# Non-standard Frobenius: Introduction

Martin Hils

Équipe de Logique Mathématique, Institut de Mathématiques de Jussieu
Université Paris Diderot – Paris 7

Workshop "Model theory of difference fields and applications"
Université Paris-Sud (Orsay, France), 5 – 9 December 2011

# Plan "Special afternoon on Frobenius"

1. Introduction and motivation (this talk)
2. Proof sketch of the *twisted Lang-Weil estimates*, mainly using difference algebraic geometry. (Talks by Giabicani-Laszlo.)
3. A glimpse of the model theoretic part of the proof, using valued difference fields.

**References:**


- E. Hrushovski, *The Elementary Theory of the Frobenius Automorphisms*, arXiv:math/0406514, 2004.

  (Preprint since 1996; major changes in 2004; still unpublished.)
- Notes of some talks from a working group organised by J.-B. Bost, Y. Laszlo and F. Loeser in Paris (2004-2005).
- G. Giabicani's PhD thesis.

# Outline

Finite and pseudofinite fields

Hrushovski's work on the non-standard Frobenius

Some applications

- Jacobi's bound for difference equations
- Uniformity results for finite simple groups
- Some applications to algebraic dynamics

# Preliminaries: ultrafilters

Recall that $\mathcal{U} \subseteq \mathcal{P}(I)$ is a **filter** on the set $I$ if

- $\emptyset \notin \mathcal{U}$ and $I \in \mathcal{U}$;
- if $A \subseteq B \subseteq I$ and $A \in \mathcal{U}$, then $B \in \mathcal{U}$;
- $A, B \in \mathcal{U} \Rightarrow A \cap B \in \mathcal{U}$.

If $A \in \mathcal{U}$ or $I \setminus A \in \mathcal{U}$ for all $A$, then $\mathcal{U}$ is called an **ultrafilter**.

$\mathcal{U}$ is **non-principal** if it contains no finite subset of $I$.

## Fact

1. *Every filter is contained in an ultrafilter. In particular, there are non-prinicpal ultrafilters on every infinite set $I$.*
2. $\mathcal{U} \mapsto \mu_{\mathcal{U}} : \mathcal{P}(I) \to \{0, 1\}$, $\mu_{\mathcal{U}}(A) = 1$ *iff* $A \in \mathcal{U}$
   *(a finitely additive probability measure)*

# Preliminaries: ultraproducts

Given: $\mathcal{U}$ an ultrafilter on $I$, $\mathcal{M}_i = \langle M_i, \ldots \rangle_{i \in I}$ $\mathcal{L}$-structures.

- On $M := \prod_{i \in I} M_i$, define $(x_i) \sim (y_i) :\Leftrightarrow x_i = y_i$ for a.a. $i \in I$ (i.e. $\{i \in I \mid x_i = y_i\} \in \mathcal{U}$).
- On $M^* = M/\!\sim$ define an $\mathcal{L}$-structure $\mathcal{M}^*$ as follows:
  $c^{\mathcal{M}^*} := (c^{\mathcal{M}_i})/\!\sim$
  $R^{\mathcal{M}^*}(a^1/\!\sim, \ldots, a^n/\!\sim) :\Leftrightarrow R^{\mathcal{M}_i}(a_i^1, \ldots, a_i^n)$ for a.a. $i \in I$
  (similar for functions using their graph)
- $\mathcal{M}^* = \prod_{\mathcal{U}} \mathcal{M}_i$ is the **ultraproduct** of the $\mathcal{M}_i$ (along $\mathcal{U}$).

## Theorem (Łoś's theorem)

*For $\varphi$ an $\mathcal{L}$-sentence, one has $\mathcal{M}^* \models \varphi \Leftrightarrow \mathcal{M}_i \models \varphi$ for a.a. $i \in I$.*

# Pseudofinite fields

Recall that a field $K$ is **pseudofinite** if

- $K$ is perfect;
- $\mathrm{Gal}(K) = \hat{\mathbb{Z}}$; and
- $K$ is PAC, i.e. every absolutely irreducible variety defined over $K$ has a $K$-rational point.

Let $\mathrm{Psf}$ ($\mathrm{Psf}_p$) be the theory of pseudofinite fields (of char. $p$).

Denote by $\mathrm{Abs}(K) \subseteq K$ the (relative) algebraic closure of the prime subfield of $K$ inside $K$.

## Fact (Ax)

*For $K, L \models \mathrm{Psf}$, the following are equivalent:*

- $K \equiv L$;
- $\mathrm{Abs}(K) \cong \mathrm{Abs}(L)$.

# The Lang-Weil estimates

## Theorem (Lang-Weil)

*For $m, n, e \in \mathbb{N}$ there is a constant $C(m, n, e)$ such that*

- *for every finite field $\mathbb{F}_q$ and*
- *polynomials $f_1(\overline{x}), \ldots, f_m(\overline{x}) \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree $\leq e$,*

*if the the variety $V$ defined by $(f_1, \ldots, f_m)$ is absolutely irreducible of dimension $d$, then*

$$|\operatorname{card}(V(\mathbb{F}_q)) - q^d| \leq Cq^{d-\frac{1}{2}}.$$

*In particular, $V(\mathbb{F}_q) \neq \emptyset$ for $q >> 0$.*

# Ax's results on finite and pseudofinite fields

Let $P$ be the set of prime numbers, $Q$ the set of prime powers.
Let $T_{ff}$ be the common theory of all finite fields.

## Theorem (Ax 1968)

1. *Every infinite model of $T_{ff}$ is pseudofinite. In particular, if $\mathcal{U}$ is a non-principal ultrafilter on $Q$, then $\prod_{\mathcal{U}} \mathbb{F}_q \models \mathrm{Psf}$.*
2. *Conversely, if $K \models \mathrm{Psf}$, there is $\mathcal{U}$ such that $K \equiv \prod_{\mathcal{U}} \mathbb{F}_q$. If $\mathrm{char}(K) = 0$, then even $\prod_{\mathcal{U}'} \mathbb{F}_p \equiv K$ for some $\mathcal{U}'$ on $P$.*

## Corollary

- $\mathrm{Psf} = T_{ff} +$ *'there are infinitely many elements'* $= \{\varphi \mid \mathbb{F}_q \models \varphi \ \forall q >> 0\}$
- $\mathrm{Psf}_0 = \{\varphi \mid \mathbb{F}_p \models \varphi \ \forall p >> 0\}$.
- *$T_{ff}$ is decidable.*

# Proof of Ax's results

Let $L = \prod_{\mathcal{U}} \mathbb{F}_q$.

- Elementary: $L$ is perfect and $\mathrm{Gal}(L) \cong \hat{\mathbb{Z}}$.
- Being PAC is expressed by a scheme of axioms $\{\psi\}_{\psi \in A}$. By the **L-W estimates**, the set $S_\psi = \{q \in Q \mid \mathbb{F}_q \models \psi\}$ is cofinite in $Q$ for every $\psi \in A$, so $S_\psi \in \mathcal{U}$. This shows $L$ is PAC.

Conversely, given $K \models \mathrm{Psf}$, we have to find $\mathcal{U}$ such that $L = \prod_{\mathcal{U}} \mathbb{F}_q \equiv K$, or equivalently $\mathrm{Abs}(K) \cong \mathrm{Abs}(L)$.

- If $\mathrm{char}(K) > 0$, this is elementary.
- If $\mathrm{char}(K) = 0$, using **Čebotarev's density theorem**, one may find $\mathcal{U}'$ on $P$ such that $\mathrm{Abs}(K) \cong \mathrm{Abs}(\prod_{\mathcal{U}'} \mathbb{F}_p)$.

# The non-standard Frobenius

For $q = p^n$ denote by $\varphi_q$ the Frobenius automorphism $x \mapsto x^q$.
The difference field $K_q = (\mathbb{F}_p^{alg}, \varphi_q)$ is called a **Frobenius field**.
Note that $(k, \varphi_q) \equiv K_q$ for all $k \models ACF_p$.

## Conjecture

*For any non-principal ultrafilter $\mathcal{U}$ on Q one has $\prod_{\mathcal{U}} K_q \models ACFA$, i.e. the non-standard Frobenius automorphism is generic.*

- The conjecture arose from work of van den Dries, Macintyre and Wood on *ACFA* (around 1990).
  Hope: results on finite fields may be lifted to Frobenius fields.
- Hrushovski (1996) proved the conjecture, by establishing a twisted version of the L-W estimates.
- Independently, Macintyre (1997) announced the result.

# Twisted Lang-Weil estimates

For $q = p^n$ denote by $\Phi_q \subseteq \mathbb{A}^{2m}$ the graph of $\varphi_q$.

## Main Theorem (Hrushovski 1996)

*For every $d, \delta$ there exists $C(d, \delta) > 0$ such that for all*

- *$k \models ACF_p$;*
- *$V$ irred. subvariety of $\mathbb{A}^m$ $/k$ of dimension $d$;*
- *$S$ irred. subvariety of $V \times V^{\varphi_q}$ $/k$ such that both $\pi_1 : S \to V$ and $\pi_2 : S \to$ are dominant, one of them being quasi-finite,*

*then, if $q > C(d, \deg(V) + \deg(S))$, one has*

$$\mathrm{card}((V,S)^{\#}(k)) = \mathrm{card}[S(k) \cap \Phi_q(k)] = aq^d + e,$$

*where* $a = \frac{[k(S):k(V)]}{[k(S):k(V^{\varphi_q})]_{ins}}$ *and* $|e| \leq C(d, \deg(V) + \deg(S))q^{d-\frac{1}{2}}$.

# Twisted Lang-Weil estimates (continued)

## Remark

*In the statement, the degrees of $V$ and $S$ are taken with respect to some embeddings into projective space.*

Note the following consequence of the twisted Lang-Weil estimates:

## Corollary

*In the situation of the theorem, for $q >> 0$, one has*

$$S(k) \cap \Phi_q(k) \neq \emptyset.$$

Talks of Gabriel Giabicani and Yves Laszlo:
Presentation of the **proof architecture** of the Main Theorem.

# From twisted L-W to *ACFA*

Recall that $(K, \sigma)$ is a model of *ACFA* iff it satisfies

(1) $K \models ACF$,

(2) $\sigma \in \mathrm{Aut}(K)$, and

(3) for every (affine) irreducible variety $V$ /$K$ and every irreducible $S \subseteq V \times V^\sigma$ /$K$ such that both $\pi_1 : S \to V$ and $\pi_2 : S \to V^\sigma$ are dominant, there is a tuple $a$ in $K$ such that $(a, \sigma(a)) \in S$.

## Fact

*If $(K, \sigma)$ satisfies (1), (2) and every instance of (3) where in addition the projections $\pi_i$ are quasi-finite, then $(K, \sigma) \models ACFA$.*

# The non-standard Frobenius automorphism

## Fact

*If* $(K,\sigma),(K',\sigma') \models ACFA$, *then* $(K,\sigma) \equiv (K'\sigma')$ *if and only if* $(\mathrm{Abs}(K), \sigma\restriction_{\mathrm{Abs}(K)}) \cong (\mathrm{Abs}(K'), \sigma'\restriction_{\mathrm{Abs}(K')})$.

## Theorem (Hrushovski 1996)

1. *For* $\mathcal{U}$ *non-principal (on* $Q$*),* $\prod_{\mathcal{U}} K_q \models ACFA$ .
2. *If* $(K,\sigma) \models ACFA$, *there is* $\mathcal{U}$ *such that* $(K,\sigma) \equiv \prod_{\mathcal{U}} K_q$.
   *If* $\mathrm{char}(K) = 0$, *then even* $\prod_{\mathcal{U}'} K_p \equiv (K,\sigma)$ *for some* $\mathcal{U}'$ *on* $P$.

## Corollary

- $ACFA = \{\varphi \mid K_q \models \varphi \ \forall q >> 0\}$.
- $ACFA_0 = \{\varphi \mid K_p \models \varphi \ \forall p >> 0\}$.
- *The common theory of all difference fields* $K_q$ *is decidable.*

‘

# Proof of Hrushovski's results

Let $(L, \sigma) = \prod_{\mathcal{U}} K_q$.

- Elementary: $L \models ACF$ and $\sigma \in \mathrm{Aut}(L)$.
- Satisfying (3) restricted to instances with quasi-finite projections is expressed by a scheme of axioms $\{\psi\}_{\psi \in A}$.

  **Twisted L-W** $\Rightarrow$ the set $S_\psi = \{q \in Q \mid K_q \models \psi\}$ is cofinite in $Q$ for every $\psi \in A$, so $S_\psi \in \mathcal{U}$. Thus, $(L, \sigma) \models ACFA$.

Now, given $(K, \sigma) \models ACFA$, we want to find $(K', \sigma') = \prod_{\mathcal{U}} K_q$ such that $(\mathrm{Abs}(K), \sigma \restriction_{\mathrm{Abs}(K)}) \cong (\mathrm{Abs}(K'), \sigma \restriction_{\mathrm{Abs}(K')})$ holds.

- If $\mathrm{char}(K) > 0$, this is elementary.
- If $\mathrm{char}(K) = 0$, this follows from **Čebotarev's density theorem**.

# Conclusion

Hrushovski's results on the Frobenius automorphism **widely generalise** the results on **finite and pseudo-finite fields** presented in the first part:

- **Twisted L-W $\Rightarrow$ non-twisted L-W**

  Suppose $V/\mathbb{F}_q$ is absolutely irreducible, so $V^{\varphi_q} = V$.

  Let $\Delta \subseteq V \times V$ be the diagonal, $k := \mathbb{F}_q^{alg}$, $d = \dim(V)$.

  Twisted L-W $\Rightarrow$ $\mathrm{card}[\Delta(k) \cap \Phi_q(k)] = q^d + O(q^{d-\frac{1}{2}})$.

  $\Delta(k) \cap \Phi_q(k) \cong \{(a \in V(k) \mid a = \varphi_q(a)\} = V(\mathbb{F}_q)$,

- The results on the non-standard Frobenius specialise to Ax's results: if $(K, \sigma) \models ACFA$, then $Fix(\sigma) \models \mathrm{Psf}$.

# Jacobi's bound for difference equations

Let $\overline{x} = (x_1, \ldots, x_n)$ and $u_1(\overline{x}), \ldots, u_n(\overline{x}) \in K[\overline{x}]_\sigma$ .

$X =$ difference variety defined by $u_1(\overline{x}) = \ldots = u_n(\overline{x}) = 0$.

$h_k^i =$ **order** of $x_i$ in $u_k$ (with $h_k^i = -\infty$ if no $x_i^{\sigma^m}$ occurs in $u_k$).

**total dimension** of $X := \sup\{td(K(a)_\sigma/K) \mid a \in X(\mathbb{U})\}$.

## Theorem (Hrushovski)

*Let $W$ be a component of $X$ of finite total dimension $d$. Then*

$$d \leq \max_{\tau \in Sym(n)} \sum_{k=1}^{n} h_k^{\tau(k)}.$$

## Remark

*This is a difference analogue of Jacobi's conjecture (still open) which asserts the same bound in the differential algebraic case.*

# Jacobi's bound: proof idea

## Lemma (Strong version of Bezout )

*Let $U_1(\overline{x}), \ldots, U_n(\overline{x}) \in K[\overline{x}]$, and $H_k^i$ = degree of $x_i$ in $U_k$. Let $Z_0$ be the 0-dimensional part of the variety defined by the $U_i$. Then*

$$|Z_0| \leq \sum_{\tau \in Sym(n)} \prod_{k=1}^{n} H_k^{\tau(k)}.$$

Let $(D, \sigma) \subseteq (K, \sigma)$ be fin. generated with $u_k \in D[\overline{x}]_\sigma$ for all $k$, $\varphi : D \to K_q$ be a specialisation, $U_k := \varphi(u_k) \in K_q[\overline{x}]$.

There is $p(z) \in \mathbb{N}[z]$ of degree $h_k^i$ s.t. for $q >> 0$, $H_k^i = p(q)$, say $p(q) = mq^{h_k^i} +$ lower terms. $\Rightarrow \lim_{q\to\infty} \log_q H_k^i = h_k^i$.

Linearising, twisted L-W gives $|W(K_q)| = \alpha q^d + O(q^{d-\frac{1}{2}})$.

So $d = \lim_{q\to\infty} \log_q(w_q) \leq \lim_{q\to\infty} \log_q(\sum_\tau \prod_{k=1}^n H_k^{\tau(k)}) = \max_\tau \sum_{k=1}^n h_k^{\tau(k)}$ .

□

Apart from the family of alternating groups $(A_n)_{n\geq 5}$ the infinite families of finite simple groups are

1. either of the form $\{G(\mathbb{F}_q)\}_q$, where $G$ is some (fixed) algebraic group;
2. or twisted variants of these (Ree, Suzuki), whose definition involves an algebraic group and a field automorphism.

In the **algebraic case**, for $\mathcal{U}$ non-principal one gets $\prod_{\mathcal{U}} G(\mathbb{F}_q) = G(F)$, where $F = \prod_{\mathcal{U}} \mathbb{F}_q \models \mathrm{Psf}$.

The members of the **twisted** families get uniformly definable in the language of difference rings, and are given by $H(K_q)$, for $H$ a quantifier free definable set of finite total dimension in *ACFA*.

One gets $\prod_{\mathcal{U}} H(K_q) = H(K)$, for $K = \prod_{\mathcal{U}} K_q \models \mathit{ACFA}$.

# Uniformity results for finite simple groups

Using results of Hrushovski-Pillay on definable groups of finite total dimension in *ACFA*, one obtains for example:

## Theorem (Hrushovski)

*For any of the above families (algebraic or twisted algebraic), there is $N \in \mathbb{N}$ such that for any finite simple group $G$ from the family, any non-trivial conjugacy class $C \subseteq G$ generates $G$ in at most $N$ steps.*

# An application to endomorphisms of groups of finite rank

## Theorem

*Let $G$ be a definable group (e.g. a $\sigma$-algebraic group) of finite total dimension in ACFA, and let $f \in \mathrm{End}(E)$ be definable. Then*

$$\mathrm{card}(\ker(f)) = (G : \mathrm{im}(f)).$$

## Proof.

For $q >> 0$, $G$ gives rise to a finite definable group in $K_q$, where the result is clear. Pass to the limit. □

Let $(\mathbb{Q}^{alg}, \mathrm{id}) \subseteq (K, \sigma) \models ACFA$. By Zoé's talks, the equation $\sigma(x) = x^2$ defines a locally modular subgroup $G$ of $\mathbb{G}_m$ of rank 1.

- $G$ is **torsion free** (by the assumption on $\sigma$)
- $G$ is **divisible** (by the theorem)
- $G$ is **strongly minimal** (since no subgroups of finite index)

# Zariski density of periodic points

## Theorem (Fakhruddin 2003)

*Let $X$ be a projective variety over an algebraically closed field $k$, $\varphi = X \to X$ be a dominant morphism and $L$ a line bundle on $X$ such that $\varphi^* L \otimes L^{-1}$ is ample. Then the set of periodic points $\{a \in X(k) \mid \varphi(a) = a\}$ is Zariski dense in $X$.*

Fakhruddin deduces this theorem from the following consequence of the Main Theorem (twisted Lang-Weil estimates).

## Proposition (Poonen)

*Let $X$ be an algebraic variety over $\mathbb{F}_p^{alg}$ and $\varphi : X \to X$ a finite and surjective morphism. Then the set of periodic points $\{a \in X(\mathbb{F}_p^{alg}) \mid \varphi(a) = a\}$ is Zariski dense in $X$.*

# Existence of non-preperiodic algebraic points

Somewhat dually, Amerik used twisted Lang-Weil to obtain the following.

## Theorem (Amerik 2011)

*Let $X$ be an algebraic variety defined over $\mathbb{Q}^{alg}$, and let $f : X \cdots > X$ be a rational dominant self-map, $f$ defined over $\mathbb{Q}^{alg}$. Assume $f$ is not of finite order. Then there is $a \in X(\mathbb{Q}^{alg})$ such that $a$ is not pre-periodic.*