Arithmetical Method to Detect Integrability in Maps

J. A. G. Roberts[1] and F. Vivaldi[2]

[1]School of Mathematics, The University of New South Wales, Sydney NSW 2052, Australia

[2]School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, United Kingdom

(Received 31 July 2002; published 24 January 2003; publisher error corrected 11 February 2003)

We develop a method to detect the presence of integrals of the motion in symplectic rational maps, by representing these maps over finite fields and examining their orbit structure. We find markedly different orbit statistics depending upon whether the map is integrable or not.

DOI: 10.1103/PhysRevLett.90.034102 PACS numbers: 05.45.–a

Integrable dynamical systems have a distinguished history and model many natural phenomena. These systems have no chaos, their future can be predicted, and some of their features persist under perturbation, as prescribed by the Kol'mogorov-Arnol'd-Moser theory [1]. Famous examples with continuous time include the two-body problem, various spinning tops, the Toda Hamiltonian, and various soliton equations appearing in numerous physical contexts [1]. Recently, there has been intense study into integrable dynamical systems with discrete time, including integrable maps and partial difference equations (see [2] and the excellent overviews [3]). As [2,3] show, discrete integrable systems prominently feature in increasingly numerous areas: exactly solvable models in statistical mechanics, discrete analogs of integrable systems in classical mechanics or solid state physics, reductions or discretizations of integrable soliton (partial) differential equations, and discrete geometries.

A dynamical system is integrable if it possesses a sufficient number of *integrals* of the motion, in involution with respect to a symplectic structure. How do we know *a priori* whether a discrete system might be integrable, and how do we distinguish integrable from near integrable? An important early integrability detector was the singularity confinement method [4], an analog of the Painlevé criterion for differential equations. While effective at isolating the candidate integrable parameter values in a multiparameter space, singularity confinement is not sufficient for integrability [5] and is also not invariant under birational transformation. A more sensitive and birationally invariant test involves calculating the algebraic entropy of a rational map, the conjecture being that entropy vanishes if and only if the map is integrable [5,6]. A drawback is that carrying free parameters in the algebraic entropy test is computationally delicate. Other recent approaches to integrability detection include studying difference equations in the complex plane utilizing the Nevanlinna theory [7] and characterizing integrability of birational maps using classical algebraic geometry [8].

An n-dimensional rational map is usually made to act on $\mathbf{C}^n$ or $\mathbf{R}^n$, but the complex or real field can be replaced by any field in which the coefficients and parameters of the map can be represented. In this Letter we consider autonomous rational maps acting over *finite fields*, the simplest instance of which are the integers modulo a prime number p, denoted by $\mathbf{F}_p$. Any rational map whose coefficients are algebraic numbers (roots of polynomials with integer coefficients) can be represented over infinitely many finite fields. Over these fields, the dynamics can be described by finite exact computation, and our diagnostic test described below—based on counting orbits—is simple and dimension independent. We will show that substantial inference on the presence or absence of an integral of the motion in a parametrized family of maps can often be made by analyzing the family over a single finite field, which can be quite small. To identify the values of the parameters at which an integral occurs, we describe a sieve algorithm, involving several fields. Finally, the broader picture is revealed by analyzing the asymptotic (large fields) period distribution functions, which show structural differences between the integrable and nonintegrable cases. For simplicity, we restrict our attention to *rational* parameter values, which feature prominently in the literature. Dynamical systems over finite fields are an established area of research, interesting in their own right [9]. However, integrability in this context has attracted relatively little attention other than in connection with cellular automata [10]. We hope that our methodology can lead to fast and decisive recognition of discrete integrability in the many physical contexts outlined above where it is relevant.

For illustration, consider the following one-parameter family of two-dimensional maps:

$$x' = y, \qquad y' = -x - \frac{1 + 2y + \epsilon y^3}{1 + y^2}, \tag{1}$$

which for $\epsilon = 0$ has the following integral of motion:

$$\begin{aligned} &I(x', y') = I(x, y), \\ &I(x, y) = x^2y^2 + x^2 + y^2 + 2xy + x + y. \end{aligned} \tag{2}$$

This family belongs to a class of area-preserving integrable maps discovered by McMillan [11].

The family (1) can be made to act on the finite space $\mathbf{F}_p^2$ for all rational values of the parameter ϵ, whose

 0031-9007/03/90(3)/034102(4)$20.00

denominator is coprime to p. The polynomial $1 + y^2$ has no roots modulo p when $p \equiv 3 \pmod 4$ ([12], theorem 82); thus our map is invertible over these fields, and the p^2 phase points decompose into cycles.

Significantly, since the Eqs. (2) are algebraic, they still hold over $\mathbf{F}_p$. Integrability no longer translates into the trademark picture of a foliation of phase space by curves. Nevertheless, each level set of the integral is still an invariant algebraic curve C, now over a finite field $\mathbf{F}_p$. The number $\#C(\mathbf{F}_p)$ of points on such a curve (including points "at infinity," see below), is sharply constrained by the celebrated *Hasse-Weil bound*

$$p + 1 - 2g\sqrt{p} \leq \#C(\mathbf{F}_p) \leq p + 1 + 2g\sqrt{p}, \tag{3}$$

which applies to any *irreducible* curve of *genus* g. The sharpness of this bound (which is invariant under birational transformations and admits higher-dimensional generalizations) stems from its equivalence to the Riemann hypothesis for function fields [13] (see the last of these references for recent applications). Since the genus is bounded by the square of the degree of the integral, the bound (3) yields an *equidistribution* result: the p^2 phase points foliate into $O(p)$ level sets with $O(p)$ points each. This estimate holds also for reducible curves, where an orbit can spread among several irreducible components.

To see how the upper bound in (3) affects the orbit structure, we compute the lengths of all cycles of (1) over $\mathbf{F}_p$. As the parameter space is *finite*, we display the maximal period among all cycles, for each parameter $\epsilon \in \{0, 1, \ldots, p-1\}$ (Fig. 1). The case $\epsilon = 0$ is distinguished by a markedly lower maximal period, which lies below the Hasse-Weil bound for $g = 1$ (the horizontal line). This choice of g is justified by the fact that for a rational map on $\mathbf{C}^2$ or $\mathbf{R}^2$, which is of infinite order and possesses a rational integral, the genus of each level set of this integral is at most 1 (see the second reference in [3]). Generically, the genus will be 1, dropping to zero on curves possessing extra singularities.

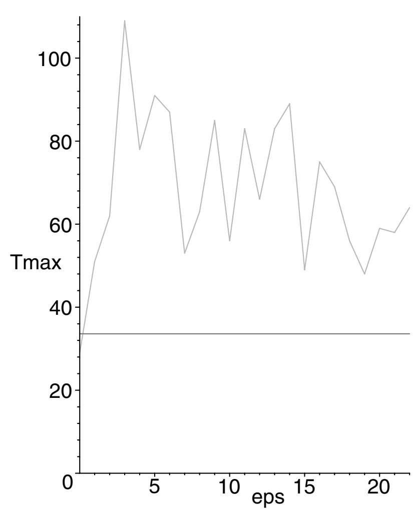

FIG. 1. Maximal cycle length as a function of ϵ, for the map (1) over $\mathbf{F}_p$ with $p = 23$. The minimum occurs for $\epsilon = 0$. The horizontal line represents the Hasse-Weil bound (3) for $g = 1$.

The Hasse-Weil estimate, while providing a rigorous and birationally invariant *necessary* condition for maximal cycle length in an integrable map, may cause incorrect inference if the integral is reducible, or if the maximal cycle length is low due to fluctuations. The *mean* period $\langle T \rangle$ [with $T = T(x)$, $x \in \mathbf{F}_p^2$, averaged with respect to the uniform measure], and the number of cycles N_c are more stable observables, which also clearly detect the integrable parameter value $\epsilon = 0$ in (1).

Note that the concept of near integrability does not exist here, e.g., $\epsilon = 10^{-1000} \equiv 13 \pmod{23}$. Indeed each computation refers to an *infinite equivalence class of maps*, since every element of $\mathbf{F}_p$ is the image of a set of algebraic numbers which is *dense* on the complex plane. In particular, the integrable parameter value $\epsilon \equiv 0 \pmod{23}$ represents all rationals with the numerator divisible by the prime $p = 23$. One notes that among those rationals, zero is the one of *minimal complexity*. We shall return to this point below.

The analysis of the family (1) was simplified by a straightforward characterization of its singularities: the denominator $1 + y^2$ has two roots modulo p for $p = 2$ and $p \equiv 1 \pmod 4$. To illustrate a more typical situation, we consider the map

$$x' = y, \qquad y' = \frac{f_1(y) - xf_2(y)}{f_2(y) - xf_3(y)}, \tag{4}$$

where

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix}(y) = A_0 Y \times A_1 Y, \qquad Y = \begin{pmatrix} y^2 \\ y \\ 1 \end{pmatrix}.$$

Here A_0 and A_1 are 3×3 matrices. When one of them is symmetric, the map is measure preserving; when both are symmetric, it becomes the integrable symmetric Quispel-Roberts-Thompson map [14], with integral $I = (X \cdot A_0 Y)/(X \cdot A_1 Y)$. The denominator of y' in (4) is in general a quintic polynomial in two variables, with a complicated root structure.

We deal with singularities by studying the dynamics on the two-dimensional projective space $\mathbf{P}(\mathbf{F}_p)^2$ with homogeneous coordinates (X, Y, Z); it comprises 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). (The projective map is obtained by substituting the expressions $x = X/Z$, $y = Y/Z$ in the original map, and then clearing denominators; see [5] for an example.) We then construct the *orbit graph* of the map on the $p^2 + p + 1$ points, by connecting two projective points (vertices) with an oriented arc whenever one vertex is the image of the other under the map. This graph decomposes into connected subgraphs, which are either cyclic (the periodic orbits), or noncyclic, containing vertices of degree greater than 1 (the noninvertible points), and edges without outgoing arcs (the points where the map is undefined).

TABLE I. Candidate ϵ values for integrability of (4) for various primes p.

p	$\epsilon \in$ HW	$\min_\epsilon \langle T \rangle$	$\max_\epsilon N_c$
31	6,**20**,29	6	**20**
37	3,5,6,**24**	21	**24**
41	7,**13**,16,20	16	**13**
43	**28**	39	**28**
47	**15**,16	16	**15**
53	**17**,20	**17**	**17**
59	**19**,32	**19**	**19**
61	**40**	**40**	**40**

The vertices of degree greater than 1 are effectively *base points* of an integral (if present), that is, members of every level set. In the presence of noncyclic components, we have adopted two strategies: (i) perform the statistical analysis on cycles only; (ii) apply the Hasse-Weil test to cycles as well as to the orbit segments obtained by removing the vertices of degree greater than 1 from each noncyclic component.

To illustrate these procedures, we specialize (4) as follows:

$$A_0 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 7 \end{pmatrix}, \qquad A_1 = \begin{pmatrix} 9 & \epsilon & 3 \\ -2/3 & 6 & 5 \\ 3 & 5 & 1 \end{pmatrix}.$$

Integrability now occurs for the single value $\epsilon = -2/3$ (so the field $\mathbf{F}_3$ must be excluded). In Table I, we display for various primes, the result of selecting ϵ according to various criteria, with the correct value $\epsilon \equiv -2/3 \pmod p$ in boldface. HW represents the Hasse-Weil selection on the fragmented graph [as per strategy (ii)], while the average period $\langle T \rangle$ and the number of cycles N_c are both computed considering cycles only [as per strategy (i)]. Maximizing N_c seems consistently reliable even for small primes, while the other criteria over/under select for small primes, to become reliable for larger ones.

To recover the rational value $\epsilon = -2/3$ from the candidate integrable parameter value(s) ϵ_i modulo various primes p_i, we use a sieve method based on continued fractions [15]. The idea is to order the infinitely many rationals r/s congruent to ϵ_i modulo p_i in order of ascending *height* h, where $h(r/s) = |rs|$. As the number of primes p_i considered increases, all rationals—except ϵ—will have diverging height, and will fluctuate erratically. This makes the identification of ϵ possible.

For illustration, we apply the sieve to the ϵ values of the last six primes of the HW column of the table. The two rationals of smallest height are displayed below, together with the associated sequence of residues ϵ_i

$$-\frac{2}{3} \quad [13, 28, 15, 17, 19, 40],$$

$$\frac{223}{77044} \quad [20, 28, 16, 20, 19, 40].$$

The inference $\epsilon = -2/3$ is compelling.

Integrability may occur at several parameter values, for instance in the mapping

$$x' = y + 1 - \epsilon, \qquad y' = x\frac{y - \epsilon}{y + 1}. \tag{5}$$

This map possesses a rational integral for $\epsilon = 0, 1, 1/2, 1/3$ [16]. The cycle statistics become unequivocal for $p > 50$. Reduction modulo $p = 89$ (Fig. 2), singles out four parameter values: $\epsilon = 0, 1, 30, 45$, congruent to $0, 1, 1/3, 1/2$, respectively. By inspection, we have localized the four peaks in the number N_c of cycles, for the five largest primes $p < 100$, obtaining a total of $4^5 = 1024$ combinations of parameters, giving as many congruences modulo $M = 4132280413$. The corresponding continued fractions give several thousand rational

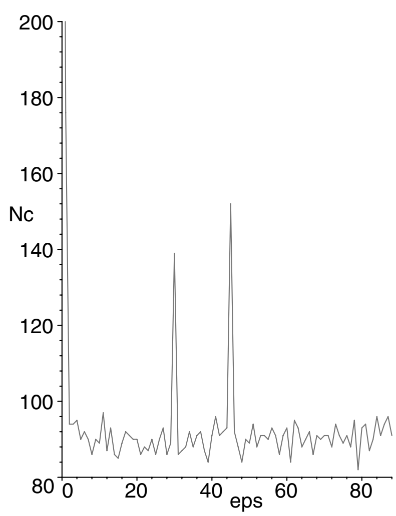

FIG. 2. Number N_c of cycles of the map (5) over $\mathbf{F}_p$ with $p = 89$, as a function of ϵ. The peaks occur at $\epsilon = 0, 1, 30, 45$ which are congruent (mod 89) to $\epsilon = 0, 1, 1/3, 1/2$.

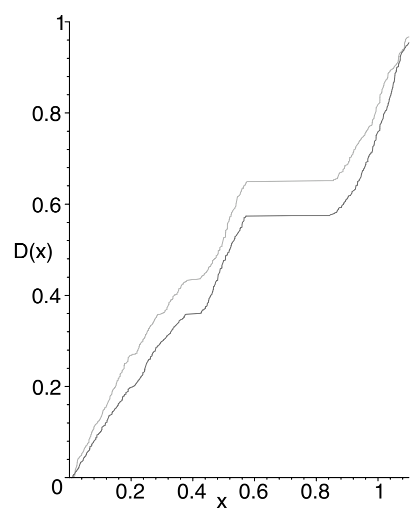

FIG. 3. Period distribution function $D(x)$ for the maps (1) (top curve) and (4), at their respective integrable values [i.e., 0 and $-2/3 \pmod p$]. The data are obtained by averaging over primes p in the range $150 < p < 180$.

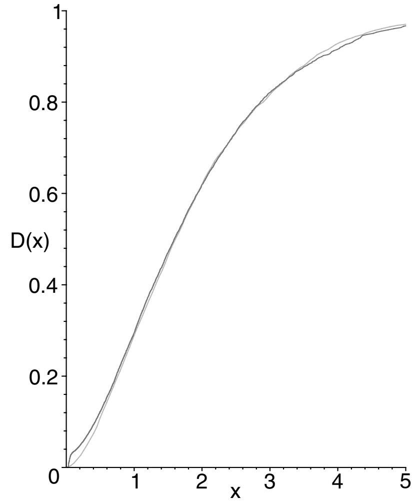

FIG. 4. Period distribution function $D(x)$ for the maps (1) and (4) at $p = 103$ and 131, respectively, averaged over all nonintegrable ϵ values. Averaging over p for fixed nonintegrable ϵ gives the same curve.

numbers as candidates for the four sought ϵ values. Of these, the five of smallest height are

$$\epsilon = 0, 1, \frac{1}{2}, \frac{1}{3}, -\frac{149426}{5}.$$

The convergence of the first four is confirmed by repeating the computation on subsets of these primes.

Finally, we briefly describe the underlying asymptotic regime [15]. Let C_p be the set of periodic points in phase space, for a given map. We define

$$D_p(x) = \#\{y \in C_p \mid T(y) \leq rx\}/\#C_p,$$

where T is the period, while $r = p$ and $r = \sqrt{\#C_p}$ for integrable and nonintegrable maps, respectively. Extensive numerical evidence suggests that $\lim_{p\to\infty} D_p(x) = D(x)$ exists. In the integrable cases, the distribution function features a rich structure, with gaps of forbidden periods, suggestive of a devil's staircase, and some rigidity, i.e., in the location of gaps for different maps (Fig. 3). By contrast, in the nonintegrable case, there appears to be a unique, possibly smooth, distribution (Fig. 4), which differs from that of a random permutation [for the latter, one would have $D_p(x) = x/p$, using Parker's lemma [17]]. Moreover, the expected length of the longest cycle is $O(p^2)$ for random permutations [18], while in our case it seems to grow at a slower rate.

Extensions of the above ideas to rational maps that are multiparameter, nonautonomous, and/or higher dimensional are currently being investigated.

The authors thank P. J. Cameron, A. Veselov, and C.-M. Viallet for useful discussions.

[1] V. I. Arnold, *Mathematical Methods of Classical Mechanics* (Springer-Verlag, New York, 1978).

[2] *Symmetries and Integrability of Difference Equations*, edited by P. A. Clarkson and F. W. Nijhoff, London Mathematical Society Lecture Note Series Vol. 255 (Cambridge University Press, Cambridge, 1999).

[3] M. Bruschi, O. Ragnisco, P. M. Santini, and T. Gui-Zhang, Physica (Amsterdam) **49D**, 273–294 (1991); A. P. Veselov, Russian Math. Surveys **46**, 1–51 (1991); B. Grammaticos, F. W. Nijhoff, and A. Ramani, in *The Painleve Property: One Century Later*, edited by R. Conte (Springer, New York, 1999), pp. 413–516.

[4] B. Grammaticos, A. Ramani, and V. Papageorgiou, Phys. Rev. Lett. **67**, 1825–1828 (1991); A. Ramani, B. Grammaticos, and J. Hietarinta, Phys. Rev. Lett. **67**, 1829–1832 (1991).

[5] J. Hietarinta and C. Viallet, Phys. Rev. Lett. **81**, 325–328 (1998).

[6] A. Veselov, Commun. Math. Phys. **145**, 181–193 (1992); G. Falqui and C. Viallet, Commun. Math. Phys. **154**, 111–125 (1993); M. P. Bellon and C.-M. Viallet, Commun. Math. Phys. **204**, 425–437 (1999); C.-M. Viallet, in *SIDE III*, CRM Proceedings of Lecture Notes Vol. 25 (AMS, Providence, 2000), pp. 439–444; T. Takenawa, J. Phys. A **34**, 10 533–10 545 (2001).

[7] M. J. Ablowitz, R. Halburd, and B. Herbst, Nonlinearity **13**, 889–905 (2000).

[8] K. V. Rerikh, J. Geom. Phys. **24**, 265–290 (1998).

[9] E. Jen, Commun. Math. Phys. **119**, 13–28 (1988); F. Vivaldi, Nonlinearity **5**, 133–147 (1992); A. Batra and P. Morton, Rocky Mountain J. Math. **24**, 453–481 (1994); **24**, 905–932 (1994); P. Morton, Finite Fields Appl. **3**, 11–24 (1997); S. D. Cohen and D. Hachenberger, Contemp Math. **225**, 17–32 (1999).

[10] A. Bobenko, M. Bordemann, C. Gunn, and U. Pinkall, Commun. Math. Phys. **158**, 127–134 (1993); M. Bruschi and P. M. Santini, Physica (Amsterdam) **70D**, 185–209 (1994); Y. Nakamura and A. Mukaihira, Phys. Lett. A **249**, 295–302 (1998).

[11] E. M. McMillan, in *Topics in Modern Physics. A Tribute to E. U. Condon*, edited by E. Britton and H. Odabasi (Colorado University Press, Boulder, 1971), pp. 219–244.

[12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, Oxford, 1979).

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Application Vol. 20 (Addison-Wesley, Reading, MA, 1983); H. Stichtenoth, *Algebraic Function Fields and Codes* (Springer-Verlag, New York, 1991); H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications* (Cambridge University Press, Cambridge, 2001).

[14] G. R. W. Quispel, J. A. G. Roberts, and C. J. Thompson, Phys. Lett. A **126**, 419–421 (1988); Physica (Amsterdam) **34D**, 183–192 (1989).

[15] J. A. G. Roberts and F. Vivaldi (to be published).

[16] N. Abarenkova, J-Ch. Anglès d'Auriac, S. Boukraa, and J-M Maillard, Physica (Amsterdam) **144D**, 387–433 (2000).

[17] P. J. Cameron, *Permutation Groups* (Cambridge University Press, Cambridge, 1999).

[18] L. A. Shepp and S. P. Lloyd, Trans. Am. Math. Soc. **121**, 340–357 (1966).