SINGULARITY PROPERTIES OF CONVOLUTIONS OF ALGEBRAIC MORPHISMS AND PROBABILISTIC WARING TYPE PROBLEMS

YOTAM HENDEL (JOINT WORK WITH ITAY GLAZER)

1. Motivation: Waring's problem

Theorem 1.1 (Lagrange, 1770). *For every number $x \in \mathbb{N}$, we have $x = a^2 + b^2 + c^2 + d^2$ for some $a, b, c, d \in \mathbb{N}$.*

Question 1.2 (Waring's problem, 1770). *Let $k \in \mathbb{N}$. Does there exist $g(k) \in \mathbb{N}$ such that for every $x \in \mathbb{N}$ we have $x = \sum_{i=1}^{g(k)} a_i^k$?*

Answer: Yes! (Hilbert, 1909).

Definition 1.3 (Convolution). *Let $\varphi : X \to G$ and $\psi : Y \to G$ be maps from sets X and Y to an algebraic structure $(G, \cdot)$. We define their convolution $\varphi * \psi : X \times Y \to G$ by*

$$\varphi * \psi(x, y) = \varphi(x) \cdot \psi(y).$$

We further denote the m-th self-convolution of φ by $\varphi^{*m} : X \times \ldots \times X \to G$.

Example 1.4. *Given $k \in \mathbb{N}$, take $\varphi_k : X := \mathbb{N} \to (\mathbb{N}, +)$ to be $\varphi_k(x) = x^k$.*

Then $\varphi_k^{*m}(x_1, \ldots, x_m) = x_1^k + x_2^k + \ldots x_m^k$ where $\varphi_k^{*m} : \mathbb{N}^m \to \mathbb{N}$.

Waring's problem can thus be rephrased as follows:

Question 1.5. *Does there exist $m \in \mathbb{N}$ such that $\varphi_k^{*m} : \mathbb{N}^m \to \mathbb{N}$ is surjective?*

2. Waring type and probabilistic Waring type problems

Given the definition of convolution as above, by replacing φ_k and $(\mathbb{N}, +)$, we may ask an analogue of Waring's problem, referred to as a Waring type problem.

Definition 2.1 (Words, Lie algebra words)**.**

(1) *A word is an element of the free group F_r on r elements (e.g. the commutator word $w = xyx^{-1}y^{-1} \in F_2$).*

(2) *A Lie algebra word is an element of the free Lie algebra $\mathcal{L}_r$ on r elements (e.g. $w = 2X - 7Y + [[[X, Y], Y], Y] \in \mathcal{L}_r$).*

Words and Lie algebra words give rise to word map by plugging in groups or Lie algebras.

Example 2.2. *Let $w \in F_2$ be the commutator word. Then it induces a word map on every group G by $\varphi_w(x, y) = xyx^{-1}y^{-1}$ and its self-convolution is the word map induced by the concatenation $w * w$:*

$$\varphi_w^{*2} = \varphi_w * \varphi_w = \varphi_{w*w}(x_1, y_1, x_2, y_2) = (x_1y_1x_1^{-1}y_1^{-1}) \cdot (x_2y_2x_2^{-1}y_2^{-1}).$$

Furthermore, if G is an algebraic group then these maps are algebraic morphisms.

Some interesting results on Waring type problems in different families:

(1) **Borel '83:** If $1 \neq w \in F_r$, then $\varphi_w : G^r \to G$ is dominant(=has dense image) for any connected semi-simple algebraic group G. In particular $\varphi_w^{*2} : G^{2r} \to G$ is surjective.

(2) **Larsen-Shalev-Tiep '11:** For any $1 \neq w \in F_r$ there exists $N(w)$ such that for any non-abelian finite simple group G with $|G| > N(w)$ the map $\varphi_w^{*2} : G^{2r} \to G$ is surjective.

(3) **Bandman-Gordeev-Kunyavskii-Plotkin '12:** If $w \in \mathcal{L}_r$ is a Lie algebra word such that $\varphi_w : \mathfrak{sl}_2^r \to \mathfrak{sl}_2$ is non-trivial, then $\varphi_w : \mathfrak{g}^r \to \mathfrak{g}$ is dominant for any semi-simple Lie algebra $\mathfrak{g}$.

We are interested in the relative analogue of Waring type problems:

Question 2.3 (Non-precise)**.** *Let $\varphi : X \to G$ be a map from a set X to a group G. Does there exist $k \in \mathbb{N}$ such that $\varphi^{*k} : X^k \to G$ has uniform fibers?*

The word 'uniform' can mean different things in different settings. For example,

(A) Algebraic Geometry (X algebraic variety, G algebraic group):

(B) Finite Groups (X, G finite):

Remark 2.4 (The probabilistic Waring type problem)**.** *In the settings of finite sets, let ν_X be the uniform probability measure on X. $\varphi : X \to G$ induces a random walk on G whose probability measure is $\varphi_*(\nu_X)(g) := \frac{|\varphi^{-1}(g)|}{|X|}$, and it also holds that*

$$\varphi_*(\nu_X) * \varphi_*(\nu_X)(g) = \sum_{h\in G} \varphi_*(\nu_X)(h)\varphi_*(\nu_X)(h^{-1}g) = \sum_{h\in G} \frac{|\varphi^{-1}(h) \times \varphi^{-1}(h^{-1}g)|}{|X|^2} = (\varphi^{*2})_*(\nu_X)(g).$$

Thus item (B) can be rephrased as follows:

Question 2.5. *How many convolution powers do we need so that φ^{*k} induces a measure which is close to the uniform probability measure ν_G on G?*

3. Our settings: algebraic Waring type problems

- Let $\varphi : X \to G$ be a dominant $\mathbb{Z}$-morphism where $X_{\mathbb{Q}}$ is a smooth, geometrically irreducible variety, and G is a connected algebraic group.

The following two aspects of $\varphi : X \to G$ are closely related:

(A) The singularity properties of $\varphi : X \to G$.

(B) Given a family $\mathcal{A}$ of finite rings, the distance of $\varphi_*(\nu_{X(A)})$ from the uniform probability measure $\nu_{G(A)}$ on $G(A)$, when $A \in \mathcal{A}$ varies.

Let's consider the connection between (A) and (B) for two families of finite rings.

3.1. Flatness and counting points over finite fields.

- We first consider φ with respect to the family $\mathcal{F} = \{\mathbb{F}_p\}_{p\in\mathcal{P}}$.
- Studying the probabilistic Waring problem with respect to $\{\varphi : X(\mathbb{F}_p) \to G(\mathbb{F}_p)\}_p$ corresponds to asking when is $\varphi^{*k} : X^k \to G$ flat.

Fact 3.1. *A dominant morphism $\varphi : X \to Y$ between smooth irreducible varieties is flat if and only if* $\dim(\varphi^{-1} \circ \varphi(x)) = \dim(X) - \dim(Y)$ *for all* $x \in X$.

By the Lang-Weil estimates, the number of points of a $\mathbb{Z}$-scheme over finite fields is governed by its dimension:

Theorem 3.2 (Lang-Weil estimates)**.** *Let X be a finite type $\mathbb{Z}$-scheme and let $c(X,p)$ denote the number of top dimensional geometrically irreducible components of $X_{\overline{\mathbb{F}}_p}$ defined over $\mathbb{F}_p$. Then for every p large enough it holds that*

$$\left| \frac{|X(\mathbb{F}_p)|}{p^{\dim X_{\mathbb{Q}}}} - c(X,p) \right| < O(p^{-\frac{1}{2}}).$$

3.2. **The (FRS) property and counting points over finite rings of the form $\mathbb{Z}/p^k\mathbb{Z}$.**

- We now consider the family of finite rings $\mathcal{R} = \{\mathbb{Z}/p^k\mathbb{Z}\}_{p,k}$, i.e. the family of maps $\{\varphi : X(\mathbb{Z}/p^k\mathbb{Z}) \to G(\mathbb{Z}/p^k\mathbb{Z})\}_{p,k}$.
- Studying probabilistic Waring type problem with respect to $\mathcal{R}$ corresponds to trying to get a morphism whose fibers have tame singularity properties after enough convolutions.

Definition 3.3. *Let X be a variety. We say X has rational singularities if*

(1) *X is normal.*

(2) *For every resolution of singularities $p : \widetilde{X} \to X$ we have $R^i p_*(\mathcal{O}_{\widetilde{X}}) = 0$ for $i > 0$.*

Example 3.4. $\{\sum_{i=1}^{r} x_i^{n_i} = 0\} \subset \mathbb{A}^r$ *has rational singularities if and only if* $\sum_{i=1}^{r} \frac{1}{n_i} > 1$ *($r \geq 2$).*

Theorem 3.5 (Aizenbud-Avni '18)**.** *Let X be a $\mathbb{Z}$-scheme such that $X_{\mathbb{Q}}$ is a local complete intersection equidimensional variety. Then X has rational singularities if and only if there*

exists a finite set of primes S such that for every $p \notin S$ and every $k \in \mathbb{N}$ we have

$$\left| \frac{|X(\mathbb{Z}/p^k\mathbb{Z})|}{p^{k \dim X_{\mathbb{Q}}}} - c(X,p) \right| < O(p^{-\frac{1}{2}}).$$

Definition 3.6. *Let $\varphi : X \to Y$ be a map between smooth varieties. We say φ is (FRS) if it is a flat morphism with reduced fibers of rational singularities.*

Remark 3.7. *In an upcoming work (Cluckers-Glazer-H. '20) we prove a uniform version (i.e. for morphisms) of the above theorem using model-theoretic tools.*

4. Main results

4.1. Convolutions in algebraic geometry - the general case.

Proposition 4.1. *Let S be a property of morphisms which is preserved under base change and composition. Let $\varphi : X \to G$ be a K-morphism with property S, let $\psi : Y \to G$ be any K-morphism, and assume that $Y \to \mathrm{Spec}(K)$ satisfies S. Then $\varphi * \psi : X \times Y \to G$ has S.*

Theorem 4.2 (Glazer, H. '19)**.** *Let X be a smooth geometrically irreducible variety, G be an algebraic group and let $\varphi : X \to G$ be a dominant morphism.*

1. *The morphism $\varphi^{*n} : X^n \to G$ is flat if $n \geq \dim G$.*
2. *The morphism $\varphi^{*n} : X^n \to G$ is flat with reduced fibers if $n \geq \dim G + 1$.*
3. *The morphism $\varphi^{*n} : X^n \to G$ is flat with normal fibers if $n \geq \dim G + 2$.*
4. *There exists $N \in \mathbb{N}$ such that $\varphi^{*n} : X^n \to G$ is (FRS) for every $n \geq N$.*

4.2. Convolutions in algebraic geometry - word maps and uniform bounds.

Definition 4.3. *Given $w \in \mathcal{L}_r$ we define the degree of w to be the maximal grade of $\mathcal{L}_r$ in which w is non-zero (where we consider the natural gradation on $\mathcal{L}_r$).*

Example 4.4. *$X - 2[Y,X] + [[X,Y],Y]$ has degree 3.*

Theorem 4.5 (Glazer-H. '19)**.** *Let $w \in \mathcal{L}_r$ be a Lie algebra word of degree d. Then there exists $C < 10^6$ such that for any simple Lie algebra $\mathfrak{g}$ with $\varphi_w|_{\mathfrak{g}^r} \neq 0$ we have*

(1) *if* $n \geq Cd^4$ *then* φ_w^{*n} *is flat,*

(2) *if* $n \geq Cd^6$ *then* φ_w^{*n} *is (FRS).*

Remark 4.6. *n as above must be atleast linear in d as the Lie algebra word map induced by the Engel word $w = [\dots[[X, \underbrace{Y], Y]\dots, Y}_{d \text{ times}}]$ is not flat after $d-1$ self-convolutions.*

Corollary 4.7 (Glazer-H. '19)**.** *Let $w \in F_r$ be a word of length $\ell(w)$. Then there exists $C < 10^6$ such that for any connected semi-simple group G the morphism $\varphi_w^{*n} : G^{nr} \to G$ is (FRS) at $(e, \dots, e)$ if $n \geq C\ell(w)^6$.*

Remark 4.8. *The flatness of group word maps after $O(\ell(w)^4)$ convolutions was proved in a 2019 paper by Larsen-Shalev-Tiep (using different methods than us).*

A case of significant particular interest is the case of the commutator map.

Theorem 4.9 (Glazer-H. '19)**.** *Let $w = [X, Y] \in \mathcal{L}_2$ be the commutator Lie algebra word. Then for every semi-simple Lie algebra $\mathfrak{g}$:*

(1) *The map $\varphi_w^{*2} : \mathfrak{g}^4 \to \mathfrak{g}$ is flat.*

(2) *The map $\varphi_w^{*4} : \mathfrak{g}^8 \to \mathfrak{g}$ is (FRS).*

Corollary 4.10. *$\varphi_{w'}^{*4} : G^8 \to G$ where $w' = xyx^{-1}y^{-1}$ is (FRS) for every semi-simple algebraic group G.*

Remark 4.11. *If $\mathfrak{g} = \mathfrak{sl}_n$, Budur proved (2018) that φ_w^{*2} is already (FRS). For other types, our result gives the best known bounds.*

Theorem 4.12 (Aizenbud-Avni '16, '18)**.** *Let G be a semi-simple, simply connected algebraic group, and let Γ be either*

(1) *a compact open subgroup of $G(\mathbb{Q}_p)$ for some prime p; or*

(2) *$G(\mathbb{Z})$, provided that G has $\mathbb{Q}$-rank≥ 2.*

Set $w' = xyx^{-1}y^{-1}$ and assume that $\varphi_{w'}^{*n} : G^{2n} \to G$ is (FRS). Then there exists a constant C such that, for any $N \in \mathbb{N}$

$$\#\{N\text{-dimensional irreducible } \mathbb{C}\text{-representations of } \Gamma\} < CN^{2n-1}.$$

5. Methods used in the proof of Theorem 4.5

The proof of Theorem 4.5 can roughly be divided as follows:

(1) Reduce to the case of d-homogeneous Lie algebra word maps.
(2) Use brute force (i.e. our previous results on general morphisms on the level of jets) to take care of Lie algebras of low rank ($\mathrm{rk}(\mathfrak{g}) \leq 4d$ where d is the degree of the word).
(3) Encode d-homogeneous word maps using a combinatorial object. Furthermore, make sense of what it means for that combinatorial object to be flat, (FRS) and raised to a convolution power.
(4) Using a sequence of convolutions and degenerations simplify the combinatorial object.
(5) Solve the problem for a simple combinatorial object.

The hard part of the proof is Item (4).

Definition 5.1. *Let $\widetilde{\varphi} : \widetilde{X} \to \widetilde{Y}$ be an $\mathbb{A}^1$-morphism between smooth $\mathbb{A}^1$-varieties where the corresponding diagram over $\mathbb{A}^1$ is $\mathbb{G}_m$ equivariant. $\widetilde{\varphi}_0 : \widetilde{X}_0 \to \widetilde{Y}_0$ is called a degeneration of $\widetilde{\varphi}_1 : \widetilde{X}_1 \to \widetilde{Y}_1$.*

Example 5.2. $X = \{(x, y, t) \in \mathbb{A}^3 : xy = t\}$.

Proposition 5.3. *Given a $\mathbb{G}_m$-equivariant $\mathbb{A}^1$-family as above and a $\mathbb{G}_m$-equivariant section $s : \mathbb{A}^1 \to \widetilde{X}$, if $\widetilde{\varphi}_0 : \widetilde{X}_0 \to \widetilde{Y}_0$ is flat (resp. (FRS)) at $s(0)$, then $\widetilde{\varphi}_1 : \widetilde{X}_1 \to \widetilde{Y}_1$ is flat (resp. (FRS)) at $s(1)$.*

Definition 5.4.

(1) *For any tuple $w = (w_1, \ldots, w_n) \in \mathbb{Z}^n$, we define the w-degree of a monomial* $\deg_w(x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}) := \sum_{i=1}^{n} w_i a_i$.
(2) *We define the symbol* $\mathrm{symb}_w(f)$ *of $f \in K[x_1, \ldots, x_n]$ as the sum of monomials of smallest w-degree.*

Corollary 5.5. *Let $\varphi = (\varphi_1, \ldots, \varphi_m) : \mathbb{A}^n \to \mathbb{A}^m$ be a morphism where φ_i are homogenous degree d polynomials, $w \in \mathbb{Z}^n$ and let $\mathrm{symb}_w(\varphi) = (\varphi_1, \ldots, \varphi_m)$ be the symbol of φ. If $\mathrm{symb}_w(\varphi)$ is flat (resp. (FRS)) at $(0, ..., 0)$, then φ is flat (resp. (FRS)).*

Example 5.6. *Consider $\varphi(x, y, z) = (xy, yz)$. Then*

$$\varphi^{*2}(x, y, z, w, v, u) = (xy + wv, yz + vu),$$

and choosing the weight $w = (1, 0, 0, 0, 0, 1) \in \mathbb{Z}^6$ we have $\mathrm{symb}_w(\varphi)(x, y, z, w, v, u) = (xy, vu)$ which can be thought of as two disjoint copies of the map $\psi(x, y, z) = xy$.
Taking another convolution power, ψ^{*2} can be easily shown to be (FRS), and thus we conclude $\varphi^{*4} : \mathbb{A}^{12} \to \mathbb{A}^2$ is (FRS).