The Hrushovski–Lang–Weil estimates

Yakov Varshavsky

13 December 2021

Workshop

From Geometric Stability Theory to Tame Geometry

in honor of 60^{th} birthday of Ehud Hrushovski

It is my pleasure and honor to give a talk on the conference celebrating Udi's birthday.

I would like to thank the organizers for giving me such a opportunity.

The goal of my talk is to outline the algebro-geometric proof of a twisted version of Lang–Weil estimates, first established by Udi Hrushovski around 2004 using Model Theory.

My plan is first to formulate the result, then to deduce some corollaries, and finally to outline the proof.

This is a joint work with K.V.Shuddhodan.

- Let k be an algebraically closed field, and let σ be an automorphism of k.

  For every closed algebraic subvariety $X \subset \mathbb{A}^m$, we denote by ${}^\sigma X \subset \mathbb{A}^m$ the Galois twist of X.

  Explicitly, ${}^\sigma X$ is the set of all tuples $(\sigma(a_1), \ldots, \sigma(a_m)) \in k^n$, where $(a_1, \ldots, a_m) \in X$.

  Alternatively, for every polynomial $f \in k[x_1, \ldots, x_m]$ we denote by ${}^\sigma f \in k[x_1, \ldots, x_m]$ the polynomial obtained from f by applying f to all of its coefficients.

  If X the set of common zeros of polynomials $f_1, \ldots, f_r$, then ${}^\sigma X$ is the set of common zeros of polynomials ${}^\sigma f_1, \ldots, {}^\sigma f_r$.

- Let $f : X \to Y$ be a morphism between irreducible algebraic varieties of the same dimension, which is dominant, i.e., the image of f is (Zariski) dense.

  Then the field of rational functions $k(X)$ of X is a finite extension of $k(Y)$. So we can form a degree $\deg(f) := [k(X) : k(Y)]$ and inseparable degree $\deg(f)_{\mathrm{insep}} := [k(X) : k(Y)]_{\mathrm{insep}}$.

- To every projective variety $X \subset \mathbb{P}^m$, one associates its degree $\deg(X)$, which measures the complexity of X.

  For example, if $X = Z(f)$ is the set of zeros of a homogeneous polynomial $f \in k[x_0, \dots, x_m]$, then $\deg(X) = \deg(f)$.

- For every closed subvariety $X \subset \mathbb{A}^m$, we denote by $\deg(X)$ the degree $\deg(\overline{X})$ of the closure $\overline{X} \subset \mathbb{P}^m$ of X.

  Note that $\deg({}^{\sigma}X) = \deg(X)$.

Set up:

- Let k be an algebraically closed field of positive characteristic p.
- Let q be a power of p, and let $\sigma = \sigma_q : k \to k$ be the Frobenius automorphism $x \mapsto x^q$.
- Let $X \subset \mathbb{A}^m$ be closed subvariety.
- Let $\phi_{X,q} : X \to {}^{\sigma}X$ be the geometric Frobenius morphism, defined by the formula $\phi_{X,q}(a_1, \ldots, a_m) = (a_1^q, \ldots, a_m^q)$.
- Let $\Gamma_{X,q} \subset X \times {}^{\sigma}X$ be the graph of $\phi_{X,q}$.
- Let $C \subset X \times {}^{\sigma}X \subset \mathbb{A}^{2m}$ be a closed subvariety.

Now we are ready to formulate our main result:

Theorem 1 (Hrushovski 2004)

For every pair $(m, \delta) \in \mathbb{N}$ there exists a constant $M = M(m, \delta)$ satisfying the following property:
Let (k, p, q, X, C) be a tuple as in set up such that

- $X \subset \mathbb{A}^n$ and $C \subset X \times {}^{\sigma}X$ are closed irreducible subvarieties of dimension d;
- both projections $p_1 : C \to X$ and $p_2 : C \to {}^{\sigma}X$ are dominant,
- either p_1 or p_2 is quasi-finite, i.e., has finite fibers;
- we have inequalities $\deg(X) \leq \delta, \deg(C) \leq \delta$ and $q > M$.

Then the intersection $C \cap \Gamma_{X,q}$ is finite, and its cardinality satisfies

$$\left| \#(C \cap \Gamma_{X,q}) - \frac{\deg(p_1)}{\deg(p_2)_{\mathrm{insep}}} q^d \right| \leq M(q^{d-\frac{1}{2}}).$$

If X is an algebraic variety defined over a finite field $\mathbb{F}_q$, then ${}^\sigma X \cong X$. So for every $n \in \mathbb{N}$, the geometric Frobenius is a morphism $\phi_{X,q^n} : X \to X$, thus its graph Γ_{X,q^n} is a subvariety of $X \times X$.

Therefore Theorem 1 implies the following result:

Theorem 2

Let X be an irreducible algebraic variety of dimension d defined over $\mathbb{F}_q$, and let $C \subset X \times X$ be a closed irreducible subvariety such that

- both projections $p_1 : C \to X$ and $p_2 : C \to X$ are dominant,
- either p_1 or p_2 is quasi-finite.

Then for every $n >> 0$, the intersection $C \cap \Gamma_{X,q^n}$ is finite, and its cardinality has an asymptotic

$$\#(C \cap \Gamma_{X,q^n}) = \frac{\deg(p_1)}{\deg(p_2)_{\text{insep}}} q^{nd} + O(q^{n(d-\frac{1}{2})}).$$

Theorems 1 and 2 have many consequences. For example, the following result has applications among other things to group theory, algebraic geometry and algebraic dynamics.

Corollary 1

Let X be an irreducible algebraic variety defined over $\mathbb{F}_q$, and let $C \subset X \times X$ be an irreducible subvariety such that $p_1 : C \to X$ and $p_2 : C \to X$ are dominant.

Then for every $n >> 0$, the intersection $C \cap \Gamma_{X,q^n}$ is non-empty.

Proof.

If X is affine, $C \subset X \times X$ is closed and p_1 or p_2 are quasi-finite, then the assertion immediately follows from Theorem 2.

The general case easily reduces to it. $\square$

As an illustration, let us explain how Corollary 1 is used for algebraic dynamics.

Corollary 2

In the situation of Corollary 1, the union $\cup_n(C \cap \Gamma_{X,q^n}) \subset C$ is Zariski dense.

Proof.

Let $Z := \overline{\cup_n(C \cap \Gamma_{X,q^n})} \subset C$ be the Zariski closure.

Assume that $Z \neq C$. Then $C' := C \smallsetminus Z \subset C$ is Zariski dense.

Therefore projections $p_1 : C' \to X$ and $p_2 : C' \to X$ are dominant.

So $\cup_n(C' \cap \Gamma_{X,q^n})$ is non-empty by Corollary 1, contradicting to the definition of C'. $\square$

Definition: Let $f : X \to X$ be a morphism. A point $x \in X$ is called f-periodic, if $f^n(x) = x$ for some $n \in \mathbb{N}$.

Corollary 3 (Fakhruddin)

Let X be an algebraic variety over $\overline{\mathbb{F}}_q$, and let $f : X \to X$ be a dominant morphism. Then the set of f-periodic points is Zariski dense.

Proof.

Replacing X by its irreducible component, q by q^n and f by f^m, we can assume that X is irreducible, and both X and f are defined over $\mathbb{F}_q$.

By Corollary 2 applied to the graph $\Gamma_f \subset X \times X$, we see that the subset

$$S = \{x \in X(\overline{\mathbb{F}}_q) \,|\, f(x) = \phi_{X,q^n}(x) \text{ for some } n\} \subset X$$

is Zariski dense.

But every $x \in S$ is f-periodic. Indeed, x belongs to $X(\mathbb{F}_{q^m})$ for some m, in which case we have $f^m(x) = \phi_{X,q^{nm}}(x) = x$. □

To simplify the exposition,

- we will only outline the strategy of the proof of Theorem 2.
- we will assume that p_2 is generically étale, thus $\deg(p_2)_{\mathrm{insep}} = 1$.

Before considering the general case, we will consider the following two particular cases:

1. X is smooth projective, and $p_2 : C \to X$ is étale.
2. $p_2 : C \to X$ is étale, and X has a smooth compactification $\overline{X}$ such that
   - $\overline{X} \smallsetminus X$ is a union of smooth divisors $\{X_i\}_{i \in I}$ with normal crossings;
   - $\overline{X} \smallsetminus X$ is locally C-invariant (this notion will be defined later).

Our strategy will be to express the cardinality of the intersection $\#(C \cap \Gamma_{X,q^n})$ in terms of intersection pairings $\alpha_\beta \cdot [\Gamma_{X_\beta,q^n}] \in \mathbb{Z}$, where

- each X_β is a smooth projective variety over $\mathbb{F}_q$ of dimension d_β;
- $\alpha_\beta \in A_{d_\beta}(X_\beta \times X_\beta)$ is the cycle class of middle dimension;
- $[\Gamma_{X_\beta,q^n}] \in A_{d_\beta}(X_\beta \times X_\beta)$ denotes the class of the graph of Frobenius $\Gamma_{X_\beta,q^n} \subset X_\beta \times X_\beta$.

After this is done, Theorem 2 will follow from a combination of

- Grothendieck–Lefshetz trace formula and
- Deligne's purity theorem.

Notation. Let X be an algebraic variety, and $i \in \mathbb{N}$.

- Denote by $A_i(X)$ the group of i-dimensional cycles on X modulo rational equivalence.
- For every i-dimensional closed subvariety $Y \subset X$, we denote $[Y]$ its class in $A_i(X)$.
- Denote by $H^i(X, \mathbb{Q}_\ell)$ the i-th ℓ-adic cohomology. It is a finite-dimensional vector space over $\mathbb{Q}_\ell$.
- Every morphism $f : X \to Y$ of algebraic varieties induces a morphism $f^* : H^i(Y, \mathbb{Q}_\ell) \to H^i(X, \mathbb{Q}_\ell)$ on ℓ-adic cohomologies.

Assume now that X is a smooth projective variety of dimension d. Then

- For every two cycle classes $\alpha, \beta \in A_d(X \times X)$, one can form an intersection pairing $\alpha \cdot \beta \in \mathbb{Z}$.
- every class $\alpha \in A_d(X \times X)$ defines an endomorphism $H^i(\alpha)$ of $H^i(X, \mathbb{Q}_\ell)$ for every $i = 0, \ldots, 2d$.

The following two classical results are central for what follows:

Grothendieck–Lefschetz trace formula

Let X be a smooth projective variety over k of dimension d.

Then for every class $\alpha \in A_d(X \times X)$ and every endomorphism $f : X \to X$, we have an equality

$$\alpha \cdot [\Gamma_f] = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}(f^* \circ H^i(\alpha), H^i(X, \mathbb{Q}_\ell)).$$

Deligne purity theorem (Weil I)

Let X be a smooth projective variety over $\mathbb{F}_q$.

Then for every field isomorphism $\tau : \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$, every $i \in \mathbb{N}$ and every eigenvalue $\lambda \in \overline{\mathbb{Q}}_\ell$ of the endomorphism $(\phi_{X,q})^*$ of $H^i(X, \mathbb{Q}_\ell)$, we have an equality $|\tau(\lambda)| = q^{i/2}$.

Proposition 1

Assume that X is smooth projective, and that $p_2 : C \to X$ is étale. Then the conclusion of Theorem 2 holds.

Proof.

We claim that for every $n >> 0$, we have an equality

$$\#(C \cap \Gamma_{X,q^n}) = [C] \cdot [\Gamma_{X,q^n}] = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}((\phi_{X,q^n})^* \circ H^i([C]), H^i(X, \mathbb{Q}_\ell)),$$

where

- the first equality holds for because p_2 is étale, thus intersection $C \cap \Gamma_{q^n}$ is transversal;
- the second equality is the Grothendieck–Lefschetz trace formula.

Now the asymptotic of $\#(C \cap \Gamma_{X,q^n})$ follows from a combination of Deligne's purity theorem and the observation that $\dim H^{2d}(X, \mathbb{Q}_\ell) = 1$ and $H^{2d}([C]) = \deg(p_1) \operatorname{Id}$. □

Pink's construction. Assume now that X has a smooth compactification $\overline{X}$ such that $\overline{X} \smallsetminus X$ is a union of smooth divisors $\{X_i\}_{i \in I}$ with normal crossings.

- Consider the blow-up

$$\pi : \widetilde{Y} := \mathrm{Bl}_{\cup_{i \in I}(X_i \times X_i)}(\overline{X} \times \overline{X}) \to \overline{X} \times \overline{X}$$

  of $\cup_{i \in I}(X_i \times X_i) \subset \overline{X} \times \overline{X}$.
- For a subset $J \subset I$, we set $X_J := \cap_{i \in J} X_i$ and $E_J := \pi^{-1}(X_J \times X_J)$.
- Let $i_J : E_J \hookrightarrow \widetilde{Y}$ be the inclusion, and let $\pi_J : E_J \to X_J \times X_J$ be the restriction of π.

Properties.

- $\widetilde{Y}$ is a smooth projective variety of dimension $2d$,
- X_J is a smooth projective variety of dimension $d - |J|$ (possibly empty),
- E_J is a smooth projective variety of dimension $2d - |J|$.

Explanation. Working étale locally we can replace $(\overline{X}, \{X_i\}_{i\in I})$ by $(\mathbb{A}^d, \{Z(x_i)\}_{i=1,\dots,d})$.

In this case, $\widetilde{Y}$ is replaced by $\mathrm{Bl}_0(\mathbb{A}^2)^d$, so all the properties listed above are easy.

Notation.

- For every class $\alpha \in A_d(\widetilde{Y})$ and every $J \subset I$, we set $\alpha_J := (\pi_J)_*(i_J)^*(\alpha) \in A_{d-|J|}(X_J \times X_J)$.
- Let $\widetilde{\Gamma}_{X,q^n} \subset \widetilde{Y}$ be the closure of $\pi^{-1}(\Gamma_{X,q^n}) \subset \widetilde{Y}$, where $\Gamma_{X,q^n} \subset X \times X$ is as earlier.

  (By construction, π is an isomorphism over $X \times X$).

Lemma 1

Assume that $\overline{X} \smallsetminus X$ is locally C-invariant, and let $\widetilde{C} \subset \widetilde{Y}$ be the closure of $\pi^{-1}(C) \subset \widetilde{Y}$.

Then for every $n >> 0$, we have an inclusion $\widetilde{C} \cap \widetilde{\Gamma}_{X,q^n} \subset \pi^{-1}(X \times X)$, and an equality

$$\#(C \cap \Gamma_{X,q^n}) = [\widetilde{C}] \cdot [\widetilde{\Gamma}_{X,q^n}].$$

Lemma 2

For every $\alpha \in A_d(\widetilde{Y})$, we have the following identity

$$\alpha \cdot [\widetilde{\Gamma}_{X,q^n}] = \sum_{J \subseteq I} (-1)^{|J|} \alpha_J \cdot [\Gamma_{X_J,q^n}],$$

where the intersection pairing on the LHS is inside $\widetilde{Y}$, while $\cdot$ on the LHS is inside $X_J \times X_J$.

Proposition 2

In the situation of Theorem 2, assume that $p_2 : C \to X$ is étale, and X has a smooth compactification $\overline{X}$ such that

- $\overline{X} \smallsetminus X$ is a union of smooth divisors $\{X_i\}_{i\in I}$ with normal crossings, (both $\overline{X}$ and the X_i's are defined over $\mathbb{F}_q$);
- $\overline{X} \smallsetminus X$ is locally C-invariant.

Then the conclusion of Theorem 2 holds.

Proof.

Combining Lemmas 1 and 2, we have an equality

$$\#(C \cap \Gamma_{X,q^n}) = \sum_{J\subseteq I} (-1)^{|J|} [\widetilde{C}]_J \cdot [\Gamma_{X_J,q^n}].$$

Now we finish as in Proposition 1. $\square$

Definition:

(a) Let $C \subset X \times X$ and $Z \subset X$ be closed subvarieties.

- We say that Z is <u>C-invariant</u>, if set-theoretically $p_1(p_2^{-1}(Z)) \subseteq Z$.
- We say that Z is <u>locally C-invariant</u>, if for every $x \in Z$ there exists an open neighborhood $U \subset X$ of x such that $Z \cap U \subset U$ is $C \cap (U \times U)$-invariant, where $C|_U := C \cap (U \times U) \subset U \times U$.

(b) Let $C \subset X \times X$ be closed subvariety, let $X \subset \overline{X}$ be an open subvariety, and let $\overline{C} \subset \overline{X} \times \overline{X}$ be the closure of C.

We say that $\overline{X} \smallsetminus X$ is <u>locally C-invariant</u>, if it is locally $\overline{C}$-invariant in the sense of (a).

Now we are ready to sketch the proof of Theorem 2.

Step 1. By Noetherian induction, replacing X by an open subvariety U (and C by $C \cap (U \times U)$) we can assume that X is smooth quasi-affine and p_2 étale.

Step 2. Further replacing X by an open subvariety, we can assume that there exists a compactification $\overline{X}$ of X such that the boundary $\overline{X} \smallsetminus X$ is locally c-invariant.

Step 3. By theorem of de Jong, there exists an alteration $\overline{f} : \overline{X}' \to \overline{X}$ such that $\overline{X}'$ is smooth and $f^{-1}(\overline{X} \smallsetminus X)$ is a union of smooth divisors with normal crossings.

In particular, we can carry out Pink's construction $\pi' : \widetilde{Y}' \to \overline{X}' \times \overline{X}'$ in this case.

Step 4.

- Set $X' := \overline{f}^{-1}(X) \subset \overline{X}'$, let $f : X' \to X$ be the restriction of $\overline{f}$,
- let $[C]' := (f \times f)^*([C]) \in A_d(X' \times X')$ be the refined Gysin pullback of $[C] \in A_d(X \times X)$, and
- let $\alpha' \in A_d(\widetilde{Y}')$ be the "closure" of $\pi'^{-1}([C]') \in A_d(\pi'^{-1}(X' \times X'))$.

Step 5. Combining Lemmas 1 and 2 with the projection formula, we have an equality

$$\#(C \cap \Gamma_{X,q^n}) = \frac{1}{\deg(f)} \sum_{J \subseteq I} (-1)^{|J|} \alpha'_J \cdot [\Gamma_{X'_J,q^n}].$$

Step 6. We finish as in Proposition 1.

Remark: The proof of Theorem 1 has an additional ingredient, a so-called "Hrushovski's norm" on cycle classes, introduced by Udi in his work.

Thank you very much!

Happy birthday and best wishes to Udi!