HILBERT'S NULLSTELLENSATZ AND MODULAR REDUCTIONS OF ALGEBRAIC DYNAMICAL SYSTEMS

CARLOS D'ANDREA, ALINA OSTAFE, IGOR E. SHPARLINSKI, AND MARTÍN SOMBRA

Abstract. We use an explicit form of Hilbert's Nullstellensatz to estimate the largest prime and the number of primes p such that a reduction modulo p of a zero dimensional variety over $\mathbb{Q}$ becomes of positive dimension. We apply these estimates to studying cyclic points and intersection of orbits of algebraic dynamical systems in finite fields.

1. Introduction

The goal of the work, which is still in progress, is to extend the scope of application of algebraic geometric methods to algebraic dynamical systems, that is, to dynamical systems generated by iterations of rational functions.

For simplicity, in this short description I will present the results we obtain only for polynomial systems, however, similar results also hold for rational functions, see [6].

Let

$$\mathcal{F} = \{F_1, \ldots, F_m\}, \qquad F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m], \tag{1}$$

a system of be m polynomials in m variables over $\mathbb{Z}$. For each $i = 1, \ldots, m$ we define the k-th iteration of the rational function F_i by the recurrence relation

$$F_i^{(0)} = X_i, \quad F_i^{(n)} = F_i\left(F_1^{(n-1)}, \ldots, F_m^{(n-1)}\right), \quad n = 1, 2, \ldots, \tag{2}$$

see [2, 14, 15] for a background on dynamical systems associated with such iterations.

Given a vector $\mathbf{u} \in \mathbb{C}^m$ over the complex numbers, we define the orbit of $\mathbf{u}$, which we denote by $\mathcal{O}_{\mathcal{F},\mathbf{u}}$, as the sequence of vectors $\mathbf{u}_n = (u_{n,1}, \ldots, u_{n,m}) \in \mathbb{C}^m$ defined by the recurrence relation

$$u_{n+1,i} = F_i(u_{n,1}, \ldots, u_{n,m}), \qquad n = 0, 1, \ldots, \quad i = 1, \ldots, m,$$

with $\mathbf{u}_0 = \mathbf{u}$. Sometimes we also write

$$\mathbf{u}_n = \mathcal{F}^{(n)}(\mathbf{u}).$$

We say that $\mathbf{u}$ is a periodic point of the polynomial system (1) of order $k \geq 1$ if $\mathbf{u}_n = \mathbf{u}_{n+k}$ for every $n = 0, 1, \ldots$. We note that it is convenient for us not to request that k is the smallest positive integer with this property (that is, a periodic point of order k is also a periodic point of order $k\ell$ for any integer $\ell \geq 1$).

Given a prime p we extend the above definitions in a natural way to periodic points modulo p. We refer to [1, 3, 9, 13, 16] for recent advances in the study of periodic points and period lengths in reductions of orbits of dynamical systems modulo distinct primes. In fact most of our motivation comes from the recently introduced idea of transferring the Hasse principle for periodic points and thus linking local and global periodicity properties, see [17]. Here we show that an explicit form of Hilbert's Nullstellensatz provides a powerful tool which may produce various results in this direction.

2. Number of points on modular reductions of varieties

Here we use several algebraic geometry tools, such as an explicit version of *Hilbert's Nullstellensatz*, see [5, 10], to obtain new results about orbits of reductions modulo a prime p of algebraic dynamical systems.

Our approach is based on several new results about the number of points on reductions modulo primes of an algebraic variety, defined by polynomials over $\mathbb{Z}$, that has only finitely many zeros over $\mathbb{C}$. Namely, we show that for a sufficiently large prime p, such a variety $V/\mathbb{C}$ also has finitely many zeros over the algebraic closure $\overline{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$ of p elements.

Given a polynomial $F \in \mathbb{Z}[X_1, \ldots, X_m]$, we define its height, denoted $\mathrm{h}(F)$, as the logarithm of the maximum of the absolute values of its coefficients. Using *Chow forms* and an explicit version of Hilbert's Nullstellensatz, given in [5], we derive:

Theorem 2.1. *Let $F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m]$ be polynomials of degree at most d and of height at most h. Assume that the zero set of $F_1, \ldots, F_m$ in $\mathbb{C}^m$ has a finite number T of distinct points. Then there exists $\mathfrak{A} \in \mathbb{N}$ with*

$$\log \mathfrak{A} \le (10m+4)d^{2m-1}h + (54m+98)d^{2m}\log(2m+5)$$

such that, if p is a prime not dividing $\mathfrak{A}$, then the zero set of $F_1, \ldots, F_m$ in $\overline{\mathbb{F}}_p^m$ has exactly T points.

Clearly, there are at most $O(\log \mathfrak{A}) = O(d^{2m-1}h + d^{2m})$ primes $p \mid \mathfrak{A}$ (where the impplied constant depends only on m).

We also recall that by the *Bézout theorem*, if T is finite then $T \le d^m$.

3. Periodic points and orbit intersections of polynomial dynamical systems

Estimating the growth of the height and the degrees of the iterations of polynomial systems, we show that Theorem 2.1 yields:

Theorem 3.1. *Let $F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m]$ be polynomials of degree at most d and of height at most h. Assume that a polynomial system (1) has finitely many periodic points of order k over $\mathbb{C}$. Then there exists an integer $\mathfrak{A}_k \ge 1$ with*

$$\log \mathfrak{A}_k \le d^{2km}\left((10m+4)\frac{h}{d-1} + 125(m+2)\log(m+1)\right)$$

such that, if p is a prime number not dividing $\mathfrak{A}_k$, then the reduction of $\mathcal{F}$ modulo p has at most

$$N_k(p) \le d^{km}$$

periodic points of order k.

Our next application is to frequency of orbit intersections of orbits of two polynomial systems. We note that in the univariate case, Ghioca, Tucker and Zieve [7, 8] proved that if two univariate nonlinear complex polynomials have an infinite intersection of their orbits, then they have a common iterate. Clearly such a result cannot hold in finite fields. Instead, based again on an explicit version of *Hilbert's Nullstellensatz*, see [5, 10], we obtain results for the frequency of points in an orbit of the reduction modulo p of an algebraic dynamical system that belong to a given algebraic variety or coincide with a similar point coming from another algebraic dynamical system.

Let $\mathcal{F}$ of the form (1). For a vector $\mathbf{w} \in \overline{\mathbb{Q}}^m$, we denote by

$$\mathrm{Orb}_{\mathbf{w}}(\mathcal{F}) = \{\mathcal{F}^{(n)}(\mathbf{w}) \mid n = 0, 1, \ldots\}.$$

For an algebraic variety $V = Z(\Phi_1, \ldots, \Phi_s)$, $\Phi_i \in \mathbb{Z}[X_1, \ldots, X_m]$, $i = 1, \ldots, s$, we consider the elements of orbits that fall into V and denote

$$\mathfrak{V}_{\mathbf{w}}(\mathcal{F}, V) = \left\{ n \in \mathbb{N} \mid \mathcal{F}^{(n)}(\mathbf{w}) \in V \right\}. \tag{3}$$

We say that the intersection of orbits of $\mathcal{F}$ with V is L-uniformly bounded if there is a constant L depending only on $\mathcal{F}$ and V so that for all initial values $\mathbf{w} \in \overline{\mathbb{Q}}^m$, we have

$$\#\mathfrak{V}_{\mathbf{w}}(\mathcal{F}, V) \le L.$$

For a prime p and an integer N, we define

$$\mathfrak{V}_{\mathbf{w}}(\mathcal{F}, V; p, N) = \left\{ n \in \{0, \ldots, N-1\} \mid \overline{\mathcal{F}}_p^{(n)}(\mathbf{w}) \in \overline{V}_p \right\}$$

for some initial values $\mathbf{w} \in \overline{\mathbb{F}}_p^m$, where $\overline{\mathcal{F}}_p$ and $\overline{V}_p$ are defined by the reductions of the rational function system $\mathcal{F}$ and of the polynomials Φ_j, $j = 1, \ldots, s$, modulo p.

We prove the following result.

Theorem 3.2. *Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ be a system of $m \ge 2$ polynomials in $\mathbb{Z}[X_1, \ldots, X_m]$ of degree at most d and of height at most h. Let V be an algebraic variety defined by the polynomials $\Phi_1, \ldots, \Phi_s \in \mathbb{Z}[X_1, \ldots, X_m]$ of degree at most D and height at most H. We also assume that the intersection of orbits of $\mathcal{F}$ with V is L-uniformly bounded. Then, for any $\varepsilon > 0$ there exists $\mathfrak{B} \in \mathbb{N}$ with*

$$\log \mathfrak{B} \le M^{L+1}(d^{M-1}D)^{s(L+1)} \left(s \left(4\log(m+1) + \frac{H}{d^{M-1}D} + \frac{h}{d-1} \right) + (4m+8)\log(m+3) \right),$$

where $M = \lfloor 2\varepsilon^{-1}(L+2) \rfloor + 1$, such that, if p is a prime number not dividing $\mathfrak{B}$, then for any integer $N \ge M$, we have

$$\max_{\mathbf{w} \in \overline{\mathbb{F}}_p^m} \#\mathfrak{V}_{\mathbf{w}}(\mathcal{F}, V; p, N) \le \varepsilon N.$$

We consider now two polynomial systems $\mathcal{F}, \mathcal{G}$ of the form (1). Taking the polynomials $\Phi_j = X_j - Y_j$, $j = 1, \ldots, m$, in (3), we say that $\mathcal{F}$ and $\mathcal{G}$ have a *uniformly bounded synchronised orbit intersection over* $\overline{\mathbb{Q}}$ if the size of the synchronised intersection of $\mathrm{Orb}_{\mathbf{w}}(\mathcal{F})$ and $\mathrm{Orb}_{\mathbf{w}}(\mathcal{G})$, that is, the size of the set

$$\mathfrak{I}_{\mathbf{w}}(\mathcal{F}, \mathcal{G}) = \left\{ n \in \mathbb{N} \mid \mathcal{F}^{(n)}(\mathbf{w}) = \mathcal{G}^{(n)}(\mathbf{w}) \right\}$$

is L-uniformly bounded over all initial values $\mathbf{w} \in \overline{\mathbb{Q}}^m$, as defined above.

Theorem 3.2 implies that for polynomial systems over $\mathbb{Z}$ with a uniformly bounded synchronised orbit intersection over $\overline{\mathbb{Q}}$, the orbits of their reductions modulo a prime p have a density of intersections at most $\varepsilon > 0$, provided that p does not divide a certain quantity depending only on $\varepsilon > 0$ (and the systems themselves).

Since the polynomial systems $\mathcal{F}$ and $\mathcal{G}$ are defined by polynomials over $\mathbb{Z}$, then for a prime p and an integer N, we can also define, for $\mathbf{u}, \mathbf{v} \in \overline{\mathbb{F}}_p^m$,

$$\mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N) = \left\{ n = 0, \ldots, N-1 \mid \overline{\mathcal{F}}_p^{(n)}(\mathbf{u}) = \overline{\mathcal{G}}_p^{(n)}(\mathbf{v}) \right\},$$

where $\overline{\mathcal{F}}_p$ and $\overline{\mathcal{G}}_p$ are the reductions of the polynomial systems $\mathcal{F}$ and $\mathcal{G}$ modulo p. Note that the quantity $\mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N)$ is defined in a more general situation for arbitrary initial points $\mathbf{u}, \mathbf{v} \in \overline{\mathbb{F}}_p^m$ while the uniform boundness is requested only for the same initial vector. However this distinction is not essential (as if two orbit intersect, after this intersection they can be considered as orbits originating from the same point). For instance, we obviously have

$$\max_{\mathbf{u},\mathbf{v} \in \overline{\mathbb{F}}_p^m} \# \mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N) \le 1 + \max_{\mathbf{w} \in \overline{\mathbb{F}}_p^m} \# \mathfrak{I}_{\mathbf{w},\mathbf{w}}(\mathcal{F}, \mathcal{G}; p, N).$$

We derive from Theorem 3.2 the following result:

Corollary 3.3. *Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ and $\mathcal{G} = \{G_1, \ldots, G_m\}$ be two systems of polynomials in $\mathbb{Z}[X_1, \ldots, X_m]$ of degree at most d and of height at most h and with an L-uniformly bounded synchronised orbit intersection over $\overline{\mathbb{Q}}$. For any $\varepsilon > 0$ there exists $\mathfrak{B} \in \mathbb{N}$ with*

$$\log \mathfrak{B} \le M^{L+1} d^{m(M-1)(L+1)} \left(h \frac{m}{d-1} + (12m + 8) \log(2m + 3) \right),$$

where $M = \lfloor 2\varepsilon^{-1}(L+2) \rfloor + 1$, such that, if p is a prime number not dividing $\mathfrak{B}$, then for any integer $N \ge M$, we have

$$\max_{\mathbf{u},\mathbf{v} \in \overline{\mathbb{F}}_p^m} \# \mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N) \le \varepsilon N.$$

Remark 3.4. Our bounds depend on the bounds on degree and height (that is, the size of the coefficients) growth of the iterates (2). So it is natural to expect that when the growth is slower then "generic" one can expect stronger estimates. In [6] we demonstrate this on the example of the polynomial system $\mathcal{F} = \{F_1, \ldots, F_m\}$ with

$$F_i = X_i G_i + H_i, \qquad G_i, H_i \in \mathbb{Z}[X_{i+1}, \ldots, X_m], \ i = 1, \ldots, m,$$

satisfying certain conditions. Such systems have been introduced in [12], where it is also shown that the degree of the kth iterates grows polynomially with k (instead of the typically expected exponential growth).

Acknowledgements

The authors are very grateful to Dragos Ghioca, Luis Miguel Pardo, Thomas Tucker and Michael Zieve for many valuable discussions.

During the preparation of this work, D'Andrea was partially supported by the MICINN research project MTM2010-20279, Ostafe was by the Swiss National Science Foundation Grant PA00P2–139679, Shparlinski by the Australian Research Council Grant DP130100237, and Sombra by the MINECO research project MTM2012-38122-C03-02.

References

[1] A. Akbary and D. Ghioca, 'Periods of orbits modulo primes', *J. Number Theory*, **129** (2009), 2831–2842.

[2] V. Anashin and A. Khrennikov, 'Applied algebraic dynamics', Walter de Gruyter, Berlin. 2009.

[3] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon and T. J. Tucker, 'Periods of rational maps modulo primes', *Math. Ann.*, **355** (2013), 637–660.

[4] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge Univ. Press, Cambridge, 2006.

[5] C. D'Andrea, T. Krick and M. Sombra, 'Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze', *Annales Sci. de l'ENS* **46** (2013), 549-627.

[6] C. D'Andrea, A. Ostafe, I. Shparlinski and M. Sombra, 'Hilbert's Nullstellensatz and modular reductions of algebraic dynamical systems', *Preprint*, 2014.

[7] D. Ghioca, T. Tucker and M. Zieve, 'Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture', *Inventiones Math.*, **171** (2008), 463–483.

[8] D. Ghioca, T. Tucker and M. Zieve, 'Linear relations between polynomial orbits', *Duke Math. J.*, **161** (2012), 1379–1410.

[9] R. Jones, 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials', *J. Lond. Math. Soc.*, **78** (2008), 523–544.

[10] T. Krick, L. M. Pardo, and M. Sombra, 'Sharp estimates for the arithmetic Nullstellensatz', *Duke Math. J.*, **109** (2001), 521–598.

[11] M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, Berlin, 1992.

[12] A. Ostafe and I. E. Shparlinski, 'On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators', *Math. Comp.*, **79** (2010), 501–511.

[13] J. A. G. Roberts and F. Vivaldi, 'A combinatorial model for reversible rational maps over finite fields', *Nonlinearity*, **22** (2009), 1965–1982.

[14] K. Schmidt, *Dynamical systems of algebraic origin*, Progress in Math., v.128. Birkhäuser Verlag, Basel, 1995.

[15] J. H. Silverman, *The arithmetic of dynamical systems*, Springer, New York, 2007.

[16] J. H. Silverman, 'Variation of periods modulo p in arithmetic dynamics', *New York J. Math.*, **14** (2008), 601–616.

[17] A. Towsley, 'A Hasse principle for periodic points', *Intern. J. Number Theory*, **8** (2013), 2053–2068.

Departament d'Àlgebra i Geometria, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain

E-mail address: cdandrea@ub.edu

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: alina.ostafe@unsw.edu.au

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au

ICREA and Departament d'Àlgebra i Geometria, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain

E-mail address: sombra@ub.edu