Pseudofinite dimension and measure in pseudofinite fields

Martin Bays

19.05.2021

Contents

1 Preliminaries

1.1 Notation

- $\mathcal{L} := \{+, \cdot\}$.
- $x, y, z, a, b, c, \dots$ denote tuples.
- $|x|$ denotes the length of the tuple x.
- $M^x := M^{|x|}$.

1.2 Pseudofinite cardinality

Definition 1.1. If $\mathcal{U}$ is an ultrafilter on a set I and $(X_i)_{i \in I}$ are finite sets, we define the **pseudofinite cardinality** of the ultraproduct by

$$\left| \prod_{i \to \mathcal{U}} X_i \right| := \lim_{i \to \mathcal{U}} |X_i| \in \mathbb{N}^{\mathcal{U}}.$$

In particular, if $\mathcal{M}_i$ are finite $\mathcal{L}$-structures and $\phi(x,y)$ is an $\mathcal{L}$-formula, and $b_i \in (\mathcal{M}_i)^y$, then

$$\left| \phi(\prod_{i \to \mathcal{U}} \mathcal{M}_i, \lim_{i \to \mathcal{U}} b_i) \right| = \lim_{i \to \mathcal{U}} |\phi(\mathcal{M}_i, b_i)|.$$

2 Chatzidakis - van den Dries - Macintyre

2.1 Finitary version

Theorem 2.1 (Chatzidakis - van den Dries - Macintyre)**.** *Let $\phi(x,y)$ be an $\mathcal{L}$-formula. Then there are*

- $C \in \mathbb{R}_{>0}$,
- $G \subseteq_{\text{fin}} (\{0, \dots, |x|\} \times \mathbb{Q}_{>0}) \cup \{(0,0)\}$, *and*
- *$\mathcal{L}$-formulas* $(\theta_{\phi,d,m}(y))_{(d,m) \in G}$,

such that for any finite field $\mathbb{F}_q$,

- $\mathbb{F}_q \models \forall y.\ \bigvee_{(d,m) \in G} \theta_{\phi,d,m}(y)$
- *for each* $(d,m) \in G$, *for* $b \in (\mathbb{F}_q)^y$,

$$\mathbb{F}_q \models \theta_{\phi,d,m}(b) \Leftrightarrow \left| |\phi(\mathbb{F}_q, b)| - mq^d \right| \leq Cq^{d - \frac{1}{2}}$$

2.2 Asymptotic version

To prove Theorem 2.1, it suffices to prove it with "for any finite field" replaced by "for all sufficiently large finite fields". Indeed, we can then increase C and modify the $\theta_{\phi,d,m}$ to handle the finitely many remaining finite fields.

Explicitly: to deal with fields of size $\leq q_0$, *set*

- $C' := \max(C, q_0^{|x| + \frac{1}{2}} + 1)$, *so* $|\phi(\mathbb{F}_{q_0}, b)| \leq q_0^{|x|} \leq C' q_0^{-\frac{1}{2}}$;
- $\theta'_{\phi,0,0}(y) := \theta_{\phi,0,0}(y) \vee \exists^{\leq q_0} x.\ x = x$;
- $\theta'_{\phi,d,m}(y) := \exists^{> q_0} x.\ x = x \wedge \theta_{\phi,d,m}(y)$ *for* $(d,m) \neq (0,0)$.

2.3 Pseudofinite version

By Łoś, this asymptotic statement is equivalent to the following, which we will prove using the model theory of pseudofinite fields.

Theorem 2.2 (CDM, pseudofinite version)**.** *Let $\phi(x,y)$ be an $\mathcal{L}$-formula.*

Then there are

- $C \in \mathbb{R}$,
- $G \subseteq_{\text{fin}} (\{0, \dots, |x|\} \times \mathbb{Q}_{>0}) \cup \{(0,0)\}$, *and*
- *$\mathcal{L}$-formulas* $(\theta_{\phi,d,m}(y))_{(d,m) \in G}$,

such that for any infinite ultraproduct of finite fields F,

- $F \models \forall y.\ \bigvee_{(d,m) \in G} \theta_{\phi,d,m}(y)$
- *for each* $(d,m) \in G$, *for* $b \in F^y$,

$$F \models \theta_{\phi,d,m}(b) \ \Leftrightarrow \ \left| |\phi(F,b)| - m|F|^d \right| \leq C|F|^{d - \frac{1}{2}}$$

Remark. Given $b \in F^y$, we can recover the corresponding d, m from $N := |\phi(F,b)|$ as

$$d = \operatorname{st}(\log_{|F|}(N));\ m = \operatorname{st}\left(\frac{N}{|F|^d} \right).$$

Hence the $\theta_{\phi,d,m}(y)$ are pairwise inconsistent, so form a partition.

Remark. In fact $d = \dim(\phi(F,b)^{\mathrm{Zar}})$. We will see that this falls out of the proof.

Remark. $|\phi(F,b)| < (m+1)|F|^d$ since $|F|^{\frac{1}{2}} > \mathbb{R} \ni C$.

Remark. Let $F \models \mathrm{Psf}$ and $b \in F^y$.

If F is not an ultraproduct of finite fields, then $|F|$ and $|\phi(F,b)|$ are undefined.

But F is elementarily equivalent to an ultraproduct of finite fields,
so $b \models \theta_{\phi,d,m}(y)$ for some unique $(d,m) \in G$,
so this assigns a well-defined dimension and measure to $\phi(F,b)$.

2.4 "Local" version

Since an ultraproduct of ultraproducts of finite fields is an ultraproduct of finite fields, Theorem 2.2 is in turn equivalent to:

Theorem 2.3 (CDM, local version)**.** *Let $\phi(x,y)$ be an $\mathcal{L}$-formula.*

Let F be an infinite ultraproduct of finite fields, and let $b \in F$. Then there are

- $(C,d,m) \in \mathbb{R} \times (\{0, \dots, |x|\} \times \mathbb{Q}_{>0} \cup \{(0,0)\})$ *and*
- *an $\mathcal{L}$-formula* $\theta(y) \ni \operatorname{tp}^F(b)$ *such that:*

for any infinite ultraproduct of finite fields F' and any $b' \in F'$, (*)

$$F' \models \theta(b') \ \Rightarrow \ \left| |\phi(F',b')| - m|F'|^d \right| \leq C|F'|^{d - \frac{1}{2}}$$

Sketch proof of Theorem 2.2 from Theorem 2.3.

- Let $\Xi \subseteq \mathbb{N} \times \{0, \dots, |x|\} \times \mathbb{Q}_{>0} \cup \{(0,0)\} \times \mathcal{L}$ be the set of 4-tuples (C,d,m,θ) satisfying (*).
- Theorem 2.2 asserts that for some finite subset of Ξ, the corresponding θ cover any F. (We use here the disjointness of the θ for distinct pairs (d,m).)
- If not, taking an ultraproduct over finite subsets of Ξ of counterexamples $b \in F$, we obtain $b^* \in F^*$ for which $F^* \models \neg\theta(b^*)$ for any $(C,d,m,\theta) \in \Xi$, contradicting Theorem 2.3.

$\square$

3 Proof

We prove Theorem 2.3. So let $\phi(x,y)$ be an $\mathcal{L}$-formula.

Let F be an infinite ultraproduct of finite fields, and let $b \in F^y$.

We consider a series of increasingly complicated cases for the definable set $\phi(F,b)$, and in each case we find C, d, m, θ as required.

3.1 Case 1: $\phi(F,b) = V(F)$, V absolutely irreducible.

Fact 3.1. *Let $\overline{f}(x,y) = (f_i(x,y))_{i<m}$ be polynomials over $\mathbb{Z}$, and let $d \in \mathbb{N}$. Then there is a quantifier-free ring formula $A_{\overline{f},d}(y)$ such that for any field F and $b \in F^y$,*

$$F \models A_{\overline{f},d}(b) \ \Leftrightarrow \ \mathcal{V}(\overline{f}(x,b))) \text{ is absolutely irreducible of dimension } d.$$

Fact 3.2 (Lang-Weil)**.** *There is a function $C_{LW} : \mathbb{N}^2 \to \mathbb{R}$ such that if $\mathbb{F}_q$ is a finite field and W is an absolutely irreducible variety defined by polynomials in $\mathbb{F}_q[X_1, \dots, X_n]_{\leq D}$,*

$$\left| |W(\mathbb{F}_q)| - q^{\dim(W)} \right| \leq C_{LW}(n,D) q^{\dim(W) - \frac{1}{2}}.$$

We deduce:

Lemma 3.3. *If $F = \prod_{i \to \mathcal{U}} \mathbb{F}_{q_i}$ is an infinite ultraproduct of finite fields and W is an absolutely irreducible variety defined by polynomials in $F[X_1, \dots, X_n]_{\leq D}$,*

$$\left| |W(F)| - |F|^{\dim(W)} \right| \leq C_{LW}(n,D) |F|^{\dim(W) - \frac{1}{2}}.$$

Proof.

- Say $W = \mathcal{V}(\overline{f}(x,c))$ where $f_i \in \mathbb{Z}(x,y)$ and $c = \lim_{i \to \mathcal{U}} c_i \in F^y$.
- Let $d := \dim W$.
- By Łoś, the following holds for $\mathcal{U}$-many i:
  - $\mathbb{F}_{q_i} \models A_{\overline{f},d}(c_i)$; hence
  - $W_i := \mathcal{V}(\overline{f}(x,c_i))$ is absolutely irreducible of dimension d; hence
  - $\left| |W_i(\mathbb{F}_{q_i})| - q_i^{\dim(W)} \right| \leq C_{LW}(n,D) q_i^{\dim(W) - \frac{1}{2}}$.
- We conclude since $|W(F)| = \lim_{i \to \mathcal{U}} |W_i(\mathbb{F}_{q_i})|$ and $|F| = \lim_{i \to \mathcal{U}} q_i$.

$\square$

Now suppose $\phi(F,b) = V(F)$ for an absolutely irreducible variety $V = \mathcal{V}(\overline{f}(x,c))$ where $f_i(x,y)$ has degree $\leq D$ in x and $c \in F^y$.

Then we can take:

- $C := C_{LW}(|x|, D)$,
- $d := \dim(V)$,
- $m := 1$,
- $\theta(y) := \exists z.\ (A_{\overline{f},d}(z) \wedge \forall x.\ (\phi(x,y) \leftrightarrow x \in \mathcal{V}(\overline{f}(x,z))))$.

3.2 Case 2: $\phi(F,b) = V(F)$

- Suppose $\phi(F,b) = V(F)$ where V is a Zariski-closed set.
- Replacing V with the Zariski closure of $V(F)$, we may assume that $V(F)$ is Zariski dense in V.
- V has an irreducible decomposition $V = \bigcup_{i<n} V_i$ where V_i is an absolutely irreducible variety, and $V_i \not\subseteq V_j$ for $i \neq j$.
- We show that our estimate on $|V(F)|$ holds with

$$d := \dim V = \max_i \dim(V_i)$$
$$m := |\{i : \dim(V_i) = d\}|.$$

- Since $V(F) = \bigcup_i V_i(F)$ is Zariski-dense in V, also $V_i(F)$ is Zariski-dense in V_i for all i.
- So each V_i is F-invariant, and F is perfect, so each V_i is defined over F.
- Any intersection of two or more of the V_i has dimension $< d$.
- By inclusion-exclusion,

$$|\phi(F,b)| = \left| \bigcup_i V_i(F) \right| = \sum_{\emptyset \neq I \subseteq n} (-1)^{|I|-1} \left| \left(\bigcap_{i \in I} V_i \right)(F) \right| = \sum_i |V_i(F)| + \dots$$

- Applying Case 1 to the V_i, and inductively applying the present case to the lower dimensional intersections, we conclude:

$$\left| \phi(F,b) - m|F|^d \right| \leq \sum_{i<m} C_i |F|^{d - \frac{1}{2}} + C'|F|^{d-1} \leq C|F|^{d - \frac{1}{2}},$$

  where $C' \in \mathbb{R}$ is large enough to bound the terms in the inclusion-exclusion formula arising from the finitely many lower dimensional V_i and the intersections of two or more V_i, and setting $C := \sum_{i<m} C_i + 1$ (and using $|F|^{\frac{1}{2}} > \mathbb{R} \ni C'$).

- Set

$$\begin{aligned} \theta(y) := \exists y_0, \dots, y_{n-1}.\ ((\forall x.\ \phi(x,y) \leftrightarrow \bigvee_{i<n} \psi_i(x,y_i)) \\ \wedge \bigwedge_i \theta_i(y_i) \\ \wedge \bigwedge_{I \subseteq n, |I| \geq 2} \theta_I((y_i)_{i \in I})), \end{aligned}$$

  where
  - $V_i(F) = \psi_i(F, b_i)$,
  - θ_i are as in Case 1 for ψ_i,
  - θ_I are obtained by inductive application of the present case to $\bigwedge_{i \in I} \psi_i(x, y_i)$.
- Note that we do have $d = \dim(\phi(F,b)^{\mathrm{Zar}})$ in this case.

3.3 Case 3: $\phi(F,b) = X(F)$, X constructible

(*Constructible* means: boolean combination of Zariski-closed.)

- Intersecting with $X(F)^{\mathrm{Zar}}$, we can assume $X(F)$ is Zariski-dense in X.
- We can write X as a disjoint union $X = \dot{\bigcup}_i V_i \setminus W_i$ where V_i is absolutely irreducible and $W_i \subsetneq V_i$ is a proper closed subset.
- Set $d := \max_i \dim(V_i) = \dim(X(F)^{\mathrm{Zar}})$ and $m := |\{i : \dim(V_i) = d\}|$.
- $$|X(F)| = \sum_i (|V_i(F)| - |W_i(F)|),$$

  so the estimate follows by applying Case 2 to each V_i and W_i,
  using $\dim(W_i) < d$ and the Zariski density of $V_i(F)$ in V_i.

  (Note: we could alternatively use the Rabinovich trick here.)

  (Alternative alternative (thanks to Martin Hils for suggesting this): note that $X^{\mathrm{Zar}} \setminus X$ is constructible of lower dimension; use this case inductively to handle it, and Case 2 for X^{Zar} (in which F-points are Zariski-dense).)

- θ expresses that this decomposition and the estimates for the various terms hold.

3.4 Case 4: $\phi(F,b) = X(F)$ arbitrary

- Recall: there exists a Zariski-closed set V over F and a co-ordinate projection π such that $\pi_F := \pi|_{V(F)} : V(F) \twoheadrightarrow X(F)$ is surjective with boundedly finite fibres.
- So we have a definable partition $X(F) = \dot{\bigcup}_{1 \leq n \leq M} X_n(F)$ where

$$X_n(F) := \{a \in X(F) : |\pi_F^{-1}(a)| = n\}.$$

- We may assume that $V(F)$ is Zariski-dense in V.
- Consider the constructible sets

$$W_k := \{(x_1, \dots, x_k) : x_i \in V,\ \pi(x_i) = \pi(x_j),\ x_i \neq x_j\ (\forall i \neq j)\} \subseteq V^k,$$

  and maps

$$\pi_{k,F} : W_k(F) \to X(F);\ (x_1, \dots, x_k) \mapsto \pi(x_1).$$

- For $a \in X_n(F)$ and $1 \leq n, k \leq M$,

$$|\pi_{k,F}^{-1}(a)| = P_{kn} = \begin{cases} \frac{n!}{(n-k)!} & (k \leq n) \\ 0 & (k > n) \end{cases}.$$

- Now the matrix P is lower triangular, and non-zero on the diagonal, so P has an inverse $P^{-1} \in \mathrm{GL}_M(\mathbb{Q})$.

$$|W_k(F)| = \sum_{1 \leq n \leq M} P_{kn} |X_n(F)|,$$

  hence

$$|X_n(F)| = \sum_{1 \leq k \leq M} (P^{-1})_{nk} |W_k(F)|.$$

- Now

$$|X(F)| = \sum_{1 \leq n \leq M} |X_n(F)|.$$

  By Case 3 we can estimate $|W_k(F)|$ with (d_k, m_k) say,
  so we obtain our estimate for $|X(F)|$ with

$$d := \max_i d_i$$
$$m := \sum_{\{(n,k)\,:\,d_k = d\}} (P^{-1})_{nk} m_k \in \mathbb{Q}.$$

- $\theta(y)$ expresses that $\phi(F,y)$ is a projection of $V^y(F)$ with fibres bounded by M, and the estimate works for the corresponding $|W_k^y(F)|$ (which we can express by Case 3).
- To see $d = \dim(X(F)^{\mathrm{Zar}})$:
  - Recall $V = V(F)^{\mathrm{Zar}}$.
  - From the way V was obtained, $\pi : V \to X(F)^{\mathrm{Zar}}$ has finite fibres on $X(F)$, so also each $\pi_k : W_k \to X(F)^{\mathrm{Zar}}$ has generically finite fibres.
  - Then $d_1 = \dim(V) = \dim(X(F)^{\mathrm{Zar}})$ and $d_k \leq \dim(W_k) \leq \dim(X(F)^{\mathrm{Zar}})$.
  - So $d = \dim(X(F)^{\mathrm{Zar}})$.