f_2, f_3)(y) = (A_0 Y) \times (A_1 Y), \qquad (g_1, g_2, g_3)(x') = \left(A_0^T X'\right) \times \left(A_1^T X'\right), \tag{5}$$

while the integral is the ratio of two biquadratics

$$I(x, y) = \frac{X \cdot A_0 Y}{X \cdot A_1 Y}. \tag{6}$$

The level sets of I correspond to particular one-parameter families of biquadratic curves:

$$\begin{aligned} B(x, y, t) = {} & \alpha(t)x^2y^2 + \beta(t)x^2y + \delta(t)xy^2 + \gamma(t)x^2 + \kappa(t)y^2 \\ & + \epsilon(t)xy + \xi(t)x + \lambda(t)y + \mu(t) = 0, \end{aligned} \tag{7}$$

in which the coefficients are affine functions of t.

The purpose of this paper is to elucidate the dynamics of a birational map (a rational map with rational inverse) that acts on an algebraic curve C, one defined by a polynomial function of the variables. An obvious motivation is the aforementioned induced dynamics of a rational integrable map on the level sets of its rational integral. However, the results here have wider applicability. In the first instance, this is because the results apply to the case where a family of algebraic curves is preserved by a non-rational map of the plane that acts birationally on each curve (see [5, 6] for examples of the latter involving quite general parametrized families of biquadratics (7)). In the second instance, this is because our methods use results from algebraic geometry that are applicable over a quite general field K, including all fields of characteristic zero and all finite fields (excluding characteristics 2 and 3).

It will be shown below that the generic problem is to understand the dynamics when C is an elliptic curve E defined over a field K, denoted E/K. In this case, theorem 3 shows that, typically, the dynamics of a birational map is conjugate to a translation

$$P \mapsto P + \Omega \tag{8}$$

on the Abelian group formed by the points of E (P is an arbitrary point on E, Ω is a particular point with coordinates in K on E and '+' is the associated group law on the Weierstrass cubic

corresponding to E). A variant of this result characterizes birational maps that preserve a planar foliation of algebraic curves (theorem 4).

Examples or special cases of our result for $K = \mathbb{C}$ (more properly, for the rational function field over $\mathbb{C}$) have appeared recently in the literature. In [29], it is shown constructively that the dynamics of the symmetric or asymmetric QRT maps on their families of preserved biquadratics (7) is equivalent to (8) on the corresponding Weierstrass cubics. Earlier, in [3], which studies the geometry of repeated folding of quadrilaterals, this was shown explicitly for the square of a simple case of a symmetric QRT, namely[6]

$$T_\alpha : x' = y, \qquad y' = \frac{y+\alpha}{x}. \tag{9}$$

Also, [32] showed explicitly that examples of the rational maps of [9], which possess an integral that is a ratio of *biquartics* in x and y, could be reduced to additions on associated Weierstrass curves. Other planar integrable rational maps conjugate to translations have been described in [1]. Finally, our results also relate to the algebraic geometric approaches to the Painlevé equations contained in [25] and [8] (in particular, the latter shows that the elliptic Painlevé equation of the former is equivalent to translation on a moving elliptic curve).

The one-to-one correspondence between the action of (infinite order) birational maps preserving algebraic curves with the corresponding points that they add via (8) affords an opportunity to compare maps acting on birationally equivalent curves by comparing the points that they add. This is done for both power-relations between maps (proposition 2) and conjugacy of maps (proposition 3). The correspondence to (8) also allows us to prove that birational maps preserving algebraic curves are the composition of two birational involutions (see proposition 1). This *reversibility* property is well known for the QRT maps; e.g., (3) is the composition $H \circ G$ with

$$H : x' = x, \quad y' = \frac{g_1(x) - y g_2(x)}{g_2(x) - y g_3(x)}, \qquad G : x' = \frac{f_1(y) - x f_2(y)}{f_2(y) - x f_3(y)}, \quad y' = y. \tag{10}$$

The plan of the paper is as follows. In section 2, we will give a few preliminaries from algebraic geometry that help make our discussion more self-contained. In section 3, we present our main theorem, its proof and some corollaries. In section 4, we discuss the application of the theorem when the field K is a function field. This allows all elliptic curves in a one-parameter family to be treated simultaneously (as in [29]) so that the added point Ω in (8) becomes a function of the curve in the family. In section 5, we discuss the application of the theorem when K is a finite field. We show how this can be used to explain some recent results ([21, 23]) concerning universal aspects of the distribution functions of periodic orbits of integrable maps over finite fields.

2. Preliminaries from algebraic geometry

Most of the theory we need can be obtained from [27]. We will assume throughout the paper that K is a field with a characteristic different from 2 or 3.[7]

An algebraic curve over K, denoted by C (or by C/K when the field needs to be made explicit), is the set of solutions of an equation $F(x, y) = 0$, where F is a polynomial with

[6] The map T_α actually has a rich history, as described in [3], having been previously studied by Lyness [14], and later by Zeeman (see also [10, 11], where various generalizations are also given). The fact that it had an integral was known already to Lyness. In this way, T_α appears to be one of the first systematically studied integrable maps, although the McMillan map [16] seems more well known in the integrable maps community.

[7] Although [27] assumes for the most part that K is a perfect field, our main tool—the conversion to Weierstrass form over the field K—is valid without this restriction (we are grateful to J Silverman and M Szydlo for clarification on this point).

coefficients in K.[8] One way to classify algebraic curves is via the *genus*, a non-negative integer dependent on the degree of F and on the number and nature of any singular points on C. An elliptic curve E/K is an algebraic curve of genus 1 with a distinguished point $\mathcal{O}$ with co-ordinates in K. The set of all points of E with co-ordinates in K, denoted $E(K)$, is called the set of K-rational points of E (so $\mathcal{O} \in E(K)$).

If E/K is an elliptic curve, there exists another curve W/K of the form

$$y^2 = x^3 + Ax + B \tag{11}$$

such that E and W are birationally equivalent. Furthermore, the birational map $\phi : E \to W$ that connects E and W can be taken to have coefficients in K and satisfy $\phi(\mathcal{O}) = [0, 1, 0] \in W(K)$. Here $[0, 1, 0]$, the (projective) point at infinity on W, is the distinguished point, $\mathcal{O}_W$, of W [27, proposition 3.1]. The curve W/K is called the Weierstrass cubic or Weierstrass normal form corresponding to E/K. The set $W(K)$ of K-rational points of W form an Abelian group with identity $[0, 1, 0]$. Geometrically, the group operation (which we write '+') corresponds to a chord-tangent construction on W [27, p 58]. The group law on W induces—via ϕ^{-1}—a group law on the original curve E (which we still call '+') with identity $\mathcal{O}$ [27, proposition 3.4]. The Weierstrass form (11) for a given E is not unique, e.g., the transformation

$$x' = u^2 x, \qquad y' = u^3 y, \tag{12}$$

where $u \in K^*$ returns a primed version of (11) with

$$A' = u^4 A, \qquad B' = u^6 B. \tag{13}$$

Conversely, any two Weierstrass forms W_1/K and W_2/K in the form (11) for the curve E/K are related by a transformation (12) with $u \in K^*$ [27, proposition 3.1].

A rational map defined over an algebraic curve C/K which maps the curve to itself is called a morphism of the curve. An isomorphism is a morphism with a rational inverse, and the set of birational maps of a curve to itself form a group. The following result is known as Hurwitz theorem [15]:

Theorem 1. *The group of birational maps of a smooth algebraic curve of genus $g \geqslant 2$ to itself is finite, of order at most $84(g - 1)$.*

As a consequence, there can be no infinite order birational maps preserving such a curve. For this possibility, one is then necessarily confined to elliptic curves (genus 1) or conics (genus 0); in relation to integrable maps, [31] appears to have been the first to apply Hurwitz theorem in this way.

An endomorphism of an elliptic curve E is a morphism $\iota : E \to E$ such that $\iota(\mathcal{O}) = \mathcal{O}$. It turns out that the invariance of $\mathcal{O}$ is sufficient to ensure that an endomorphism actually respects the group law on E [27, theorem 4.8]:

$$\iota(P_1 + P_2) = \iota(P_1) + \iota(P_2) \qquad \forall P_1, P_2 \in E(K). \tag{14}$$

Endomorphisms of elliptic curves are called *isogenies*. Any morphism of E can then be characterized as follows [27, p 75]:

Lemma 1. *Any morphism F defined over K that maps an elliptic curve E/K to itself can be written as the composition of an isogeny and a translation under the group law.*

Proof. Define $Q = F(\mathcal{O})$ and let T_Q be the translation that adds Q to its argument, i.e., $T_Q : P \mapsto P+Q$, and similarly, $T_{-Q} : P \mapsto P-Q$ which is the inverse of T_Q. It can be shown

[8] Strictly speaking, one works with projective coordinates $[X, Y, Z]$, with $x = X/Z$, $y = Y/Z$, so as to include points at infinity. For ease of notation, we try and present things using just the affine coordinates x and y as much as possible.

that T_Q and T_{-Q} are morphisms on E [27, theorem 3.6], whence they are isomorphisms. Then $T_{-Q} \circ F$ is an isogeny (as the image of $\mathcal{O}$ is $\mathcal{O}$), which we call ι. Then $F = T_{-Q}^{-1} \circ \iota = T_Q \circ \iota$ as required. □

Note in lemma 1 that $Q \in E(K)$, ensuring that ι is defined over K.

The endomorphisms of E form a ring (under composition and addition). The invertible endomorphisms, or automorphisms, form a group $\mathrm{Aut}(E)$ (hence the automorphisms are the birational maps of E to itself that preserve the identity element $\mathcal{O}$). The structure of the endomorphism ring, while well known, can be quite complicated [27, section III.9]. However the group of automorphisms of E is always a small cyclic group [27, section III.10].

Theorem 2. *The group $Aut(E)$ of automorphisms of an elliptic curve is isomorphic to either C_2, C_4 or C_6.*

Which possibility occurs for $\mathrm{Aut}(E)$ can be decided using $j(E)$, the j-invariant for the curve. For the Weierstrass form (11),

$$j(W) = 1728\frac{4A^3}{4A^3 + 27B^2}. \tag{15}$$

If E, and hence its corresponding W, are defined over K, then $j(E) = j(W) \in K$. More generally, any two elliptic curves which are birationally equivalent over K share the same j-invariant. Conversely, two elliptic curves with the same j-invariant are birationally equivalent over $\bar{K}$, the algebraic closure of K (and not necessarily over K).

3. Main theorem and corollaries

We can use the above results to now characterize the dynamics of a birational map on an elliptic curve. Because, computationally, it is useful to work with the Weierstrass version of E, we frame the proof in this setting. However, the statement of the theorem is actually correct with W replaced by E and the corresponding group law '+' on E. Recall that the notation E/K denotes an elliptic curve which has at least one point $\mathcal{O}$ with coordinates in K, the field of coefficients.

Theorem 3. *Let L be a birational map over K that leaves fixed an elliptic curve E/K with a corresponding Weierstrass curve W/K. Then L is conjugate to a birational map $\widetilde{L}$ which fixes W/K and can be expressed in terms of the group law $+$ on W as one of the following:*

(i) $\widetilde{L} : P \mapsto P + \Omega$
(ii) $\widetilde{L} : P \mapsto \iota(P) + \Omega$

where $\Omega = \widetilde{L}([0, 1, 0]) \in W(K)$ and ι is an automorphism of W/K of order 2, or possibly orders: 4 (if $j(E) = 1728$), 3 or 6 (if $j(E) = 0$). In case (ii), $\widetilde{L}$ (and hence L) has finite order, the same order as ι.

Proof. Let $\phi : E \to W$ be the birational map defined over K that takes E to its Weierstrass form W with $\phi(\mathcal{O}) = [0, 1, 0] \in W(K)$. Then the composition $\widetilde{L} = \phi \circ L \circ \phi^{-1}$ is a birational map defined over K that leaves W fixed. Its inverse is $\widetilde{L}^{-1} = \phi \circ L^{-1} \circ \phi^{-1}$. Let $\Omega = \widetilde{L}([0, 1, 0]) = \phi \circ L(\mathcal{O}) \in W(K)$. The proof of lemma 1 tells us that $\iota = T_{-\Omega} \circ \widetilde{L}$ is an isogeny over K on W. The inverse of ι exists, and is given by $\iota^{-1} = \widetilde{L}^{-1} \circ T_\Omega$, which is clearly a morphism of W. In fact, ι^{-1} is also an isogeny since

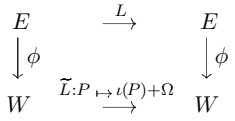

Figure 1. Commuting diagram, and group isomorphism, implied by theorem 3.

$\iota^{-1}([0,1,0]) = \widetilde{L}^{-1}(T_\Omega([0,1,0])) = \widetilde{L}^{-1}(\Omega) = [0,1,0]$. Hence ι is an automorphism over K of W with

$$\widetilde{L} = T_\Omega \circ \iota : P \mapsto \iota(P) + \Omega.$$

The possible automorphisms ι over K follow from theorem 2 and [27, theorem 10.1]. If $\iota = id$, we obtain case (i) listed above, that of a translation. Otherwise, on W of (11), automorphisms necessarily take the form (12) with $u \in K$ satisfying (13) with $A' = A$ and $B' = B$. Consequently, if $AB \neq 0$, so from (15) we see $j(E) \neq \{0, 1728\}$, then necessarily $u = \pm 1$, so the only new possibility apart from the translation is the involution $P \mapsto -P + A$. If $B = 0$ ($j(E) = 1728$), and $u \in K$ can be a fourth root of unity, the possibility of $\widetilde{L}$ of order 4 is created. If $A = 0$ ($j(E) = 0$), and $u \in K$ can be a 6th root of unity, the possibility of $\widetilde{L}$ of order 6 is created (its square then having order 3). □

Let $\mathcal{L}$ denote the group (under map composition) of birational maps over K that preserve the elliptic curve E/K. On a given Weierstrass W/K corresponding to E, consider the set

$$\widetilde{\mathcal{L}} = \{P \mapsto \iota(P) + \omega : \iota \in \mathrm{Aut}(W), \omega \in W(K)\}. \tag{16}$$

Each element of $\widetilde{\mathcal{L}}$ is a composition on W of an automorphism and a translation and, in fact, $\widetilde{\mathcal{L}}$ is a group

$$\widetilde{\mathcal{L}} = \mathcal{T} \rtimes \mathrm{Aut}(W), \tag{17}$$

where $\rtimes$ denotes semi-direct product and $\mathcal{T}$, a normal subgroup of $\widetilde{\mathcal{L}}$ which intersects $\mathrm{Aut}(W)$ only in the identity, is the (Abelian) group of translations

$$\mathcal{T} = \{P \mapsto P + \omega : \omega \in W(K)\}. \tag{18}$$

Theorem 3 then shows that the conversion $\phi : E \to W$ can be used to define a map

$$\Phi : \mathcal{L} \to \widetilde{\mathcal{L}} \qquad L \mapsto \widetilde{L} = \phi \circ L \circ \phi^{-1}, \tag{19}$$

which is easily seen to be a group isomorphism between $\mathcal{L}$ and $\widetilde{\mathcal{L}}$ (with inverse $\Phi^{-1} : \widetilde{L} \mapsto L = \phi^{-1} \circ \widetilde{L} \circ \phi$). This isomorphism is summarized by figure 1.

Since $\mathcal{T}$ of (18) is itself isomorphic to $W(K)$, we obtain information about the group $\mathcal{L}$ of birational maps of E from (17) and (19), namely

$$\mathcal{L} \simeq W(K) \rtimes \mathrm{Aut}(W). \tag{20}$$

In the typical situation (with respect to the j-invariant) when $\mathrm{Aut}(W) \simeq C_2$, a birational map that leaves invariant an elliptic curve corresponds, on W, to either

(i) a translation $P \mapsto P + \Omega$ (i.e., corresponds to an element of $\mathcal{T}$ of (18) and so commutes with all other birational maps that correspond to elements of $\mathcal{T}$); or
(ii) an involution $P \mapsto -P + \Omega$ (it is easily checked that $P \mapsto -P + S$, for any $S \in W(K)$ is always an involution).

Furthermore, the translation and the involutions of the aforementioned type are related:

Proposition 1. *A birational map L on an elliptic curve E corresponding to the translation $\widetilde{L} : P \mapsto P + \Omega$ is reversible, i.e., can be written as the composition $H \circ G$ of birational involutions, with G corresponding to $\widetilde{G} : P \mapsto -P + S$ and H to $\widetilde{H} : P \mapsto -P + \Omega + S$, where $S \in W$ is arbitrary.*

So it is clear that once L is identified as being conjugate to a translation (a sufficient condition is that L is infinite order), it can be decomposed into rational involutions in many ways depending on the choice of S. In particular, taking $S = \mathcal{O}$, we can use the decomposition of the translation into $\widetilde{G} : P \mapsto -P$ and $\widetilde{H} : P \mapsto -P + \Omega$. For more on the properties and history of reversible maps, see [12].

From (20), birational maps that correspond to translations are in one-to-one correspondence with points of $W(K)$. This elucidates various comparisons of birational maps preserving elliptic curves.

Proposition 2. *Let L_1 and L_2 be birational maps on an elliptic curve that correspond, respectively, to translations $P \mapsto P + \Omega_1$ and $P \mapsto P + \Omega_2$ on an associated Weierstrass. For $m, n \in \mathbb{Z}$,*

$$L_1^m = L_2^n \quad \Longleftrightarrow \quad m\Omega_1 - n\Omega_2 = \mathcal{O}_W = [0, 1, 0], \tag{21}$$

where

$$j\Omega_i := \underbrace{\Omega_i + \Omega_i + \cdots + \Omega_i}_{j\text{times}}.$$

Proof. This is an automatic consequence of the isomorphism Φ, noting that L_i^j is conjugate to $P \mapsto P + j\Omega_i$. □

Proposition 2 shows that L_1 and L_2 are power-related if and only if their corresponding points on W are linearly-dependent over $\mathbb{Z}$. As a particular case, taking L_2 as the identity, L_1 is of finite order m on the curve E/K if and only if

$$m\Omega_1 = \mathcal{O}_W = [0, 1, 0]. \tag{22}$$

This means that Ω_1 is a point of order m on W. Dynamically speaking, Ω_1 being of finite order m on W is equivalent to saying that all points on the curve E have one and the same period m under L.

A second comparison concerns conjugacy of birational maps. This will be treated in more detail elsewhere [7]. A special case of the results proved in [7] is the following:

Proposition 3. *Let L_1, L_2 be birational maps on, respectively, elliptic curves E_1 and E_2 with L_1 corresponding to the translation $P \mapsto P + \Omega_1$ on the associated Weierstrass W_1. If L_2 is birationally conjugate to L_1, i.e., if there exists G birational such that*

$$L_2 = GL_1G^{-1}, \tag{23}$$

then L_2 corresponds to a translation $P \mapsto P + \Omega_2$ on W_1 with

$$\Omega_2 = \iota(\Omega_1) \tag{24}$$

and $\iota \in Aut(W_1)$.

Note in proposition 3 that, necessarily, $E_2 = G(E_1)$ and E_2 and E_1 share the same j-invariant.

The Mordell–Weil theorem [26] tells us that the set of rational points $E(\mathbb{Q})$, or $W(\mathbb{Q})$ for the associated Weierstrass, is a finitely-generated Abelian group. This means that any point $\omega \in W(\mathbb{Q})$ can be written as a linear combination

$$\omega = k_1\omega_1 + k_2\omega_2 + \cdots + k_r\omega_r + T. \tag{25}$$

In (25), the ω_is have infinite order and are linearly independent, T is a so-called torsion point (it has finite order) and k_i are integers uniquely determined by ω. The integer $r \geqslant 0$ is called the rank of $W/\mathbb{Q}$ (or $E/\mathbb{Q}$). Furthermore, the set of all torsion points in $W(\mathbb{Q})$ is a finite subgroup with a known structure. Via the isomorphism Φ, a birational map L over $\mathbb{Q}$ of an elliptic curve $E/\mathbb{Q}$ that corresponds to a translation can be written uniquely as the composition

$$L = L_1^{k_1} L_2^{k_2} \ldots L_r^{k_r} L_T \tag{26}$$

where L_i is an infinite order birational map corresponding to $P \mapsto P + \omega_i$, L_T is a finite order birational map and elements of $\{L_i, L_T\}$ pairwise commute. Conversely, we can, in principle use the isomorphism to construct birational maps over $\mathbb{Q}$ that preserve a given rational elliptic curve $E/\mathbb{Q}$ and correspond to translations. We do this by finding in (25) appropriate ω_is and torsion points on the corresponding Weierstrass and then use Φ^{-1}.

4. Two applications

One of the noteworthy points to make about theorem 3, and the ensuing propositions, is that they apply for fairly general fields. We now give two applications of the result via two particular choices of K.

4.1. The function fields case

Let $\mathbb{C}(t)$ be the field of rational functions over $\mathbb{C}$ in the indeterminate t, called the function field of the complex line[9].

By applying theorem 3 to the case $K = \mathbb{C}(t)$, we obtain a result that directly applies to many traditional discrete planar integrable systems. The crucial step lies in thinking of a one-parameter family of elliptic curves such as (7) as a single elliptic curve over the field $\mathbb{C}(t)$, which is possible as long as the dependence on the parameter is given by rational functions.

To make things precise, let $C(x, y, t) = 0$ be a family of curves with complex coefficients, parametrized by the complex parameter t. The equation $C(x, y, t) = 0$ defines a *foliation* of the xy plane if there exists a function $\tau : \mathbb{C}^2 \to \mathbb{C}, (x, y) \mapsto \tau(x, y)$ which is defined apart from, possibly, finitely many points, and such that $C(x, y, \tau(x, y)) = 0$. The finitely many exceptional points are the so-called *base-points*. A map $L : (x, y, t) \mapsto (x', y', t)$ that preserves the foliation curve-wise will satisfy the condition

$$C(x, y, \tau(x, y)) = 0 \quad \Longrightarrow \quad C(x', y', \tau(x', y')) = 0,$$

highlighting that $\tau(x, y)$ is an integral of motion under L.[10]

To allow an algebraic-geometric approach, we specialize to the case in which $C(x, y, t)$ is algebraic (in which case we talk of an *algebraic foliation*), and L is birational and can have explicit algebraic dependence on t. In the latter case—in the language of [5, 6]—L is a *curve-dependent* birational map, meaning that the one-parameter family of maps over each curve of the foliation has now become a single (global) map defined over the function field $\mathbb{C}(t)$.

Combining theorems 1 and 3 with $K = \mathbb{C}(t)$ and proposition 1, we obtain

[9] Thus $\mathbb{C}(t)$ is the set of ratios of polynomials in t, with complex coefficients.

[10] This description of a foliation and the map preserving it follows [5, 6], where conditions to ensure the existence of τ are also investigated.

Theorem 4. *Let L be an infinite order birational map defined over $\mathbb{C}(t)$ that preserves an algebraic foliation $C(x, y, t) = 0$ where $C = E/\mathbb{C}(t)$ is an elliptic curve. Then L is conjugate to a map $\widetilde{L} : P \mapsto P + \Omega(t)$ on the associated Weierstrass $W/\mathbb{C}(t)$, where $\Omega(t) = (\omega_1(t), \omega_2(t))$ and $\omega_i(t) \in \mathbb{C}(t)$. Furthermore, L is reversible, i.e., can be written as the composition of two rational involutions over $\mathbb{C}(t)$, and the dynamics of L on each curve can be parametrized in terms of Weierstrass elliptic functions.*

With reference to theorem 4, we remark:

(i) The theorem as stated presumes there exists a point on $C(x, y, t) = 0$ with x and y in $\mathbb{C}(t)$. However, if $C = E/K$ with K a subfield of $\mathbb{C}(t)$ (e.g. $\mathbb{R}(t)$ and $\mathbb{Q}(t)$) or K an extension of $\mathbb{C}(t)$, and if L is also defined over K, the theorem stands with $\mathbb{C}(t)$ replaced by K. Plainly, K is to be chosen as economically as possible, ideally in the field of coefficients of the curve; in any case, a point on the curve will be found in a finite algebraic extension of such a field.

(ii) The inference in the statement of the theorem that the algebraic foliation $C(x, y, t) = 0$ is actually an elliptic curve represents an application of Hurwitz theorem—our theorem 3.

(iii) Theorem 4 can be viewed as an analogue of the Arnold–Liouville theorem in the sense that it tells us that a birational map preserving an algebraic foliation is conjugate to translation by a point that depends on the curve. For rational measure-preserving maps of the plane satisfying (1), a discrete Liouville theorem due to Veselov [31, p 8] gives that the dynamics on a compact non-singular level set of I is conjugate to the rotation $\theta \mapsto \theta + \Omega(I)$. Interestingly, theorem 4 has no measure-preservation requirement.

(iv) The decomposition of integrable planar maps, such as the QRT maps ((3) and (10)), as the composition of two involutions has been much exploited to elucidate their properties (in fact, reversibility was presumed from the start in order to create the QRT maps [19, 20]).

A further consequence of theorem 4 is that it suggests how to determine all the possible finite orders of maps L satisfying the assumption of the theorem (this now refers to the global finite order of L instead of its action on one particular curve). From (22), the issue is to calculate the possible finite orders of the translative point $\Omega = (\omega_1(t), \omega_2(t)) \in W/\mathbb{C}(t)$. This has been resolved in [2] and [18] who have provided a structure theorem for the Mordell–Weil group of elliptic curves E defined over $\mathbb{C}(t)$ with $j(E)$ not belonging to $\mathbb{C}$ and having a long Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with coefficients a_i being polynomials in t of degree at most i. Elliptic curves defined over $\mathbb{C}(t)$ that satisfy the aforementioned condition on coefficients are called *rational elliptic surfaces*.

Proposition 4. *Let L be a birational map preserving a rational elliptic surface whose j-invariant is not in $\mathbb{C}$. Then, if L has finite order, its order does not exceed 6.*

Proof. The proof is a direct application of [18, corollary 2.1] to the translative point $\Omega = (\omega_1(t), \omega_2(t))$ as given in theorem 4. □

In [29], it is has been shown, constructively, that the QRT maps preserving (7) with coefficients depending affinely on t are equivalent to translations on a rational elliptic surface. The finite order possibilities described in proposition 4 are found and examples of each are given.

Example 1. Our first example illustrates theorem 4. Consider the one-parameter family of curves

$$B(x, y, t) = x^2y^2 - t^2(x^2 + y^2) - 2xy + 1 = 0 \tag{27}$$

which constitutes a single algebraic curve defined over $\mathbb{Q}(t)$ (a subfield of $\mathbb{C}(t)$), since it contains the smooth point $\left(0, \frac{1}{t}\right)$.[11] This means that the conversion-to-Weierstrass functions ϕ and ϕ^{-1} are defined over $\mathbb{Q}(t)$. The associated Weierstrass equation is[12]

$$W(u, v, t^2) = v^2 + u^3 + \left(-\tfrac{1}{3}(t^2)^4 - 4(t^2)^2\right) u + \tfrac{2}{27}(t^2)^6 - \tfrac{8}{3}(t^2)^4 = 0. \tag{28}$$

Theorem 4 applies for any infinite order birational maps that preserve B. One such map is

$$L : x' = y, \qquad y' = -x + \frac{2y}{y^2 - t^2}. \tag{29}$$

Note that L is defined over $\mathbb{Q}(t)$; it is the *curve-dependent McMillan map* preserving the algebraic foliation $B(x, y, t) = 0$ [5, 6]. Since the function $\tau(x, y)$ obtained from solving (27) for t^2 is rational in x and y, replacing t^2 in (29) by τ produces an alternative form of (29) which is still birational

$$L : x' = y, \qquad y' = \frac{2y^3 - x(y^4 - 1)}{y^4 - 1 + 2xy}. \tag{30}$$

This is a symmetric QRT map. (It is shown in [5, 6] that all symmetric and asymmetric QRT maps admit a curve-dependent McMillan description.)

Using theorem 4 we can find the additive point $\Omega(t) = (\omega_1(t), \omega_2(t))$ utilizing a transformation ϕ taking B to W (an explicit form for ϕ can be found using an algorithm given in [30] and implemented in the MAPLE computing package). We find that

$$\Omega(t) = \left(-\tfrac{1}{3}(5t^2 - 6)t^2, -2(t^2 - 2)t^4\right). \tag{31}$$

As expected, the coordinates of Ω are in $\mathbb{Q}(t)$.

In table 1, we list various birational maps that preserve the foliation $B = 0$ and their corresponding actions on W, including L and L^2. The other entries relate to finite order maps. In particular, we show the standard involutions H and G such that $L = H \circ G$. Another decomposition into orientation-reversing involutions is $L = N \circ R$.

If we take $z = t^2$, we observe that $W(u, v, z)$ of (28) is a rational elliptic surface with j-invariant equal to $16(z^2 + 12)/(z^2 - 4)^2$. Furthermore, all the points involved in the maps of table 1, including (31), are in $\mathbb{Q}(z)$. Since in our table we have one point of infinite order (corresponding to the map given by (29)–(30)) and also three points of order two (corresponding to the simple involutions I_1, I_2 and I_3, which form a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$) we are immediately left with only one possible structure for the group of $\mathbb{C}(z)$ points on W, namely

$$\mathbb{Z}^r \oplus (\mathbb{Z}/2\mathbb{Z})^2$$

with $1 \leqslant r \leqslant 2$ [18]. In particular, this structure restriction tells us that the three simple involutions I_1, I_2 and I_3 are the *only* finite order rational maps corresponding to points in $\mathbb{C}(z)$ that commute with the QRT map. Of course, there are other possibilities for finite order maps preserving the foliation $B = 0$ that do not commute with the QRT map. However these must all be involutions. By theorem 3, they all act on W of (28) as $P \mapsto \iota(P) + \omega$ and since W has j-invariant not equal to 0 or 1728, the only possibility for ι is ± 1. When $\iota = -1$, the resulting transformation is necessarily of order two, but does not commute with infinite order maps of translative type.

[11] Note that an alternative starting point is to note that (27) is an elliptic curve over $\mathbb{Q}(\sqrt{2}, i = \sqrt{-1}, t^2)$ since it contains the point $(\frac{(1-i)}{\sqrt{2}}, \frac{-(1+i)(t^2-i)}{\sqrt{2}(t^2+i)})$.

[12] Our Weierstrass here, and in example 2 below, is in the form outputted by MAPLE and is related to (11) by $u = -x$, $v = y$.

Table 1. Examples of birational maps preserving (27) and their corresponding description on (28).

Map on W	Map on B
$P \mapsto -P$	$N(x, y) = \left(-x, y - \frac{2x}{x^2-t^2}\right)$
$P \mapsto -P + \left(-\frac{t^2}{3}(5t^2-6), 2(t^2-2)t^4\right)$	$R(x, y) = (-y, -x)$
$P \mapsto -P + \left(-\frac{t^2}{3}(5t^2+6), -2(t^2+2)t^4\right)$	$G(x, y) = (y, x)$
$P \mapsto -P + \left(-\frac{2}{3}t^4, 0\right)$	$H(x, y) = \left(x, -y + \frac{2x}{x^2-t^2}\right)$
$P \mapsto P + \left(-\frac{2t^4}{3}, 0\right)$	$I_1(x, y) = (-x, -y)$
$P \mapsto P + \left(\frac{1}{3}t^4 + 2t^2, 0\right)$	$I_2(x, y) = \left(\frac{1}{x}, \frac{1}{y}\right)$
$P \mapsto P + \left(\frac{1}{3}t^4 - 2t^2, 0\right)$	$I_3(x, y) = \left(-\frac{1}{x}, -\frac{1}{y}\right)$
$P \mapsto P + \left(-\frac{t^2}{3}(5t^2-6), -2(t^2-2)t^4\right)$	$L(x, y) = \left(y, -x + \frac{2y}{y^2-t^2}\right)$
$P \mapsto P + \left(-\frac{2}{3}t^4 - 1, -1 + t^4\right)$	L^2

Example 2. Our second example uses propositions 2 and 3 and the concept of rank of an elliptic curve to find two independent birational maps preserving the same foliation.

The one-parameter family of curves

$$B(x, y, t) = (1-t)x^2y^2 - t(x^2+y^2) - 3txy + x - 3y = 0 \tag{32}$$

is an elliptic curve defined over $\mathbb{C}(t)$, in fact over its subfield $\mathbb{Q}(t)$, since it contains e.g. the point $(1/t, 0)$. It has associated Weierstrass equation

$$W(u, v, t) = v^2 + u^3 + \left(-\frac{25}{48}t^4 + \frac{29}{2}t(t-1)\right)u - \frac{125}{864}t^6 + \frac{601}{24}t^3(t-1) - \frac{9}{4}(t-1)^2 = 0. \tag{33}$$

Since (32) is a biquadratic of the form (7), it is preserved by an asymmetric QRT map L_1, namely (3) with

$$(f_1, f_2, f_3)(y) = (-10y^2, y(y^3+3y^2+3), -3y^3+y^2+1)$$
$$(g_1, g_2, g_3)(x) = (6x^2, x(x^3-x^2-1), -3(x^3+x^2+1).$$

We find that L_1 and the involutions H and G of (10) correspond, respectively, to the following elements of (16) acting on (33):

$$\widetilde{L}_1 : P \mapsto P + \Omega(t), \qquad \Omega(t) = \left(-\frac{17}{12}t^2, \frac{3}{2}(t^3 - t + 1)\right)$$
$$\widetilde{H} : P \mapsto -P + \tau_1(t), \qquad \tau_1(t) = \left(-\frac{91}{36}t^2, \frac{209}{54}t^3 + \frac{3}{2}(t-1)\right)$$
$$\widetilde{G} : P \mapsto -P + \tau_2(t), \qquad \tau_2(t) = \left(-\frac{233}{12}t^2, -\frac{171}{2}t^3 - \frac{3}{2}(t-1)\right).$$

The points $\Omega(t)$, $\tau_1(t)$ and $\tau_2(t)$ belong to $W(\mathbb{Q}(t))$ with $\Omega(t) = \tau_1(t) - \tau_2(t)$ as expected. Consider the new translation on W based upon the point $\tau_2(t)$:

$$\widetilde{L}_2 : P \mapsto P + \tau_2(t). \tag{34}$$

Evidently, $\widetilde{L}_2 = \widetilde{G} \circ \widetilde{N}$, where $\widetilde{N} : P \mapsto -P$. Via the isomorphism of figure 1, $\widetilde{L}_2$ generates another birational map $L_2 = G \circ N$ preserving the foliation (32) that commutes with the QRT

Table 2. Calculations showing the linear independence of $\Omega(t)$ and $\tau_2(t)$ for various $t \in \mathbb{Q}$ on the elliptic curve $W(u, v, t)$ of (33). The last column expresses $\tau_2(t)$ in terms of infinite order and linearly independent elements of $W(\mathbb{Q})$, one of which is always $\Omega(t)$.

t-value	QRT Point $\Omega(t)$	Point $\tau_2(t)$	Decomposition of $\tau_2(t)$
2	$\left(\frac{-17}{3}, \frac{21}{2}\right)$	$\left(\frac{-233}{3}, \frac{-1371}{2}\right)$	$-\left(\frac{-17}{3}, \frac{21}{2}\right) - \left(\frac{-35}{3}, \frac{81}{2}\right) - \left(\frac{-59}{12}, \frac{45}{8}\right)$
$-\frac{31}{10}$	$\left(\frac{-16\,337}{1200}, \frac{-77\,073}{2000}\right)$	$\left(\frac{-223\,913}{1200}, \frac{5\,106\,561}{2000}\right)$	$0\left(\frac{-16\,337}{1200}, \frac{-77\,073}{2000}\right) + \left(\frac{-223\,913}{1200}, \frac{5106\,561}{2000}\right)$
11	$\left(\frac{-2057}{12}, \frac{3963}{2}\right)$	$\left(\frac{-28\,193}{12}, \frac{-227\,631}{2}\right)$	$\left(\frac{-1337}{12}, \frac{1593}{2}\right) + 0\left(\frac{-2057}{12}, \frac{3963}{2}\right) - \left(\frac{-1073}{12}, \frac{629}{2}\right)$

map L_1. The explicit form of the involution N is found to be

$$\begin{aligned}
x' = &-(110x^2y^2 + 27y^3x^3 - 9y^4 + 27yx^3 - 27x^2y^3 - 252xy^2 - 27y^3 \\
&+ 19y^4x^3 - 27x^2y - 152x - 627y - 114y^3x - 9x^2y^4) \\
&\times (-110xy^2 + 21x^2y^3 + 114x^2y - 9x^2y^2 - 81y^2 + 9x^3y^2 \\
&+ 33y^3x^3 + 8x^2y^4 - 60xy - 361 - 27y^3 - 9x^2 + 9x^3)^{-1} \\
y' = &(-y^3x^3 + 3x^4y^2 + 152y - 28x^2y - 3xy^2 - 3x^3 + 3x^4 \\
&- 171x + 19x^4y^3 - y^3x - 114x^2y^2 + 46yx^3 - 3x^3y^2) \\
&\times (8x^4y^2 - 9y^3x^3 - 17x^3y^2 - x^3 + 3x^2y^3 + 9x^2y^2 \\
&- 114x^2y + x^2 + 46xy^2 + 108xy + 3y^3 + 9y^2 + 361)^{-1}
\end{aligned}$$

With relation to proposition 3, L_2 and L_1 are not birationally conjugate since $\Omega(t) \neq \pm\tau_2(t)$ (here $j(W) \neq 0, 1728$, so that $\mathrm{Aut}(W) = \{P \mapsto \pm P\}$. We also claim that L_2 is not power-related to the QRT map L_1 as described in proposition 2. If this were true, it would mean there exist integers m, n satisfying

$$m\Omega(t) - n\tau_2(t) = [0, 1, 0], \tag{35}$$

an identity in t. Using the elliptic curve computational package Apecs (Arithmetic of Plane Elliptic Curves)[13], we can specialize $W(u, v, t)$, $\Omega(t)$ and $\tau_2(t)$ to various $t \in \mathbb{Q}$. Table 2 indicates some of the results showing that (35) cannot be satisfied, so $\tau_2(t)$ is linearly independent of $\Omega(t)$.[14] In line with the Mordell–Weil theorem over $\mathbb{C}(t)$ [18] and (25), this indicates that the rank of $W(\mathbb{C}(t))$ is at least 2. Furthermore, the torsion group in $W(\mathbb{C}(t))$ is also found to be trivial here, so the structure of $W(\mathbb{C}(t))$ appears to be $\mathbb{Z}^r$ with $2 \leqslant r \leqslant 8$.

4.2. The finite fields case

For the second application of theorem 3 we turn now to finite fields $K = \mathbb{F}_q$ where q, the cardinality of the field, is a prime power (see [13] for background). Considering maps over such fields underpins the arithmetic test for integrability recently developed in [21, 23]. In this context the map over the finite field is obtained by reducing to $\mathbb{F}_q$ a planar map L defined over, say, $\mathbb{Q}^2$. Details of the reduction process can be found in [24].

If L preserves a planar algebraic foliation, one has to allow for the existence of singular curves—the separatrices. We remark that the process of reduction to $\mathbb{F}_q$ may introduce spurious singular curves into the foliation, which do not have a counterpart in the original system. (The number of such singular curves admits a q-independent bound.) Note that the process of

[13] http://www.math.mcgill.ca/connell/.

[14] We remark that the corresponding $L_2 = G \circ N$ that could be created in example 1 from G and N of table 1 *is* power-related to the QRT map L of (29), satisfying $L_2^2 = L^{-2}$. This follows since the point of $\mathbb{C}(t^2)$ corresponding to H in table 1 has order two.

reduction may alter completely the dynamics: for instance, the foliation $C(x, y, t) = 0$ may degenerate, as a result of the integral becoming a constant. To avoid such pathologies, we speak of *good reduction* meaning the degree of each component of the map, and of the integral, do not change under reduction.

The existence of invariant curves over a finite field requires the analysis of the number of points they contain. The number of points on a curve C over a finite field $\mathbb{F}_q$ is rigidly restricted by the Hasse–Weil bound

$$q + 1 - 2g\sqrt{q} \leqslant \#C \leqslant q + 1 + 2g\sqrt{q}, \tag{36}$$

where g is the genus of the curve.

We consider a birational map that preserves $E/\mathbb{F}_q(t)$, with associated Weierstrass $W/\mathbb{F}_q(t)$. From theorems 3 and 4 (and remark (i) following), the dynamics on $W(t)$ is translation by $\Omega(t)$. It follows that we have equidistribution: for each t, all orbits on $W(t)$ are periodic, and their common period is ord $\Omega(t)$, which must be a divisor of $\#W(t)$ (see equation (22)). Denoting the period on a particular level set by $\#O_W(t)$ and by $n = n(t)$ the number of orbits on that level set, we rewrite (36) for elliptic curves as

$$q + 1 - 2\sqrt{q} \leqslant n\#O_W(t) \leqslant q + 1 + 2\sqrt{q}.$$

Now dividing throughout by $n(q + 1 + 2\sqrt{q})$, we obtain

$$\frac{1}{n}\left(1 - \frac{4\sqrt{q}}{q + 1 + 2\sqrt{q}}\right) \leqslant \frac{\#O_W(t)}{q + 1 + 2\sqrt{q}} \leqslant \frac{1}{n} \qquad n = 1, 2, \ldots. \tag{37}$$

The above inequalities tell us that if a translation on $W(t)$ preserves an elliptic curve, then the normalized length of an orbit (divided by $HW_1(q) = q + 1 + 2\sqrt{q}$) on such curve must lie in one of the allowed intervals ('windows') prescribed by (37). If we fix q, then for n large enough the windows will overlap. Indeed, the overlap condition

$$\frac{1}{n+1} \geqslant \frac{1}{n} - \frac{4\sqrt{q}}{nHW_1(q)}$$

gives

$$n \geqslant \frac{\sqrt{q}}{4} + \frac{1}{4\sqrt{q}} - \frac{1}{2}.$$

Because $n\#O_W(t) \sim q$, we see that if the period of the orbit is sufficiently small (of order $\sqrt{q}$), there are no restrictions on the value of the period.

As $q \to \infty$, the windows (37) shrink to the points $1/n$, that is, the normalized periods are quantized. Note that, from the Hasse–Weil bound (36), it follows that the windows for t values corresponding to invariant conics (genus $g = 0$) are also just $[1/n, 1/n]$, with normalizing factor $HW_0(q) = q + 1$.

We return now to the issue of reduction. Let L be a birational planar map which preserves an elliptic curve $E/\mathbb{Q}$, and let O be an infinite rational orbit of L on E. If, upon reduction, the orbit is periodic, we can exploit the isomorphism between the reduced elliptic curve and its associated Weierstrass to obtain

Corollary 1. *Let L be a planar birational map of infinite order, and let O be a periodic orbit of the reduction of L over $\mathbb{F}_q^2$. Furthermore, assume that O does not satisfy (37) for any n (with $\#O_W(t) \to \#O$). Then one of the following is true:*

(i) L does not preserve a curve containing O;
(ii) L preserves a conic containing O;
(iii) L preserves a singular elliptic E curve containing O, and O contains a singular point of E.

Proof. Because L is birational of infinite order, from theorem 1 we have that any curve left invariant by L must have genus 0 or 1. This result is now an easy consequence of the Hasse–Weil bound. □

Corollary 1 furnishes a necessary condition for L to preserve an algebraic foliation, which can be regarded as a refinement of the Hasse–Weil bound test of [23, 21].

The quantization of periods deriving from the bounds (37) for large q has an interesting probabilistic interpretation. Let L be as above, and let $q = p^k$, p a prime. In what follows, the orbit O and the integer k are regarded as being fixed. For every value of q of good reduction as defined above, and for which the reduced orbit is periodic, we define the 'random variable' $\theta(q) := \#O/q$.

Does $\theta(q)$ have an asymptotic density over the set of q of good reduction? From the above discussion we conclude that this density—if it exists—must be supported on the set of reciprocals of the natural integers.

Now, from theorem 3 it follows that the case $n = 1$ in (37) will occur precisely when the group of the curve is cyclic, and the reduction Ω_q of Ω is a generator. The existence of a density for the set of primes such that Ω reduces to a generator is a classical problem in arithmetic geometry, concerning the so-called elliptic analogue of Artin's conjecture. Some partial results are known (with some conditions on the curve) due to the work of Heath-Brown, Gupta, Ram-Murty, Serre, and others, but a general proof remains elusive (see [17] and references therein).

It is natural to extend such a conjecture to account for all values of n in (37) (letting $q \to \infty$ first, that is). Numerical experiments suggest that such density exists for every n [21, 23]. So we put forward the following.

Conjecture. *Let $q = p^k$. As $p \to \infty$, the random variable θ admits a limiting density, supported on the reciprocals of the natural integers.*

The dependence of this density on the particular choice of the orbit O and on the degree k is an important issue for future investigations. Determining the orbit dependence is likely to be delicate, as it may require knowledge of the Mordell–Weil group of the curve. By contrast, studying the k-dependence seems easier: the growth of the number points on a curve over the field $\mathbb{F}_{p^k}$ is very regular, and determined by a zeta-function, whose form can be inferred from the data corresponding to $k = 1$ [28, section V.1].

There is a complementary approach to the same asymptotic problem. Let L be a birational planar map defined over $\mathbb{Q}$, which preserves a foliation of elliptic curves. If $q = p^k$ and p is a prime of good reduction for L, let Π_q be the set of periodic points of the reduction of L over $\mathbb{F}_q$, equipped with the uniform probability measure. We define the random variables $\theta_q(z) = \#O(z)/q$ where $O(z)$ is the periodic orbit through $z \in \Pi_q$. Thus the quantity $\theta_q(z)$ records the normalized period through z, sampled over a foliation of distinct elliptic curves.

For computational purposes, it is convenient to introduce the cumulative distribution function

$$\mathcal{I}_q(x) := \frac{1}{\#\Pi_q} \#\{z \in \Pi_q : \theta_q(z) \leqslant x\}. \tag{38}$$

Thus $\mathcal{I}_q(x)$ represents the probability that a periodic point chosen at random belongs to an orbit of period not exceeding qx. Because the corresponding density is supported on the 'windows' (37), the distribution function will be a step-function, with steps within such

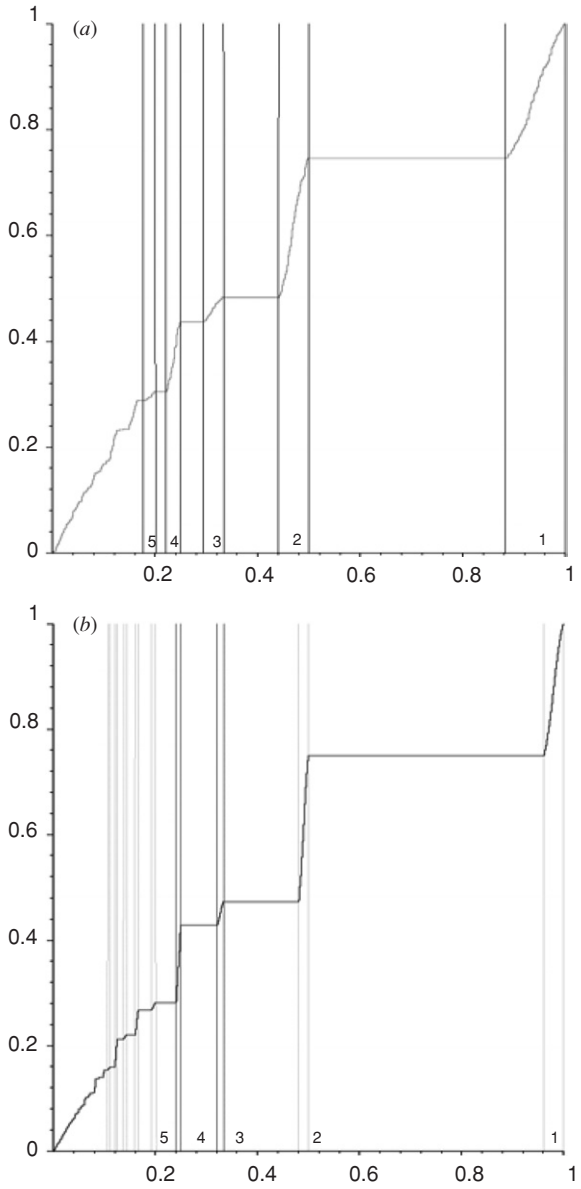

Figure 2. Integrable maps over finite fields $\mathbb{F}_q$. Shown are distribution functions associated with the reduction to a finite field of the integrable map (39) and allowed windows prescribed by (37). (*a*): direct computation of $\mathcal{I}_q$ for the case $q = p = 1019$, together with distribution of ord $\Omega(t)$ over the t level sets (the two distributions are indistinguishable from one another); (*b*): distribution of ord $\Omega(t)$ for $q = p = 10\,007$.

windows. In figure 2 we show $\mathcal{I}_q$ for the integrable QRT map

$$x' = -x - \frac{y+1}{y^2+1}, \qquad y' = -y - \frac{x'-1}{(x')^2+1} \tag{39}$$

for the field $\mathbb{F}_q$ with $q = p = 1019$. From the discussion above (37), this corresponds to the distribution of ord $\Omega(t)$ over the t level sets. The latter distribution for $p = 10\,007$ is also

Table 3. Decomposition of $\mathbb{F}_{11}^2$ by the integrable map L of (29) on the curves (27) when they are elliptic.

t^2	$\Omega(t)$	ord $\Omega(t)$	W-orbits	$\#B(t)$	B-orbits
1	[4,2,1]	4	4,4	6	s2 s,s2 s
3	[2,4,1]	8	8,8	14	8,s2 s,s2 s
4	[7,2,1]	8	8,8	14	s6 s,s6 s
5	[5,4,1]	6	6,6	10	s4 s,s4 s
6	[7,9,1]	6	6,6	12	6,6
7	[2,5,1]	8	8,8	16	8,8
8	[1,2,1]	8	8,8	16	8,8
10	[0,6,1]	4	4,4	8	4,4

shown in figure 2. If not all orbits are periodic, the experimental distribution (38) does not necessarily coincide with the corresponding distribution of ord $\Omega(t)$ on Weierstrass curves, although the two distributions will have the same support. Nonetheless, it is conceivable that the random variable $\theta_q(z)$ could also admit a limiting distribution as $q \to \infty$ (with k fixed), although we have not investigated this issue in depth.

To illustrate the kind of phenomena that occur when all points—not just the periodic ones—are taken into account; consider the map L of (29) which preserves the family of curves (27) with corresponding Weierstrass equation (28), but now over $\mathbb{F}_{11}$—see table 3 ($t^2 = 0, 2$ and 9 in (28) (mod 11) give conics and are omitted). The column $\Omega(t)$ is the translating point we expect according to equation (31) and its order is also given. The periods of the orbits on $W(t)$ are also given under the induced translation (so '8,8' means that there are two orbits of length 8) and similar descriptions apply for $\#B(t)$ and B-orbits. In B-space, the map L has singularities. These are represented in the table by the symbol 's', shorthand for the chain $[0, 1, 0] \to [1, 0, 0] \to [0, 0, 0] \to [0, 0, 0] \to \cdots$ under forward iteration and $[1, 0, 0] \to [0, 1, 0] \to [0, 0, 0]$ under backward iteration. Thus orbits listed with the form sNs are not closed. They begin with the latter chain, end with the former chain and have standard affine points in the middle.

Acknowledgments

DJ acknowledges the support of an Australian Postgraduate Research Award and a UNSW School of Mathematics Research Award. JR 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. 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.

References

[1] Anglès d'Auriac J-Ch, Maillard J-M and Viallet C M 2002 A classification of four-state spin edge Potts models *J. Phys. A: Math. Gen.* **35** 9251–72

[2] Cox D A 1982 Mordell-Weil groups of elliptic curves over $\mathbf{C}(t)$ with $p_g = 0$ or 1 *Duke Math. J.* **49** 677–89

[3] Esch J and Rogers T D 2001 The screensaver map: dynamics on elliptic curves arising from polygonal folding *Discrete Comput. Geom.* **25** 477–502

[4] Grammaticos B, Nijhoff F W and Ramani A 1999 Discrete Painlevé equations *The Painlevé Property (CRM Ser. Math. Phys.)* (New York: Springer) pp 413–516

[5] Iatrou A and Roberts J A G 2001 Integrable mappings of the plane preserving biquadratic invariant curves *J. Phys. A: Math. Gen.* **34** 6617–36
[6] Iatrou A and Roberts J A G 2002 Integrable mappings of the plane preserving biquadratic invariant curves: II. *Nonlinearity* **15** 459–89
[7] Jogia D and Roberts J A G 2006 Creation and comparison of integrable maps *Preprint* UNSW
[8] Kajiwara K, Masuda T, Noumi M, Ohta Y and Yamada Y 2003 ${}_{10}E_9$ solution to the elliptic Painlevé equation *J. Phys. A: Math. Gen.* **36** L263–72
[9] Kimura K, Yahagi H, Hirota R, Ramani A, Grammaticos B and Ohta Y 2002 A new class of integrable discrete systems *J. Phys. A: Math. Gen.* **35** 9205–12
[10] Kocić V L and Ladas G 1993 *Global Behavior of Nonlinear Difference Equations of Higher Order with Applications (Mathematics and its Applications* vol 256*)* (Dordrecht: Kluwer)
[11] Kulenović M R S and Ladas G 2002 *Dynamics of Second Order Rational Difference Equations* (Boca Raton, FL: Chapman & Hall/CRC) With open problems and conjectures
[12] Lamb J S W and Roberts J A G 1998 Time-reversal symmetry in dynamical systems: a survey *Phys.* D **112** 1–39; Time-reversal symmetry in dynamical systems (Coventry, 1996)
[13] Lidl R and Niederreiter H 1997 Finite fields *Encyclopedia of Mathematics and its Applications* 2nd edn, vol 20 (Cambridge: Cambridge University Press) with a foreword by P M Cohn
[14] Lyness R C 1945 Note 1847 *Math. Gaz.* **29** 231–3
[15] Murray Macbeath A 1999 Hurwitz groups and surfaces *The Eightfold Way of (Math. Sci. Res. Inst. Publ.* vol 35*)* (Cambridge: Cambridge University Press) pp 103–13
[16] McMillan E M 1971 A problem in the stability of periodic systems *Topics in Modern Physics. A tribute to E U Condon* ed E Britton and H Odabasi (Boulder, CO: Colorado University Press) pp 219–44
[17] Ram Murty M 1997 Artin's conjecture and elliptic analogues *Sieve methods, Exponential Sums, and Their Applications in Number Theory (Cardiff, 1995) (London Math. Soc. Lecture Note Ser.* vol 237*)* (Cambridge: Cambridge University Press) pp 325–44
[18] Oguiso K and Shioda T 1991 The Mordell–Weil lattice of a rational elliptic surface *Comment. Math. Univ. St. Paul.* **40** 83–99
[19] Quispel G R W, Roberts J A G and Thompson C J 1988 Integrable mappings and soliton equations *Phys. Lett.* A **126** 419–21
[20] Quispel G R W, Roberts J A G and Thompson C J 1989 Integrable mappings and soliton equations: II. *Phys.* D **34** 183–92
[21] Roberts J A G, Jogia D and Vivaldi F 2003 The Hasse–Weil bound and integrability detection in rational maps *J. Nonlinear Math. Phys.* **10** 166–80
[22] Roberts J A G and Quispel G R W 1992 Chaos and time-reversal symmetry. Order and chaos in reversible dynamical systems *Phys. Rep.* **216** 63–177
[23] Roberts J A G and Vivaldi F 2003 Arithmetical method to detect integrability in maps *Phys. Rev. Lett.* **90** 034102
[24] Roberts J A G and Vivaldi F 2005 Signature of time-reversal symmetry in polynomial automorphisms over over finite fields *Nonlinearity* **18** 2171–92
[25] Sakai Hidetaka 2001 Rational surfaces associated with affine root systems and geometry of the Painlevé equations *Commun. Math. Phys.* **220** 165–229
[26] Silverman J and Tate J 1992 *Rational Points on Elliptic Curves* (New York: Springer)
[27] Silverman J 1986 *The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics)* (New York: Springer)
[28] Stichtenoth H 1991 *Algebraic Function Fields and Codes* (Berlin: Springer)
[29] Tsuda T 2004 Integrable mappings via rational elliptic surfaces *J. Phys. A: Math. Gen.* **37** 2721–30
[30] van Hoeij M 1995 An algorithm for computing the Weierstrass normal form *ISSAC 95 Proc.* pp 90–5
[31] Veselov A P 1991 Integrable maps *Russ. Math. Surveys* **46** 1–51
[32] Viallet C M, Grammaticos B and Ramani A 2004 On the integrability of correspondences associated to integral curves *Phys. Lett.* A **322** 186–93