The measure of Chatzidakis-van den Dries-Macintyre

Seminar on pseudofinite structures

12.05.2021

Motivation

Motivation:

- Uniformity results for finite fields $\mathbb{F}_q$

L e.g. Is there a formula $\varphi(x)$ in $\mathcal{L}_{Ring}$ that defines $\mathbb{F}_{q^2}$ in $\mathbb{F}_q$ for all q?
(Felgner)

- What can we recover from the counting measure on finite fields?

Let F be pseudofinite, then F elt. embeds in an UP of finite fields, i.e.

$$F \models PF \Rightarrow F \preceq \prod_{i \in I} \mathbb{F}_{q_i} / \mathcal{U}$$

Proof:
Since F is pseudofinite it is elt. equiv. to an ultraproduct of finite fields. Now we can find (e.g. using the Keisler-Shelah theorem) an ultrapower of F isomorphic to an ultrapower of the ultraproduct of finite fields which is again an ultraproduct of finite fields.

Lang-Weil bounds

Theorem (Lang-Weil)

For every positive integers n, d, there is positive constant $C(n, d)$ such that for every finite field $\mathbb{F}_q$ and variety V defined by polynomials in $\mathbb{F}_q[X_1, \dots, X_n]_{\leq d}$

$$\left| |V(\mathbb{F}_q)| - q^{\dim(V)} \right| \leq C q^{\dim(V) - 1/2}$$

Goal: Extend this to definable sets

Main theorem

Theorem

Let $\varphi(x, y)$ be a formula and x, y tuples of variables. Then there is a finite set $D \subset \{0, 1, \ldots, n\} \times \mathbb{Q}^{>0} \cup \{(0,0)\}$ of pairs (d, μ), a constant $C > 0$, and formulas $\varphi_{d,\mu}(y)$ for $(d, \mu) \in D$ such that:
If $\mathbb{F}_q$ is a finite field and a an m -tuple in $\mathbb{F}_q$, then there is some $(d, \mu) \in D$ such that

$$\left| |\varphi(\mathbb{F}_q, a)| - \mu q^d \right| < C q^{d-1/2} \quad (*)$$

The formula $\varphi_{d,\mu}(y)$ defines in each $\mathbb{F}_q$ the set of tuples a such that $(*)$ holds.

- Here $\varphi(\mathbb{F}_q, a) := \{ b \in \mathbb{F}_q^n \mid \mathbb{F}_q \models \varphi(b, a) \}$
- We add $(0,0)$ for the case of $\varphi(x, a)$ defining an empty set.

Main theorem

Theorem

Let $\varphi(x, y)$ be a formula and x, y tuples of variables. Then there is a finite set $D \subset \{0, 1, \dots, n\} \times \mathbb{Q}^{>0} \cup \{(0, 0)\}$ of pairs (d, μ), a constant $C > 0$, and formulas $\varphi_{d,\mu}(y)$ for $(d, \mu) \in D$ such that:
If $\mathbb{F}_q$ is a finite field and a an m -tuple in $\mathbb{F}_q$, then there is some $(d, \mu) \in D$ such that

$$\left| |\varphi(\mathbb{F}_q, a)| - \mu q^d \right| < C q^{d-1/2} \quad (*)$$

The formula $\varphi_{d,\mu}(y)$ defines in each $\mathbb{F}_q$ the set of tuples a such that $(*)$ holds.

Observations:

- If $\varphi(x,a)$ defines a variety V, this reduces to Lang-Weil
- If $\varphi(x,a)$ defines an algebraic set W, with all irreducible components $V_1, \dots, V_n$ defined over $\mathbb{F}_q$, then $d = \max_{1 \le i \le n} \dim(V_i)$ and μ the number of the components of maximal dimension.

Main theorem

Theorem

Let $\varphi(x, y)$ be a formula and x, y tuples of variables. Then there is a finite set $D \subset \{0, 1, \ldots, n\} \times \mathbb{Q}^{>0} \cup \{(0, 0)\}$ of pairs (d, μ), a constant $C > 0$, and formulas $\varphi_{d,\mu}(y)$ for $(d, \mu) \in D$ such that:
If $\mathbb{F}_q$ is a finite field and a an m -tuple in $\mathbb{F}_q$, then there is some $(d, \mu) \in D$ such that

$$\left| |\varphi(\mathbb{F}_q, a)| - \mu q^d \right| < C q^{d-1/2} \quad (*)$$

The formula $\varphi_{d,\mu}(y)$ defines in each $\mathbb{F}_q$ the set of tuples a such that $(*)$ holds.

We have to allow for rational values and more then one pair:

Example : Consider $\varphi(x) \equiv \exists Y \; Y^2 = X$, then

- if $char(q) = 2$ we have $|\varphi(\mathbb{F}_q)| = q$ $\rightsquigarrow$ $\mu_1 = 1$
- if $char(q) \neq 2$ we have $|\varphi(\mathbb{F}_q)| = \frac{1}{2}(q+1)$ $\rightsquigarrow$ $\mu_2 = \frac{1}{2}$

Some consequences

1. If q is sufficiently large, the formulas $\varphi_{d,\mu}(y)$ will define a partition of the parameter set $\mathbb{F}_a^m$.

If $(d_1,\mu_1) \neq (d_2,\mu_2)$ then For $d_1 \neq d_2$ this is obvious.
For $\mu_1 \neq \mu_2$ choose $q >> 0$ such that $|\mu_1 - \mu_2| q^d > C q^{d-1/2}$

2. If $\phi(x,y)$ with $|x| = 1$, then there are positive numbers $A \in \mathbb{N}$ and $r \in \mathbb{Q}$ such that for every $\mathbb{F}_q$ and tuple a in $\mathbb{F}_q$

$$\text{either } |\varphi(\mathbb{F}_q, a)| < A \text{ or } |\varphi(\mathbb{F}_q, a)| \geq rq$$

Let D be the pairs associated to $\varphi(x,y)$.
Let $B = \sup\{\mu \mid (0,\mu) \in D\}$; $r_0 = \inf\{\mu \mid (1,\mu) \in D\}$ and then set
$r = r_0/2$ and $A = \sup\{A_0 + C, 4C^2/r_0^2\}$

3. If $q >> 0$ and $(0,\mu) \in D$ and $\mathbb{F}_q \models \varphi_{0,\mu}(a)$, then $q^{-1/2} \to 0$, thus $\mu = |\varphi(\mathbb{F}_q, a)|$

Some (non)-definability results for finite fields

Theorem

There is no formula ϕ in the language of rings which defines in each field $\mathbb{F}_{q^2}$ the subfield $\mathbb{F}_q$.

Proof:

Assume such a formula $\varphi(x)$ would exist.
By ② either $|\varphi(\mathbb{F}_{q^2})| < A$ or $|\varphi(\mathbb{F}_{q^2})| \geq rq$ for some $A > 0$, $r \in \mathbb{Q}_{>0}$
But $\mathbb{F}_q$ is of size $\sqrt{q^2}$ in $\mathbb{F}_{q^2}$. $\lightning$

Remark:

One can even prove:
The field $\mathbb{F}_q$ is not uniformly interpretable in $\mathbb{F}_{q^2}$.

Idea: Extend the main theorem to the context of definable equivalence relations and then use the argument from above.

Some (non)-definability results for finite fields

Theorem

There is no formula which defines in all fields $\mathbb{F}_q$ the set of generators of the multiplicative group $\mathbb{F}_q^\times$.

Proof:

We use "Euler's totient function" $\phi(n) := \#\{k \le n \mid k \text{ rel. prime to } n\}$ which has the properties:

- $\phi(p^n) = p^n - p^{n-1}$ for p prime
- $\phi(nm) = \phi(n)\phi(m)$ for n, m coprime (Chinese-remainder-theorem)

(*) • $p^n > 2 \Rightarrow \phi(p^n) \ge \sqrt{n}$

(**) • $\phi(n) = n \cdot \prod_{\substack{e \mid n \\ e \text{ prime}}} (1 - \frac{1}{e})$ ("Euler's product formula")

From (*) it already follows that $\forall c > 0 \; \#\{n \mid \phi(n) < c\} < \infty$ whence it remains to show that we can find arbitrarily small values of $\phi(n)/n$.

Some (non)-definability results for finite fields

Theorem

There is no formula which defines in all fields $\mathbb{F}_q$ the set of generators of the multiplicative group $\mathbb{F}_q^\times$.

Fix some prime p and distinct primes $\ell_1, \dots, \ell_m$ and define $M = \prod_{i=1}^{m} (\ell_i - 1)$ then $p^M \equiv 1 \bmod \ell_i$ for all $1 \le i \le m$

$$(*) \Rightarrow \quad \frac{\phi(p^M - 1)}{p^M - 1} \le \prod_{i=1}^{m} \left(1 - \frac{1}{\ell_i}\right)$$

see for example Euler's proof of the existence of infinitely many primes.

Now since $\prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty$

and we can choose the $\ell_1, \dots, \ell_m$ arbitrarily we can find $\prod_{i=1}^{m} \left(1 - \frac{1}{\ell_i}\right)$ arbitrarily small. $\blacksquare$

Dimension and measure on pseudofinite fields

Let $\varphi(x,y)$ be a formula and D, $\varphi_{d,\mu}(y)$ given as in the main theorem. Using ① (partition) and the fact that a pseudofinite field F is elementarily embedded in an ultraproduct of finite fields we get that for any $a \in F$ there is a unique pair $(d,\mu) \in D$ such that $F \models \varphi_{d,\mu}(a)$.

We then define $\dim(\varphi(x,a)) = d$ (Dimension)

and $\mu(\varphi(x,a)) = \mu$ (Measure)

Additivity + Fubini

Let F be a pseudofinite field, S, T two definable sets.

1. Assume that $T \cap S = \emptyset$. Then

$$\mu(S \cup T) = \begin{cases} \mu(S) + \mu(T) & \text{if } \dim(S) = \dim(T) \\ \mu(S) & \text{if } \dim(S) > \dim(T) \\ \mu(T) & \text{if } \dim(S) < \dim(T) \end{cases}$$

2. Assume that $f : S \to T$ is a definable function, which is onto. If for all $y \in T$ $\dim\left(f^{-1}(y)\right) = d$ then $\dim(S) = \dim(T) + d$. If moreover for every $y \in T, \mu\left(f^{-1}(y)\right) = m$ then $\mu(S) = m\mu(T)$.

Proof Idea: We have $F \equiv \prod_{i \in I} \mathbb{F}_{q_i} / \mathcal{U}$. Now let S be given by $\varphi(x, a)$ in F. Write $a = [a_{q_i}]_{\mathcal{U}}$ and define $S_q := \varphi(x, a_q) \subseteq \mathbb{F}_q^n$

Łoś) For almost all q we have $\mathbb{F}_q \models \varphi_{d,\mu}(a_q)$.

Analogously define T_q.

Then it is enough to show that the equalities hold for almost all q and $T_q \cup S_q$ which follows using the main theorem.

For the Fubini statement proceed in the same manner.

Measure on definable sets

Theorem

Let S be a definable set. Define a function m_S on definable subsets of S as follows. Assume that $T \subset S$ is definable, and let $(d, \mu) = (\dim(S), \mu(S))$, $(e, \nu) = (\dim(T), \mu(T))$. Then

$$m_S(T) = \begin{cases} 0 & \text{if } e < d \\ \nu/\mu & \text{if } d = e \end{cases}$$

Then m_S is a finitely additive measure on the set of definable subsets of S.

Relation to algebraic dimension

Theorem

Let $\bar{S}$ be the Zariski closure of S in F^{alg}. Then $\dim(S) = \dim(\bar{S})$. Here the second dimension is the algebraic dimension of the algebraic set $\bar{S}$.

Proof sketch:

We want to reduce to the case of S being an algebraic set. If this algebraic set has definable irreducible components we have already seen this as a consequence of the main theorem. Otherwise it will be seen in the proof of the main theorem that we can always reduce to that case.

Now by the previous talks we have seen that we can find an F-algebraic set $W(F) \subseteq F^{n+m}$ such that $\pi(W(F)) = S$ for the projection $\pi: F^{n+m} \to F^n$ and such that the fibers $\pi^{-1}(y) \cap W(F)$ for $y \in S$ are finite and bounded by the same $k \in \mathbb{N}$.

Now using Fubini it follows that $\dim(S) = \dim(W(F))$ and by the above described case this coincides with the algebraic dimension of $W(F)$ which can be assumed to be equal to $\dim(W)$ (algebraic dimension) because we can assume that $W(F)$ is Zariski dense in W (using parts of the proof of the main theorem again). [Note: W denotes the respective set in F^{alg} defined by the corresponding equations of $W(F)$.]

Thus it remains to show that $\dim_{alg}(S) = \dim_{alg}(W)$.

But now $S = \pi(W(F))$ is Zariski dense in $\pi(W)$ and π is finite-to-one on a Zariski dense open subset of W, so $\dim_{alg}(S) = \dim_{alg}(W)$ follows.

Application on definable groups

Theorem

Let G, H be groups definable in the pseudo-finite field F, and assume that $f : G \to H$ is a definable morphism, $\mathrm{Ker}(f)$ *is finite, and* $\dim(G) = \dim(H) = d$. *Then*

$$\mu(G)[H : f(G)] = \mu(H)|\,\mathrm{Ker}(f)|.$$

Proof: Again use $F \preceq F^* = \prod_{i \in \mathbb{Z}} \mathbb{F}_{q_i}/\mathcal{U}$.

Let $a = [a_i]_{\mathcal{U}}$ be the parameter tuple for formulas defining H, G, their group law and the graph of f.

[Note that we can indeed express that f is a morphism of groups with kernel of fixed size $m \in \mathbb{N}$]

Now we consider the respective formulas using a_q and by Łoś we get for almost all q definable groups G_q, H_q over $\mathbb{F}_q$ and a morphism $f_q : G_q \to H_q$ with kernel of size $m \in \mathbb{N}$.

Application on definable groups

Theorem

Let G, H be groups definable in the pseudo-finite field F, and assume that $f : G \to H$ is a definable morphism, $\mathrm{Ker}(f)$ is finite, and $\dim(G) = \dim(H) = d$. Then

$$\mu(G)[H : f(G)] = \mu(H)|\mathrm{Ker}(f)|.$$

Since G_q and H_q are finite we directly get

$$|G_q|\,[H_q : f_q(G_q)] = |H_q|\,|\mathrm{Ker}(f_q)|.$$

Now we can deduce (by only considering large enough q) by dividing of q^d that $\mu(G_q)[H_q : f_q(G_q)] = \mu(H_q)\,|\mathrm{Ker}(f_q)|$

$\Rightarrow$ The theorem holds in F^* whence in F.

using that $\varphi_{d,\mu}(a_q)$ then holds for almost all q, where μ fullfills the above equation

Not the strict order property

Theorem

Let $\varphi(x, y)$ be a formula. There is a number M such that in any finite or pseudo-finite field F, the length of a chain of definable subsets of F^n defined by formulas $\varphi(x, a)$ for some tuples a in F, is bounded by M.

Proof:
Assume that does not hold, then by going over to a sufficiently saturated pseudofinite field F we can obtain a sequence $(a_i)_{i\in\mathbb{N}}$ of tuples in F, such that $S_i := \varphi(x, a_i) \subsetneq \varphi(x, a_j)$ $\forall i<j$
Now let Δ be the set of pairs associated to $\varphi(x,y)$ then we can assume that $\dim(S_i)=d$, $\mu(S_i)=\mu$ for all $i\in\mathbb{N}$ [by possibly going over to a subsequence]
Now we show by induction on the dimension d, that any such sequence already had to be finite:
For $d=0$ this follows from the fact that μ denotes the size of the set S_i and the sequence could only be of length one.
For $d>0$ we consider the sets $T_i = S_0 \setminus S_i$. Then the sets T_i form a strictly increasing sequence and we have $\dim(T_i)<d$ using the additivity of the measure and that $\mu(S_i)$ is constantly μ for all $i\in\mathbb{N}$.
Now this contradicts the induction hypothesis.

Not the strict order property

Theorem

Let $\varphi(x, y)$ be a formula. There is a number M such that in any finite or pseudo-finite field F, the length of a chain of definable subsets of F^n defined by formulas $\varphi(x, a)$ for some tuples a in F, is bounded by M.

Note that in the proof we only used the existence of measure & dimension and its properties.

Finite Shelah-rank

Theorem

Let $\varphi(x, y)$ be a formula. There is a number M such that in any finite field or pseudo-finite field F, if S is a definable set and $(a_i)_{i \in I}$ is a set of tuples such that each $\varphi(x, a_i)$ defines a subset of S of the same dimension d as S, and for $i \neq j$, $\dim(\varphi(x, a_i) \wedge \varphi(x, a_j)) < d$, then $|I| \leq M$.

Proof:

Let D be the set of pairs associated to the formula $\varphi(x,y)$ and let $\nu := \inf\{\mu \mid (d, \mu) \in D\}$.

Now if $\varphi(x, a_i)$ define subsets S_i of S such that $\dim(S_i) = d$ and $\dim(S_i \cap S_j) < d$ then we get $m_S(S_i) \geq \nu / \mu(S)$ and $m_S(S_i \cap S_j) = 0$.

Thus the length of I is bounded by $\mu(S)/\nu$. ∎

Finite Shelah-rank

Theorem

Let $\varphi(x, y)$ be a formula. There is a number M such that in any finite field or pseudo-finite field F, if S is a definable set and $(a_i)_{i \in I}$ is a set of tuples such that each $\varphi(x, a_i)$ defines a subset of S of the same dimension d as S, and for $i \neq j$, $\dim(\varphi(x, a_i) \wedge \varphi(x, a_j)) < d$, then $|I| \leq M$.

Note that it follows from the theorem that the S_1- rank is bounded by the dimension.

As a result we get that the pseudofinite fields are supersimple.

[Thus it would already follow from this theorem that the theory PF does not have the strict order property]

Finite Shelah-rank

Theorem

Let $\varphi(x, y)$ be a formula. There is a number M such that in any finite field or pseudo-finite field F, if S is a definable set and $(a_i)_{i \in I}$ is a set of tuples such that each $\varphi(x, a_i)$ defines a subset of S of the same dimension d as S, and for $i \neq j$, $\dim(\varphi(x, a_i) \wedge \varphi(x, a_j)) < d$, then $|I| \leq M$.

References:

- Z. Chatzidakis, L. van den Dries, A. Macintyre Definable sets over finite fields
  J. Reine Angew. Math. 427 (1992), 107–135
- Z. Chatzidakis, Notes on the model theory of finite fields
  Course Notes, 2005