

Maps over finite fields: integrability and reversibility

FRANCO VIVALDI

(joint work with John A. G. Roberts)

In the theory of dynamical systems, integrability (existence of invariants of the motion) and reversibility (existence of conjugacy with inverse map) are important structural properties. We let two-dimensional algebraic mappings act on finite fields, and, based on experimental evidence, conjecture the existence of limit distributions of the length of the orbits for the integrable and reversible cases, as well as for the case in which both properties are absent. Such distributions feature considerable rigidity (independence from the mapping). These phenomena are relevant to the development of criteria for integrability/reversibility for algebraic mappings.

A mapping $L : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ is *integrable* if there exists a function $I : \mathbb{C}^2 \rightarrow \mathbb{C}$, non-constant and defined almost everywhere in \mathbb{C} , such that $I = I \circ L$. We speak of *algebraic integrability* if L , L^{-1} and I are rational functions. The phase space of an integrable system foliates into level sets of the function I , which are invariant under the dynamics; moreover, the motion on each level set is regular (indeed, conjugate to a rotation, for almost all bounded level sets). If L is algebraically integrable and of infinite order, then the level sets of I are algebraic curves of genus at most one [8].

A smooth mapping L is *R-reversible* if there exists an involution G such that

$$L^{-1} = G \circ L \circ G^{-1} \quad \det(dG) < 0$$

where dG is the Jacobian of G . In the polynomial case there is a well-developed theory, which, in particular, leads to normal forms for reversible maps [2, 1].

A planar mapping L with coefficients in an algebraic number field can be made to act on \mathbb{F}_q^2 , for a suitable q . (If L is rational rather than polynomial, we shall implicitly assume that the reduced map \bar{L} acts on the projective plane $P_2(\mathbb{F}_q)$.) We look for fields \mathbb{F}_q for which \bar{L} exists together with the relevant reduced quantity i.e., the integral \bar{I} , or the reversor \bar{G} . Letting $q = p^n$, we keep n fixed and let $p \rightarrow \infty$ through a suitable set of prime numbers p . These primes have positive density, from Cebotarev's theorem, and we are interested in the study of the asymptotic (large p) behaviour of the length of the orbits of \bar{L} and their distribution. For simplicity, in what follows we assume $q = p$.

Let $T(z)$ be the length of the orbit of L through the point $z \in \mathbb{F}_p^2$. We define

$$(1) \quad D_p(x) = \frac{1}{p^2} \#\{z : T(z) \leq px\} \quad D(x) = \lim_{p \rightarrow \infty} D_p(x).$$

The distribution D_p represents the probability that a point chosen at random in \mathbb{F}_p^2 belongs to a cycle of length not exceeding px , and D is its limiting value.

Extensive experimental evidence suggest the following [6, 5, 7]

Conjecture 1. *The limit (1) exists for any bi-rational map L .*

- (i) If L is algebraically integrable, then $D(x)$ is a step function with steps at $1/n, n = 1, 2, \dots$.
- (ii) If L is R -reversible and possesses a single family of reversing symmetries, then $D(x) = 1 - e^{-x}(1 + x)$.
- (iii) If L is neither integrable nor R -reversible, then $D(x) = 0$.

To obtain a non-trivial limit in case (iii) one must scale orbits differently. We define

$$D'_p(x) = \frac{1}{p^2} \#\{z : T(z) \leq p^2 x\} \quad \langle D' \rangle_p(x) = \frac{1}{\#L_p} \sum_{m \in L_p} D'_m(x).$$

The average $\langle D' \rangle_p$ is computed over the set L_p of all primes not exceeding p at which the map L can be reduced. Averaging is required by the presence of very long cycles (of order p^2), which is a signature of random permutations.

Conjecture 2. *For every non-integrable bi-rational map, which is not R -reversible and has no other symmetry, we have*

$$\lim_{p \rightarrow \infty} \langle D' \rangle_p(x) = x.$$

A heuristic justification of conjecture 1(i) goes as follows [3]. A bi-rational map of infinite order, which acts on a curve of genus one, can be shown to be conjugate to a translation $x \mapsto x + \omega$ with respect to the group law on the corresponding Weierstrass curve. Upon reduction to a finite field, all the orbits on that curve will have the same length, while the normalized (divided by p) number of points on the curve approaches 1, due to the Hasse-Weil bound. Thus the distribution D , if it exists, must have steps at the reciprocal of the positive integers, and the size of the step at $1/n$ is the probability that ω generates a subgroup of index n in E/\mathbb{F}_p , where E is the given curve. The sample space here is the set of curves that foliate \mathbb{F}_p^2 . Thus the existence of the distribution D rests on the validity of a variant of the elliptic analogue of Artin's conjecture [4].

REFERENCES

- [1] M. Baake and J. A. G. Roberts, *Symmetries and reversing symmetries of polynomial automorphisms of the plane*, Nonlinearity (2005), to appear.
- [2] A. Gómez and J. D. Meiss, *Reversors and symmetries for polynomial automorphisms of the complex plane*, Nonlinearity **17** (2004) 975-1000; nlin.CD/0304035 v2.
- [3] D. Jogia, J. A. G. Roberts, and F. Vivaldi, *An algebraic-geometric approach to integrable maps of the plane*, in preparation.
- [4] M. RamMurty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** 1988, 59–67.
- [5] J. A. G. Roberts, D. Jogia, and F. Vivaldi, *The Hasse-Weil bound and integrability detection in rational maps*, J. Nonl. Math. Phys. **10** (2003), 166–180.
- [6] J. A. G. Roberts and F. Vivaldi, *Arithmetical method to detect integrability in maps*, Phys. Rev. Lett. **90** 3 (2003), [034102].
- [7] J. A. G. Roberts and F. Vivaldi, *Signature of time-reversal symmetry in polynomial automorphisms over finite fields*, preprint (2004).
<http://www.maths.qmul.ac.uk/~fv/research/Symmetry.pdf>.
- [8] A. P. Veselov, *Integrable maps*, Russian Math. Surveys **46** (1991) 1–51.