Hilbert’s Nullstellensatz and polynomial dynamical systems

Carlos D’Andrea

EACA 2014 Barcelona – June 19 2014

with Alina Ostafe (New South Wales, Australia), Igor Shparlinski (New South Wales, Australia) & Martin Sombra (Barcelona)
\( \mathbb{K} \) is a field, 
\[ \mathcal{R} = R_1, \ldots, R_m \in \mathbb{K}(X_1, \ldots, X_m) \]
a system of \( m \) rational functions in \( m \) variables over \( \mathbb{K} \), i.e.
\[ R_i = \frac{F_i}{G_i}, \quad F_i, G_i \in \mathbb{K}[X_1, \ldots, X_m] \]
For $i = 1, \ldots, m$ we define the $k$-th iteration of $R_i$ by the recurrence relation

\[
\begin{align*}
R_i^{(0)} &= X_i \\
R_i^{(n)} &= R_i\left(R_1^{(n-1)}, \ldots, R_m^{(n-1)}\right) \\
&= \frac{F_i\left(R_1^{(n-1)}, \ldots, R_m^{(n-1)}\right)}{G_i\left(R_1^{(n-1)}, \ldots, R_m^{(n-1)}\right)} \\
n &= 1, 2, 3, \ldots
\end{align*}
\]
Orbits

Starting with $\vec{u} \in \mathbb{K}^m$, its orbit is the sequence

$$\begin{align*}
\vec{u}_0 &= \vec{u} \\
\vec{u}_{n+1} &= (R_1, \ldots, R_m)(\vec{u}_n) \\
&= (R_1^{(n+1)}, \ldots, R_m^{(n+1)})(\vec{u})
\end{align*}$$

with $n = 0, 1, 2 \ldots$
Finite orbits

The orbit terminates when $\vec{u}_n$ is a pole of one among $R_1, \ldots, R_m$

$\vec{u}$ is a $k$-periodic point of order $k \geq 1$ if $\vec{u}_n = \vec{u}_{n+k}$, $\forall n = 0, 1, \ldots$
Changing the field

- If $K = \mathbb{C}$, classical theory (37XX at MSC2010)
- If $K$ is finite, then every orbit either terminates or eventually becomes periodic
Related work

Open questions

- distribution of the period length
- number of periodic points
- number of common values in orbits of two distinct algebraic dynamical systems
- ...

Carlos D’Andrea
Hilbert’s Nullstellensatz and polynomial dynamical systems
Our results
(D-Ostafe-Shparlinski-Sombra)

Works for
\( R_1, \ldots, R_m \in \mathbb{Z}(X_1, \ldots, X_m) \) of

- degree at most \( d \geq 2 \)
- height at most \( h \)

Assuming that the dynamical system
determined by \( \mathcal{R} \) has finite periodic
points of order \( k \) over \( \mathbb{C} \)
Theorem (D-Ostafe-Shparlinski-Sombra)

\[ \exists A_k \in \mathbb{N}_{\geq 1} \text{ with } \log A_k \text{ bounded by } \]

\[ (d^k m^k + 1)^{2m+2} \left( (2k + \frac{hm}{dm - 1}) (10m + 14) + (54m + 152) \log(2m + 7) \right) \]

such that, if \( p \) is a prime not dividing \( A_k \), the dynamical system \( \mathcal{R} \mod p \) has at most \( (d^k m^k + 1)^{m+1} \) periodic points of order \( k \).
Main Tool: Effective versions of Hilbert’s Nullstellensatz

\[ F, F_1, \ldots, F_\ell \in \mathbb{K}[x_1, \ldots, x_m] \]

- **Weak Version**

\[ V_{\mathbb{K}}(F_1 = 0, \ldots, F_\ell = 0) = \emptyset \iff \langle F_1, \ldots, F_\ell \rangle = 1 \]

- **Strong Version**

\[ F \big|_{V_{\mathbb{K}}(F_1 = 0, \ldots, F_\ell = 0)} = 0 \iff F^r \in \langle F_1, \ldots, F_\ell \rangle, \ r > 0 \]
If $F, F_1, \ldots, F_\ell \in \mathbb{Z}[x_1, \ldots, x_m]$ of degree bounded by $d$ and height bounded by $h$ there exist $b \in \mathbb{Z} \setminus \{0\}$, $Q_1, \ldots, Q_\ell \in \mathbb{Z}[x_1, \ldots, x_m]$ with

$$\log b \leq C(M, \ell)d^{n+1}(h + d)$$

and $F_1 Q_1 + \ldots + F_\ell Q_\ell = bF^r$
For $F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m]$ of degrees $\leq d$ height $\leq h$, and $\#V_{\mathbb{C}}(F_1, \ldots, F_m) = T$, $\exists A \in \mathbb{Z}_{>0}$ with

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

such that $\#V_{\overline{\mathbb{F}}_p}(F_1, \ldots, F_m) = T$ if $p \nmid A$
In our case

\[ R^k_i = \frac{F^k_i}{G^k_i}, \ i = 1, \ldots, m \]

We apply the estimates to

\[ F_1^k - x_1 G_1^k, \ldots, F_m^k - x_m G_m^k \]

of degrees \( d^k \) and heights \( \leq \frac{d^k-1}{d-1} h \)
Some remarks

- There are examples showing that the bound is tight.
- Better bounds for more “tailored” systems.
- Bound is sharp in $\overline{\mathbb{F}}_p$. 
Another application: Orbit intersections

For $\vec{w} \in \mathbb{K}^m$ set

$$O_{\vec{w}}(\mathcal{R}) = \{ (R_1, \ldots, R_m)^{(n)}(\vec{w}) \mid n \geq 0 \}$$

For an algebraic variety $V$ we want to estimate the number of points in

$$O_{\vec{w}}(\mathcal{R}) \cap V$$
Related work on boundness


...
The intersection of orbits of $\mathcal{R}$ with $V$ is $L$-uniformly bounded if

\[ \exists L = L(\mathcal{R}, V) \text{ such that } \#O_{\mathbf{w}}(\mathcal{R}) \cap V \leq L \quad \forall \mathbf{w} \in \overline{K}^m \]
If $R \in \mathbb{Z}(x_1, \ldots, x_m)^m$ for a prime $p$ and $N \in \mathbb{N}$,

$$O_{\vec{w},R,V}^{p,N} = \{ R_p^{(n)}(\vec{w}) \in \overline{V}_p, \ 0 \leq n < N \}$$

$\overline{V}_p$ is the variety defined in $\overline{\mathbb{F}}_p^m$ by the equations of $V \mod p$
Our results
(D-Ostafe-Shparlinski-Sombra)

Works for \( R \in \mathbb{Z}(X_1, \ldots, X_m)^m \) of degree \( \leq d \) and height \( \leq h \)

\( V \) is defined by polynomials of degree \( \leq D \) and height \( \leq H \)

Assuming that the intersection of orbits of \( R \) with \( V \) is \( L \)-uniformly bounded in \( \mathbb{C}^m \)
Theorem (D-Olafe-Shparlinski-Sombra)

For any $\varepsilon \in (0, 1/2)$, $\exists B \in \mathbb{N}$ with

$$\log B \leq M^{L+1}(d^{M-1}Dm^{M-1} + 1)^{(s+1)(L+1)} \times$$

$$\left( (s + 1)(2(M - 1) + \frac{H}{d^{M-1}Dm^{M-1}} + h) \right)$$

$$+(4m + 12)\log(m + 4)$$

where $M = \lfloor 2\varepsilon^{-1}(L + 2) \rfloor + 1$ such that if $p \mid B$, $\forall N \geq M$ then $\max_{\vec{w} \in \mathbb{F}_p^m} \#O_{\vec{w}, \mathcal{R}, \mathcal{V}}^{p, N} \leq \varepsilon N$. 

Carlos D’Andrea

Hilbert’s Nullstellensatz and polynomial dynamical systems
More (possible) Applications of Effective Nullstellensatz

- Synchronized orbit intersections (D-Ostafe-Shparlinski-Sombra)
- Arbitrary finite fields
- “Diameters” of polynomial dynamical systems
- Points in varieties of small subgroups ...
Thanks!