Definable sets in pseudo-finite fields

I. Halupczok

Ecole Normale Superieure
rue d'Ulm, Paris

MODNET Training Workshop 2008
Model theory and Applications

Goal: general

- Let T be a theory.
  Natural question: classify 0-definable sets up to 0-definable bijection.
  Write $\mathrm{Def}(T)$ for 0-definable sets of T.
- Suppose ϕ_1, ϕ_2 are given.
  To prove $\phi_1 \overset{1:1}{\to} \phi_2$: write down the bijection.
  To prove $\phi_1 \overset{1:1}{\not\to} \phi_2$: use *invariants*:
  map $f\colon \mathrm{Def}(T) \longrightarrow \{\text{any set}\}$ s.t. $\phi \overset{1:1}{\to} \psi \Rightarrow f(\phi) = f(\psi)$

Goal: this talk

This talk:

- $\mathrm{Th}(\mathrm{PSF}_0) :=$ theory of pseudo-finite fields of characteristic 0
- Main goal: Find good invariants for $\mathrm{Th}(\mathrm{PSF}_0)$
- To start: work in fixed pseudo-finite field K
  Method: counting over finite fields
  - $\rightsquigarrow$ dimension, measure
  - $\rightsquigarrow$ even more
- Transfer results from $\mathrm{Th}(K)$ to $\mathrm{Th}(\mathrm{PSF}_0)$
- New method:
  $\rightsquigarrow$ results for $\mathrm{Th}(\mathrm{PSF}_0)$ which counting does not yield
  $\rightsquigarrow$ transfer counting results to theories where counting does not make sense

ACF-case

Start with easier example: $K \models \mathrm{Th}(\mathrm{ACF}_0) :=$ alg. closed fields of characteristic 0.

- Quantifier elimination $\Rightarrow$ any ϕ defines a "constructible" set.
- Well-defined invariants:
  - $\dim_{\mathrm{alg}} \overline{\phi(K)}$
  - #irreducible components of max. dim. of $\overline{\phi(K)}$

Can we get similar invariants if K is pseudo-finite (for arbitrary ϕ)?
(Is it true, for pseudo-finite K, that $K \overset{1:1}{\not\to} K^2$?)

Idea: counting

$\mathrm{Th}(\mathrm{PSF}_0)$ is not complete. Fix K pseudo-finite with $\mathrm{char}\, K = 0$ and work in $\mathrm{Th}(K)$.

- ϕ ring formula. $\rightsquigarrow$ can count $\#\phi(\mathbb{F}_q)$.
- This is not an invariant, but "for almost all q in ultra-filter sense":
  - $K \equiv \prod_{\mathcal{U}} \mathbb{F}_q$ for $\mathcal{U}$ ultrafilter on prime powers.
  - $K \models \chi \iff \{q \mid \mathbb{F}_q \models \chi\} \in \mathcal{U}$
  - So: $K \models \psi\colon \phi_1 \overset{1:1}{\to} \phi_2 \Rightarrow \{q \mid \#\phi_1(\mathbb{F}_q) = \#\phi_2(\mathbb{F}_q)\} \in \mathcal{U}$
- Formally: we have counting-invariant

$$cnt_K\colon \mathrm{Def}(\mathrm{Th}(K)) \longrightarrow \mathbb{N}^{\mathcal{U}}, \quad \phi \longmapsto (\#\phi(\mathbb{F}_q))_q$$

- Example: $\mathbb{A}^1 \overset{1:1}{\not\to} \mathbb{A}^2$ (always-true-formulas in 1 resp. 2 variables)
- Example: $\mathbb{A}^1 \overset{1:1}{\not\to} \mathbb{A}^1 \smallsetminus \{0\}$

What should counting yield?

Does cnt_K see the dimension and number of components of ϕ if ϕ is algebraic?

Theorem (Lang, Weil)

Let V be absolutely irreducible. Then $\#V(\mathbb{F}_q) \approx q^{\dim V}$ for $q \gg 0$.
("$\approx$" is almost independent of V!)

- Yes, if ϕ defines a union of absolutely irreducible varieties: $\#\phi(\mathbb{F}_q) \approx \#\text{comp-of-max-dim}(\phi) \cdot q^{\dim_{\mathrm{alg}} \phi}$.
- Hope: for ϕ arbitrary, there exist d, μ such that $\#\phi(\mathbb{F}_q) \approx \mu \cdot q^d$
- Call d *dimension* of ϕ and μ *measure* of ϕ.

Dimension and measure: more precisely

More precisely:

- Consider $\mu_d := \lim_{q\to\infty} \frac{\#\phi(\mathbb{F}_q)}{q^d}$.
  If $0 < \mu_d < \infty$, then define $\dim_K \phi := d, \mu_K(\phi) := \mu_d$.
  (If all $\mu_d = 0$, then $\dim_K \phi := 0, \mu_K(\phi) := 0$.)
- Problem: Limit does not need to exist.
  Example: $\phi = \{\pm\sqrt{10}\}$

$$\#\phi(\mathbb{F}_q) = \begin{cases} 0 & \text{for infinitely many } q \\ 2 & \text{for infinitely many } q \end{cases}$$

- So recall $K \equiv \prod_{\mathcal{U}} \mathbb{F}_q$ and use ultra-limit:

$$\mu_d := \lim_{\mathcal{U}} \frac{\#\phi(\mathbb{F}_q)}{q^d} \in \mathbb{R} \cup \{\infty\}$$

In particular, this is an invariant for K.

Measure: existence theorem

Problem if e.g. $\#\phi(\mathbb{F}_q) \approx \log q$.
For $\dim_K \phi, \mu_K(\phi)$ to be well defined, we need:

Theorem (Chatzidakis, van den Dries, Macintyre)

For any $\phi \neq \emptyset$, there exists $d \in \mathbb{N}$ such that $0 < \mu_d < \infty$, where

$$\mu_d := \lim_{\mathcal{U}} \frac{\#\phi(\mathbb{F}_q)}{q^d}$$

Moreover, $\mu_d \in \mathbb{Q}$.

Measure: idea of proof 1

Proof for quantifier-free formulas: use the theorem of Lang-Weil

- We already saw: ϕ union of absolutely irreducible varieties $\Rightarrow$ $\dim_K \phi =$ algebraic dimension of ϕ, $\mu_K(\phi) = \#$components of max. dim.
- If $\phi = \{(x,y) \mid y^2 = 2x^2\} = \{(x, \pm\sqrt{2}x)\}$:
  - If $\sqrt{2} \notin K$, wlog. $\sqrt{2} \notin \mathbb{F}_q \Rightarrow \phi(\mathbb{F}_q) = \{0\}$. Ok. But note: $\dim_K \phi \neq \dim_{\mathsf{alg}}(V(y^2 - 2x^2))$.
  - If $\sqrt{2} \in K$, then wlog. $\sqrt{2} \in \mathbb{F}_q$, so can decompose ϕ into $\{(x, \sqrt{2}x)\} \cup \{(x, -\sqrt{2}x)\}$.

  Same idea works for arbitrary algebraic sets.
- For constructible sets, consider the Zariski closure.

Measure: idea of proof 2

Generalize to arbitrary formulas: use:

Theorem (Almost quantifier-elimination)

For any ϕ, there exists ψ quantifier free such that for all $\overline{a} \in K$: $K \models \phi(\overline{a}) \leftrightarrow \exists \overline{y} \psi(\overline{a}, \overline{y})$
And: There is an $N \in \mathbb{N}$ such that for all $\overline{a} \in \phi(K)$: $\#\{\overline{b} \mid K \models \psi(\overline{a}, \overline{b})\} \leq N$.

- If $\#\{\overline{b} \mid K \models \psi(\overline{a}, \overline{b})\} = N$ for all $\overline{a} \in \phi(K)$, then $\#\psi(\mathbb{F}_q) = N \cdot \#\phi(\mathbb{F}_q)$. So $\dim_K \phi = \dim_K \psi$ and $\mu_K(\phi) = \frac{1}{N}\mu(\psi_K)$
- Otherwise: fiddle around. □

Properties of dimension and measure

A lot of properties follow easily from the definition:

Lemma

$$\dim_K(\phi \dot\cup \psi) = \max\{\dim_K \phi, \dim_K \psi\}$$

$$\mu_K(\phi \dot\cup \psi) = \begin{cases} \mu_K(\phi) + \mu_K(\psi) & \text{if } \dim_K \phi = \dim_K \psi \\ \mu_K(\phi) & \text{if } \dim_K \phi > \dim_K \psi \end{cases}$$

$$\dim_K(\phi \times \psi) = \dim_K \phi + \dim_K \psi$$
$$\mu_K(\phi \times \psi) = \mu_K(\phi) \cdot \mu_K(\psi)$$

If $f : \phi \twoheadrightarrow \psi$ is $n : 1$, then $\dim_K \phi = \dim_K \psi$, $\mu_K(\phi) = n \cdot \mu_K(\psi)$

Example: $f : K \to K, x \mapsto x^2$ is $2:1$ onto the set of squares, so $\mu_K(\{\text{squares}\}) = \frac{1}{2}$.

Summary of non-bijections

Using cnt_K, dimension, and measure, we can prove many non-bijections:

- $\phi = \{(x,y) \mid x^2 = y^3\}$, $\psi = \{\text{squares}\}$ $\mu_K(\phi) = 1$, $\mu_K(\psi) = \frac{1}{2} \Rightarrow \phi \overset{1:1}{\not\to} \psi$
- $\phi' = \mathbb{A}^2 \smallsetminus \phi$, $\psi' = \mathbb{A}^2 \smallsetminus \psi$ $\dim_K \phi' = \dim_K \psi' = 2$, $\mu_K(\phi') = \mu_K(\psi') = 1$. $cnt_K(\psi') = ???$ Combine cnt_K and μ_K:
  - $\mu_K(\phi) \neq \mu_K(\psi) \Longrightarrow cnt_K(\phi) \neq cnt_K(\psi)$
  - $cnt_K(\phi') + cnt_K(\phi) = cnt_K(\mathbb{A}^2)$ $cnt_K(\psi') + cnt_K(\psi) = cnt_K(\mathbb{A}^2)$
  - $\Longrightarrow cnt_K(\phi') \neq cnt_K(\psi') \Longrightarrow \phi' \overset{1:1}{\not\to} \psi'$

From $\mathrm{Th}(K)$ to $\mathrm{Th}(\mathrm{PSF}_0)$

- Up to now: $T = \mathrm{Th}(K)$ where K is pseudo-finite, $\mathrm{char}\, K = 0$. Now: $\mathrm{Th}(\mathrm{PSF}_0) :=$ theory of pseudo-finite fields of characteristic 0. (incomplete)
- In general: Suppose T_1 is L_1-theory, T_2 is L_2-theory with $L_1 \subset L_2$ and $T_1 \subset T_2$. Then:
$$\begin{aligned} \mathrm{Def}(T_1) &\longrightarrow \mathrm{Def}(T_2) \\ \phi &\longmapsto \phi \end{aligned}$$
compatible with definable bijections.
- For any K, apply this to $\mathrm{Th}(\mathrm{PSF}_0) \subset \mathrm{Th}(K)$:
$$\begin{aligned} \dim_K &: \mathrm{Def}(\mathrm{Th}(\mathrm{PSF}_0)) \longrightarrow \mathbb{N} \\ \mu_K &: \mathrm{Def}(\mathrm{Th}(\mathrm{PSF}_0)) \longrightarrow \mathbb{Q} \end{aligned}$$

Different notions of dimension

These $\dim_K$, μ_K are indeed different:

- Recall example: $\phi = \{(x,y) \mid y^2 = 2x^2\}$: $\dim_K(\phi) = 1$ if $\sqrt{2} \in K$ $\dim_K(\phi) = 0$ if $\sqrt{2} \notin K$ (So neither $\phi \overset{1:1}{\to} \{0\}$ nor $\phi \overset{1:1}{\to} \{(x,y) \mid x^2 = y^2\}$ in $\mathrm{Th}(\mathrm{PSF}_0)$.)

We may also define

$$\dim(\phi) := \max\{\dim_K(\phi) \mid K \models \mathrm{Th}(\mathrm{PSF}_0)\}$$

If ϕ is algebraic, then $\dim(\phi) = \dim_{\mathsf{alg}}(\phi)$.

Counting in $\mathrm{Th}(\mathrm{PSF}_0)$

K pseudo-finite yields $\mathrm{Def}(\mathrm{Th}(\mathrm{PSF}_0)) \longrightarrow \mathrm{Def}(\mathrm{Th}(K)) \xrightarrow{cnt_K} \mathbb{N}^{\mathcal{U}}$.
But we may also count directly for $\mathrm{Th}(\mathrm{PSF}_0)$:

- $\mathrm{Th}(\mathrm{PSF}_0) \models \phi \iff \mathbb{F}_{p^r} \models \phi$ for almost all p.
- So define
$$S = \{(n_q)_{q \text{ prime power}} \mid n_q \in \mathbb{N}\} / (n_q)_q = (n'_q)_q \text{ if } n_{p^r} = n'_{p^r} \text{ for almost all } p$$
- We get
$$\begin{aligned} cnt &: \mathrm{Def}(\mathrm{Th}(\mathrm{PSF}_0)) \longrightarrow S \\ &\phi \longmapsto (\#\phi(\mathbb{F}_q))_q \end{aligned}$$
- cnt contains *all* the counting information. In particular: $cnt(\phi_1) = cnt(\phi_2)$ implies (for any K):
  - $\dim_K(\phi_1) = \dim_K(\phi_2)$, $\mu_K(\phi_1) = \mu_K(\phi_2)$.
  - $cnt_K(\phi_1) = cnt_K(\phi_2)$
- Maybe $cnt(\phi_1) = cnt(\phi_2) \Longrightarrow \phi_1 \overset{1:1}{\to} \phi_2$??

Is cnt injective?

Example:

- $\phi = \{\text{squares}\} \smallsetminus \{0\}$, $\psi = \{\text{non-squares}\}$. If $2 \nmid q$, then $\#\phi(\mathbb{F}_q) = \#\psi(\mathbb{F}_q)$. $\Longrightarrow cnt(\phi) = cnt(\psi)$
- However, we will show: $\phi \overset{1:1}{\not\to} \psi$.
- Method: find other invariant θ with $\theta(\phi) \neq \theta(\psi)$.

Other theories

We construct θ in a more general setting.

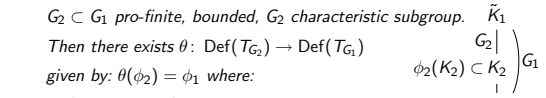
- Recall:
$$K \models \mathrm{Th}(\mathrm{PSF}_0) \iff K \text{ perfect and PAC},\ \mathrm{Gal}(\tilde{K}/K) \cong \hat{\mathbb{Z}}, \mathrm{char}\, K = 0$$
- Replace $\hat{\mathbb{Z}}$ by other group G.
- Is "$\mathrm{Gal}(\tilde{K}/K) \cong G$" first order?
Yes if G is *bounded* : $\iff$ finite number of quotients of each fixed cardinality.
- For G pro-finite, bounded, define T_G:
$$K \models T_G \iff K \text{ perfect and PAC},\ \mathrm{Gal}(\tilde{K}/K) \cong G, \mathrm{char}\, K = 0$$
- Examples: $T_{\hat{\mathbb{Z}}} = \mathrm{Th}(\mathrm{PSF}_0)$, $T_{\{1\}} = \mathrm{Th}(\mathrm{ACF}_0)$

Maps between different $\mathrm{Def}(T_G)$

There are maps between $\mathrm{Def}(T_G)$ for different G:

Theorem (H.)

$G_2 \subset G_1$ pro-finite, bounded, G_2 characteristic subgroup.
Then there exists θ: $\mathrm{Def}(T_{G_2}) \to \mathrm{Def}(T_{G_1})$
given by: $\theta(\phi_2) = \phi_1$ where:
$K_1 \models T_{G_1} \rightsquigarrow K_2 \models T_{G_2}$ $\quad \phi_1(K_1) = \phi_2(K_2) \cap K_1 \subset K_1$



Moreover θ is compatible with definable bijections.

- Main statement: $\phi_2(K_2) \cap K_1$ is definable (uniformly in K_1).
- θ can be interpreted as an invariant for T_2.

Squares $\overset{1:1}{\not\to}$ non-squares

- Let $T := \mathrm{Th}(\mathrm{PSF}_0)$.
- Recall example $\phi = \{\text{squares}\} \smallsetminus \{0\}$, $\psi = \{\text{non-squares}\}$.
- Choose $G_1 := \hat{\mathbb{Z}} \supset G_2 := 2\hat{\mathbb{Z}}$ ($\cong \hat{\mathbb{Z}}$)
- $\rightsquigarrow \theta$: $\mathrm{Def}(T_2) \longrightarrow \mathrm{Def}(T_1)$ with $T_1 = T_2 = \mathrm{Th}(\mathrm{PSF}_0)$
- Let $K_1 \models T_{G_1}$. $K_2 := \tilde{K}_1^{G_2}$ = is the extension of degree two.

$$\begin{array}{ccccc} \phi(K_2) & \subset & K_2 & \supset & \psi(K_2) \\ & & | & & \\ K_1^\times = \phi(K_2) \cap K_1 & \subset & K_1 & \supset & \psi(K_2) \cap K_1 = \emptyset \end{array}$$

- All elements of K_1 are squares of elements of K_2.
- $\implies \quad \theta(\phi) = K_1^\times \neq \emptyset = \theta(\psi) \quad \implies \phi \overset{1:1}{\not\to} \psi$

Invariants for T_G, $G \neq \hat{\mathbb{Z}}$

We know invariants for T_G if $G = \hat{\mathbb{Z}}$ or $G = \{1\}$. What about other G? If $G \subsetneq \hat{\mathbb{Z}}$:

- T_G is somewhere between $\mathrm{Th}(\mathrm{ACF}_0)$ and $\mathrm{Th}(\mathrm{PSF}_0)$
- Counting in $K \models T_G$?
Why should $\#\phi(\mathbb{F}_q)$ be an invariant?
- Instead: apply the theorem to $G \subset \hat{\mathbb{Z}}$:
$$\mathrm{Def}(T_G) \xrightarrow{\theta} \mathrm{Def}(\mathrm{Th}(\mathrm{PSF}_0)) \xrightarrow{cnt_K} \mathbb{N}^{\mathcal{U}}$$
- Example: If $G = \{1\}$, $\mathrm{Def}(T_G) \xrightarrow{\theta} \mathrm{Def}(\mathrm{Th}(\mathrm{PSF}_0)) \xrightarrow{\dim} \mathbb{N}$ gives back the algebraic dimension.

Idea of proof

For those who are interested: idea of proof of the theorem
(The others may sleep.)

- Recall: $G_2 \subset G_1$
$K_1 \models T_{G_1}$, $K_2 := \tilde{K}_1^{G_2} \models T_{G_2}$
$\theta(\phi_2) = \phi_1$ with $\phi_1(K_1) = \phi_2(K_2) \cap K_1$
- Compatibility with definable bijections:
If ψ_2 defines $\phi_2 \overset{1:1}{\to} \phi_2'$, then check that ψ_1 defines $\phi_1 \overset{1:1}{\to} \phi_1'$
- Only difficulty: $\phi_2(K_2) \cap K_1$ is definable in T_1

Definability of $\phi_2(K_2) \cap K_1$

Definablility: shown on the example $G_1 = \hat{\mathbb{Z}}$ and $\phi_2 = \{\text{squares}\}$.

- $\phi_2(K_2)$ is image of K_2 under $f\colon x \mapsto x^2$.
(In general: image of $V(K_2)$ under finite-to-1 map f.)
- f is even 2-to-1 as map $\tilde{K}_2 \to \tilde{K}_2$.
- If $x \in K_1$, then $f^{-1}(x) \subset L$, where $[L : K_1] = 2$.
- $x \in \phi_2(K_2) \iff$ ex. $y \in f^{-1}(x)$ in K_2, i.e. y fixed by G_2.
- It suffices to check if y is fixed by the image of G_2 in $\mathrm{Gal}(L/K_1)$.
- Can speak about L and $\mathrm{Gal}(L/K_1)$ in K_1.
- G_2 characteristic in $G_1 \Rightarrow$ image of G_2 in $\mathrm{Gal}(L/K_1)$ definable.
$\implies$ can say "y is fixed by this image" $\square$