1 Definable measures

1.1 Pseudo-finite fields

We work with the ring language $L = \{+, -, \cdot, 0, 1\}$. Everything in these notes is definable, even when not explicitely stated.

{D:PSF}

Definition 1.1. Let Psf be the theory of all finite fields:

$$\mathrm{Psf} := \bigcap_{q \text{ prime power}} \mathrm{Th}(\mathbb{F}_q)$$

and Psf_p be the theory that of all finite fields of characteristic p s:

$$\mathrm{Psf}_p := \bigcap_n \mathrm{Th}(\mathbb{F}_{p^n})$$

A *pseudo-finite field* (PSf) is an infinite model of Psf.

Properties of pseudo-finite fields: Let K be a pseudo-finite field. First note that K is a field (because this can be expressed in first order). Moreover, K has also the following properties:

1. K is perfect, i.e. either $charK = 0$ or $charK = p$ and $(K^\times)^p = K^\times$.

   This is true for all finite fields and it can be expressed in first order, so it's also true for pseudo-finite fields.

2. $\mathrm{Gal}(\bar{K}/K) \cong \hat{Z}$ where $\bar{K}$ is the algebraic closure of K and $\hat{Z}$ is the free profinite group in one generator. This means that for each n, there's exactly one (up to isomorphism) extension L/K of degree n.

   Again, this is true for finite fields and is first order since we can encode extensions of degree n in terms of minimal polynomials. Two such extensions become isomorphic if and only if their minimal polynomials have a root modulo the other one.

3. K is pseudo-algebraically closed. This means that every *absolute irreducible* variety over K has a K-rational point. A variety V is called *absolute irreducible* iff it ss irreducible over $\bar{K}$. (For example, $V(X^2+Y^2)$ is irreducible over $\mathbb{Q}$, but not absolute irreducible because $X^2 + Y^2 = (X + iY)(X - iY)$ over $\mathbb{Q}(i)$.)

   This is not true for finite fields, but each absolute irreducible variety V has a point in any "sufficiently large" finite fields (by the "Lang-Weil-inequalities"). So V has points for sufficiently large finite field and therefore also in pseudo-finite fields.

In fact, the converse is true:

Theorem 1.2. *Every infinite field satisfying 1.–3. is pseudo-finite.*

(The proof is not easy.)

{example:psf}

Example 1.3. Let $A = \prod_q \mathbb{F}_q$ the product of an infinite set of finite fields with componentwise operations. It is a ring. Choose some maximal ideal $\mathfrak{m}$ containing the ideal $\{(a_i)_i \mid a_i = 0 \text{ for almost all } i\}$. Then $A/\mathfrak{m}$ is a pseudo-finite field.

(This is just the ultraproduct construction, expressed in an algebraic language. In fact, this example is the *general example*; each pseudo-finite field can be constructed in this way.)

Note 1.4. Psf is *not* a complete theory. For example, Psf does not specify the characteristic. Similarly, it does not determine whether or not the field contains the third roots of unity. (There are infinitely many finite fields which do contain them as well as infinitely many which do not.)

However, there is a partial result concerning completeness:

Note 1.5. If $K, L \models$ Psf and there is an arbitrary subset $A \subset K \cap L$ such that $\mathrm{acl}_K A \cong \mathrm{acl}_L A$ (as fields), then $K \equiv_A L$.

1.2 A definable measure

The goal now is to define a measure on definable sets of pseudo-finite fields as follows: Think of our pseudo-finite field K as a limit of finite fields (in the sense of the ultra-product construction of example 1.3). Let X be a formula in the ring language. We can count the number of points of X over any finite field and consider the limit of this cardinalities in the ultra-product. We get sensible results.

More precisely, consider

$$\lim_{\mathcal{U}} \frac{|X(\mathbb{F}_q)|}{q^n}.$$

Intuitively, if this limit is some number $\mu X \neq 0$, this means that the dimension of X is n and that its size is "μX times the size of K". We will call μX the measure of X.

Moreover, we will prove that for each pseudo-finite field, there is exactly one such measure.

Let K be a pseudo-finite field and $\bar{K}$ some fixed algebraic closure. We will work in $\bar{K}$, and consider two different extensions of the ring language L: Let $\mathfrak{L}$ be the language L extended by a predicate for $K \subset \bar{K}$. (So in $\mathfrak{L}$, we can have quantifiers over K.) Let L_K resp. $\mathfrak{L}_K$ be the language L resp. $\mathfrak{L}$ extended by constants for the elements of K.

The main theorem is the following:

{thm:th}

Theorem 1.6. *In this situation, there is a unique way to assign to each $\mathfrak{L}_K$-definable set V (that is, to each $\mathfrak{L}_K$-formula) a number $\mu(V)$ ("the size of $V(K)$") such that:*

1. $\mu(\emptyset) = 0$.
2. *If V is L_K-definable and* $\mathrm{Md}(V) = 1$, *then* $\mu(V) = 1$. *(Note that we are working in the algebraically closed field $\bar{K}$, so* Md *makes sense.)*
3. *If V is finite, then $\mu(V) = |V|$.*
4. *"Fubini": If X, Y and $f\colon X \to Y$ are $\mathfrak{L}_K$-definable, then there's a partition of Y into finitely many sets Y_i such that both,* $\dim(f^{-1}(y)) =: d_i$ *and $\mu(f^{-1}(y)) =: m_i$ are constant for $y \in Y_i$, and the measure of X can be computed as follows: Let $e_{\max}$ be the maximum of the $d_i + \dim Y_i = \dim f^{-1}(Y_i)$. Then*

$$\mu(X) = \sum_{d_i + \dim Y_i = e_{\max}} \mu(Y_i) \cdot m_i$$

Example 1.7. Let $Y = \{y \mid y \neq 0 \wedge \exists x \in K\colon x^2 = y\}$ (that is, $Y(K) = (K^\times)^2$). Y is not L_K-definable since the quantifier goes only over K (and not over $\bar{K}$). (So we can't use 2. to compute $\mu(Y)$.) Now set $X = \{x \mid x \neq 0\}$. We have a definable surjection $f\colon X \to Y, x \mapsto x^2$, and each fiber has two elements. So by 4., $\mu(X) = \mu(Y) \cdot \mu(\text{two-element-set}) = \mu(Y) \cdot 2$. Now X is L_K-definable, and $\mathrm{Md}(X) = 1$, so $\mu(X) = 1$ and $\mu(Y) = \frac{1}{2}$.

1.3 Construction of the measure

The idea is the following: Each $\mathfrak{L}_K$-definable set X can be cut into finitely many pieces such that for each piece, we have a covering with an L_K-definable set. We can compute the measure of the covering using property 2. and 3. of measures, and then we use 4. to get the measure of X. The problem then is, of course, to prove that this definition does not depend on any choice and that the result has all the desired properties.

Definition 1.8. Let P, Q be partial types and let $f\colon P \to Q$ be a (definable) map. Then f is said to be *Galois* if there is a finite group H acting *strictly transitively* on the fibers of f, i.e. for each v, v' in one fiber there is exactly one $h \in H$ such that $h(v) = v'$.

H is called the *Galois group* of f.

{lemma:cover}

Lemma 1.9. *Let P, Q be partial types, with P complete, and let $g\colon P \to Q$ be definable with finite fibers. Then this can be "lifted" to a Galois map: There exists a type $\tilde{P}$ and a map $h\colon \tilde{P} \to P$ such that*

$$\begin{tikzcd} \tilde{P} \arrow[rr, "h"] \arrow[dr, "\tilde{g}"'] & & P \arrow[dl, "g"] \\ & Q & \end{tikzcd}$$

commutes and $\tilde{g}$ is a Galois covering.

Proof. Take any $a \in P$, let $b = g(a) \in Q$, and let $\bar{a} = a_1 \dots a_n = g^{-1}(b)$ be the fiber containing a, in any order. Ok, for simplicity let's say $a_1 = a$. Set $\tilde{P} = \mathrm{tp}(\bar{a})$ and $h(\bar{x}) = x_1$. Now we have to check that $\tilde{g} = g \circ h$ is Galois. Note that the fiber $\tilde{g}^{-1}(b)$ consists of those tuples $\bar{a}' \in \tilde{P}$ which are permutations of the fiber $g^{-1}(b)$. (This is because $\tilde{g}(\bar{a}') = g(a_1') = b$, so $\bar{a}'$ is in the fiber if and only of a_1' is in $g^{-1}(b)\dots$) So we can take $H = \left\{\sigma \in \mathrm{Symm}(n) \mid \sigma(\bar{a}) \in \tilde{P}\right\}$. ($\sigma$ acts on $\bar{a}$ by permuting the entries.) This H acts strictly transitive on $\tilde{g}^{-1}(b)$, and as P is complete, the same holds for any other fiber. $\square$

{note:cover}

Note 1.10. If $f\colon V \to W$ is $\mathfrak{L}_K$-definable with finite fibers with V Ł$_K$-definable of $\mathrm{Md}(V) = 1$, then the lemma can be applied to find a generic subset $V' \subset V$ of smaller codimension and a subset $W' \subset W$ such that the restriction of $f_{\restriction V'}: V' \to W'$ is Galois.

{lemma:notAtHome}

Lemma 1.11. *If W is $\mathfrak{L}_K$-definable, then there exists an L_K-definable set V and an L_K-definable map $f\colon V \to \bar{K}^n$ with finite fibers such that $f(V(K)) = W$.*

Proof. Kids, don't prove this at home! $\square$

Now, fix once and for all a (topological) generator $\sigma \in \mathrm{Gal}(\bar{K}/K) \cong \hat{Z}$ of the Galois group.

Given a Galois map $f\colon V \to W$ with Galois group H, we want to define the *Artin symbol*, which is a map from $W(K)$ to the set of conjugacy classes of H. So take a $w \in W(K)$. Choose a $v \in f^{-1}(w)$ in the fiber and look at the action of σ. As $w \in W(K)$, σ fixes w, so v^σ is again an element of $f^{-1}(w)$. By definition of a Galois map, there is exactly one element $h_v \in H$ mapping v to v^σ. We want the Artin symbol $\mathrm{Artin}(w)$ to be the conjugacy class of h_v. An easy computation yields that this conjugacy class does not depend on the choice of $v \in f^{-1}(w)$.

{D:cover}

Definition 1.12. Let $\mathcal{E}$ be the set of all "Coverings" (V, W, f, H) where

- V is L_K-definable and has $\mathrm{Md}(V) = 1$.
- W is $\mathfrak{L}_K$-definable.
- $f\colon V \to W$ is Galois with group H.

Given such a covering, we can cut a set W into parts according to the Artin symbol: For a covering $q = (V, W, f, H)$ and a subset S of the conjugacy classes in H, define $X(q, S) = \{w \in W(K) \mid \mathrm{Artin}(w) \in S\}$.

Now suppose W is any $\mathfrak{L}_K$-definable set. By lemma 1.11, there exists an L_K-definable set V and a map $f\colon V \to W$ with finite fibers. Considering the restriction to the components of V of maximal Morley rank, we can cover W piecewise by Galois coverings. Given a point w in $W(K)$, there exits some neighbourhood of w of the form $X(q_i, S_i)$ for some covering q_i and some collection of conjugacy classes S_i. By compactness, W can be written as a finite union

$W = \bigcup_i X(q_i, S_i)$. By finite additivity, it is enough to define the measure for sets of the form $X(q_i, H_i)$ and check that the measure is independent of the way we splitted W.

1.4 The proof

In this subsection we're involved in giving a proof of theorem 1.6.We have devided the proof in several steps.

- (definition) Let W be a definable set of $\mathfrak{L}_K$.By lemma 1.11, there exists an L_K-definable set V and a map $f\colon V \to W$ with finite fibers. For each point w in $W(K)$, we can consider the L_K-type P of an element of $f^{-1}(w)$. Lemma 1.9 can be applied to P, and we get a Galois covering $\tilde{f}\colon \tilde{P} \to f(P) \subset W$. The fact that $\tilde{f}$ defines a Galois covering on a certain element $w' \in W(K)$ is definable, so we already have a Galois covering of a whole neighbourhood of w.

  By compactness, we can choose a finite collection of such Galois coverings $q_i = (V_i, W_i, f_i, H_i)$ such that $W = \bigcup_i W_i = \bigcup_i X(q_i, H_i)$.

  Write H as a union of conjugacy classes and choose representantives for each of them: $H := \bigcup h_i^H$. We can decompose $V := \bigcup_{h\in H} V_h = \bigcup V_{h_i^H}$ where $V_h := \{v \in V \mid v^\sigma = h \cdot v\}$ and $V_{h_i^H} := \bigcup_{g\in H} V_{h_i^g}$. Clearly $V_{Id} = V(K)$.

  Question. It seems that in order to define coherently the measure we need that V_h is a L_K-definable set of $Md = 1$. If we knew that there exists at most one subgroup of index n, then $V_{h_i^H} = V(K_n \setminus \bigcup_{m|n} K_m)$, where n is the order of h_i and K_n the only extension of K of degree n.

  For a $w \in W(K)$, the fiber $f^{-1}(w)$ is completely included in some $V_{h_i^H}$. Observe that, for $v, v' \in f^{-1}(w)$, v and v' belong to the same V_h iff there is $g \in C_H(h)$ such that $v = g \cdot v'$. Then we get a surjection from V_h over $X(q, h^H)$ with fibers of cardinality $|C_H(h)|$.

  We will define the measure for $X(q, S)$. It´s clear that, for all $h \in H$ and $v \in V_{Id}$, $h \cdot v \in Y_{Id} = V(K)$. The restriction $f\restriction_{Y_{Id}}\colon Y_{Id} \to X(q, Id)$ is $|H|$-to-one. Y_{Id} is L_K- definable and has Md one, so it should have measure one. If we want Fubini to hold: $\mu(V(K)) = |H| \cdot \mu(X(q, Id))$ (observe that $H = C_H(Id)$), we should define $\mu(X(q, Id)) = 1/|H|$. In general, we define:

  $$\mu(X(q, h^H)) = \frac{1}{|C_H(h)|} = \frac{|h^H|}{|H|}$$

  and we extend it additivity to the sets of the form $X(q, S)$, S being a reunion of conjugation classes.

- (normal subgroup) Suppose we have the following commuting diagram

$$\begin{tikzcd} V \arrow[dr, "h"] \arrow[dd, "f"'] & \\ & W' \arrow[dl, "f'"] \\ W & \end{tikzcd}$$

where $q = (V, W, f, G)$, and $q' = (W', W, f', G')$ belong to $\mathcal{E}$ and $G' = G/N$, with $N \lhd G$. Consider $S' \subseteq G/N$ a conjugacy class and $S = \bigcup_{s \in S'} s \cdot N$ its lifting to G, i.e., a union of conjugacy classes: $S = S_1 \bigcup \ldots \bigcup S_n$. Then:

$$\mu(X(q, S)) = \sum \mu(X(q, S_i)) = \sum \frac{|S_i|}{|G|} = \frac{|S|}{|G|} = \frac{|S'|}{|G'|} = \mu(X(q', S'))$$

where the first equality is granted by definition.

- (Well defined) Suppose now that we have a $\mathfrak{L}_K$-definable set W and two coverings $q_i := (V_i, W, f_i, H_i)$ of it. Consider the L_K-set $V_1 \times_W V_2$. This set equips W with the covering $q := (V_1 \times_W V_2, W, f_1 \times f_2, H_1 \times H_2)$:

$$\begin{tikzcd} & V_1 \times_W V_2 \arrow[dl, "\pi_1"'] \arrow[dd] \arrow[dr, "\pi_2"] & \\ V_1 \arrow[dr] & & V_2 \arrow[dl] \\ & W & \end{tikzcd}$$

  We have seen in the last paragraph that if we lift from $H_1 = (H_1 \times H_2)/H_2$ to $H_1 \times H_2$ the measure doesn't change. Similarly for H_2. So the measure is well-defined.

- (Fubini finite fibers) If we have a Galois covering $q := (V, W, f, H)$ that factors through the $\mathfrak{L}_K$-definable set W':

$$\begin{tikzcd} V \arrow[dd, "f"'] \arrow[dr, "f'"] & \\ & W' \arrow[dl, "g"] \\ W & \end{tikzcd}$$

  we define the subgroup $H_1 := \{h \in H \mid f'(v) = f'(h \cdot v)\}$. Then $q' := (V, W', f', H_1)$ is a Galois covering and for all $w \in W'$, $Artin_{H_1}(w)^H = Artin_H(g(w))$. On the other hand, for all $h \in H$, $f' \colon Y_h \to X(q', h^{H_1})$ has fibers of size $|C_{H_1}(h)|$,$f \colon Y_h \to X(q, h^H)$ has fibers of size $|C_H(h)|$ and so $g \colon X(q', h^{H_1}) \to X(q, h^H)$ has fibers of size $|C_H(h)|/|C_{H_1}(h)|$.

  So we get Fubini for the $\mathfrak{L}_K$-functions $g \colon W' \to W$ having finite fibers, since we get -using finite additivity-:

$$\mu(X(q', S')) = deg(g) \cdot \mu(X(q, S))$$

  Up to now we have shown that the measure is well-defined and satisfies properties 1. to 3., and "Fubini" for maps with finite fibers.

- (Fubini Md=1) Suppose now we're dealing with a L_K-definable map $g\colon W \to Y$, where W and Y are also L_K-definable sets of Morley degree one and even the fibers have degree one. Consider a covering $q := (V, W, f, H)$ and define, for $y \in Y$, $W_y := g^{-1}$, $V_y := f^{-1}(W_y)$ and $f_y := f \restriction V_y$. Observe that, if we take $y \in Y(K)$, W_y is not empty being a L_K-definable set of degree one. So we get a set of coverings $q_y := (V_y, W_y, f_y, H)$.

  Now consider any $h \in H$ and the restriction map $g\colon X(q, h^H) \to Y$. The fibers of these map are of the form $X(q_y, h^H)$, so they have measure $1/C_H(h)$. On the other hand, $g(X(q, h^H)) = Y(K)$ (W_y is not empty, so we can find a solution of $\sigma(w) = h \cdot w$ in it). Then Fubini holds in the form:

$$\mu(X(q, h^H)) = 1/C_h(h) = (1/C_h(h)) \cdot 1 = \mu(X(q_y, h^H)) \cdot \mu(Y)$$

- Now we should take care of the following situation: $g\colon W \to Y$ is a L_K-definable map between L_K-irreducible sets where now we allow the map to have fibers of any Morley degree. The map g factors in the following way

$$\begin{tikzcd} W \arrow[rr, "g"] \arrow[dr, "g_1"'] & & Y \\ & W/\sim \arrow[ur, "g_2"'] & \end{tikzcd}$$

  where $\sim$ is the equivalent relation "belonging to the same irreducible component of some fiber". Thus $g_2^{-1}(y)$ encodes the irreducible components of $g^{-1}(y)$, g_1 has fibers of Morley degree one and g_2 has finite fibers. Since this two cases have already been studied and μ is "linear", g also verifies "Fubini".

  1.11

- (general case) Finally, let's consider any $\mathfrak{L}_K$-definable sets W, Y and any $\mathfrak{L}_K$-definable map $g\colon W \to Y$ between them. We can build the diagram

$$\begin{tikzcd} \widetilde{W \times_Y \widetilde{Y}} \arrow[d, "\phi"'] & \\ W \times_Y \widetilde{Y} \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & \widetilde{Y} \arrow[d, "\psi"] \\ W \arrow[r, "g"'] & Y \end{tikzcd}$$

  from the following steps:

  - Use 1.11 in order to find a L_K-definable set $\widetilde{Y}$ and a L_K-definable finite-to-one function ψ from $\widetilde{Y}$ onto Y.
  - Build the product $W \times_Y \widetilde{Y}$. It's a $\mathfrak{L}_K$-set, but π_2 is simply a L_K-definable function.

- Use 1.11 again to get a L_K-definable set $\widetilde{W \times_Y \widetilde{Y}}$ and a L_K-definable finite-to-one function ϕ from $\widetilde{W \times_Y \widetilde{Y}}$ onto $W \times_Y \widetilde{Y}$.
- Then $\pi_2 \circ \phi$, being a L_K-map, verifies "Fubini". Likewise $\pi_1 \circ \phi$ does, since π_1 and "a fortiori" $\pi_1 \circ \phi$ are finite-to-one maps. Since the same is true for ψ, we deduce "Fubini" for g.

2 Motivic counting

In the following, L denotes the set of formulae in the ring language. Formulae will be parameter-free (unless specified).

Motivation : for each L-formula ϕ, we want to determine $|\phi(\mathbb{F}_q)|$ for every (possibly *almost every*) finite field.

Let $\mathcal{F}$ be the ring of maps from $\{p^r : p \text{ prime}, r \geq 1\}$ to $\mathbb{Q}$. For each L-formula ϕ, we obtain a map $q \mapsto |\phi(\mathbb{F}_q)|$ in $\mathcal{F}$. Let count denote the following map:

$$\text{count} : \begin{array}{ccc} \mathrm{L} & \longrightarrow & \mathcal{F} \\ \phi & \mapsto & (q \mapsto |\phi(\mathbb{F}_q)|) \end{array}$$

In order to obtain some information, we want to construct a ring R, *as small as possible*, such that :

$$\begin{array}{ccc} L & \longrightarrow & R \\ \downarrow & \swarrow & \\ \mathcal{F} & & \end{array}$$

We consider first the ring $R_1 = \langle L \rangle_{\mathbb{Q}}$ generated by L over Q, i.e. formal finite sums $\sum a_i[\phi_i]$ with $a_i \in \mathbb{Q}$ and $\phi_i \in L$. Moreover, we identify formulae up to change of variables. This is a ring if we define multiplication as follows:

$$[\phi_1] \times [\phi_2] = [\phi_1(\bar{x}) \wedge \phi_2(\bar{y})] \text{ with } \bar{x} \cap \bar{y} = \emptyset.$$

Then :

$$\begin{array}{ccc} L & \overset{i}{\longrightarrow} & R_1 \\ \downarrow & \swarrow_{j} & \\ \mathcal{F} & & \end{array}$$

with $i(\phi) = [\phi]$ and $j(\sum a_i[\phi_i]) = \sum a_i \operatorname{count}(\phi_i)$.

Let Psf be as in 1.1 the theory of finite fields. Since we want to count the points on finite fields, we may impose on R_1 the equivalence relation $\sim_{\mathrm{Psf}}$ generated by the following properties:

1. $[\phi_1] \sim_{\mathrm{Psf}} [\phi_2]$ if $\mathrm{Psf} \models \phi_1 \iff \phi_2$;
2. $[\phi_1 \vee \phi_2] \sim_{\mathrm{Psf}} [\phi_1] + [\phi_2]$ if $\mathrm{Psf} \models \neg(\phi_1 \wedge \phi_2)$;
3. $[\phi_1] \sim_{\mathrm{Psf}} [\phi_2]$ if there exists a formula θ such that Psf $\models$ "θ is the graph of a bijection from ϕ_1 to ϕ_2" (i.e. $\mathrm{Psf} \models \phi_1 \overset{1:1}{\to} \phi_2$);
4. $[\phi_1] \sim_{\mathrm{Psf}} n[\phi_2]$ if there exists a formula θ such that Psf $\models$ "θ is the graph of an n-to-1 surjection from ϕ_1 onto ϕ_2" (i.e. $\mathrm{Psf} \models \phi_1 \overset{n:1}{\to} \phi_2$).

To shrink the ring further, we set $\mathrm{Psf}_0 = \mathrm{Psf} \cup \{\text{char} \neq p | p\}$. In this case, $\sim_{\mathrm{Psf}_0}$-equivalence of two formulae yields equivalence of the cardinalities up to finitely many primes.

Denote by R_{Psf} the ring $R_1/\sim_{\mathrm{Psf}}$ and R_{Psf_0} the corresponding ring $R_2/\sim_{\mathrm{Psf}_0}$. Furthermore, let $\sim$ be the equivalence relation on $\mathcal{F}$ defined by $f_1 \sim f_2$ if and only if $f_1(p^r) = f_2(p^r)$ for almost all p. The following holds:

$$
\begin{tikzcd}
L \arrow[r] \arrow[d] & R_1 \arrow[r] \arrow[dl] & R_{FF} \arrow[r] \arrow[dll] & R_{PSF_0} \arrow[dl] \\
\mathcal{F} \arrow[rr] & & \mathcal{F}/\sim &
\end{tikzcd}
$$

Now, R_{Psf_0} is small enough for our purposes.:

{T:gen-V}

Theorem 2.1. *R_{Psf_0} is generated by affine varieties over $\mathbb{Q}$, i.e. by the set $\{[V] : V$ affine variety over $\mathbb{Q}\}$.*

Note that an affine variety V over $\mathbb{Q}$ is defined by a conjunctions of polynomials with coefficients in $\mathbb{Z}$, hence $\mathrm{count}(V) : q \mapsto |V(\mathbb{F}_q)|$ is well-defined.

Question 2.2. *Does uniqueness of the Hrushovski's measure follow from the above result?*

From now on, let $[\phi]$ denote its corresponding element in R_{Psf_0}.

Example 2.3. Let $\phi = \{x | \exists y : y^3 = x \wedge x \neq 0\}$ and $f : y \mapsto y^3$. Thus $\phi = \operatorname{Im} f \setminus \{0\}$

If 3 does not divide q and $\mathbb{F}_q$ does not contain any 3^{rd} root of unity , then f is injective and $|\phi(\mathbb{F}_q)| = q - 1$. Otherwise f is $3:1$ and $|\phi(\mathbb{F}_q)| = (q-1)/3$.

If $p = 3$ then $f_{\mathbb{F}_3} = \mathrm{Id}$. Suppose that $p \neq 3$, then $\mathbb{F}_q$ contains all 3^{rd} roots of unity if and only if $V : x^2 + x + 1 = 0$ has two elements in $\mathbb{F}_q$. Then:

$$|\phi(\mathbb{F}_q)| = |V(\mathbb{F}_q)|/2 \times (q-1)/3 + (1 - |V(\mathbb{F}_q)|/2)(q-1),$$

and

$$[\phi] = [V]/2 \times ([\mathbb{A}^1] - 1)/3 + (1 - [V]/2)([\mathbb{A}^1] - 1)$$

where $\mathbb{A}^1$ is the affine line.

In order to prove Theorem 2.1, we will use that Psf_0 eliminates quantifiers up to Galois coverings over $\mathbb{Q}$.

Question 2.4. *Does this follow from Lemma 1.11?*

Definition 2.5. A *Galois covering* $(\pi : V \to W, G)$ consist of the following data:

1. V and W are affine varieties (over $\mathbb{Q}$).

2. π a surjective morphism (over $\mathbb{Q}$) with finite fibers.

3. G a finite group acting strictly transitively on the fibers of π (in $\overline{Q}$) by morphisms on V (over $\mathbb{Q}$).

Let $(\pi : V \to W, G)$ be a Galois covering. For each subgroup C of G, one can define an affine variety V/C (over $\mathbb{Q}$) such that

$$\begin{array}{ccccc} V & \xrightarrow{\pi_1} & V/C & \xrightarrow{\pi_2} & W \\ v & \mapsto & C \cdot v & \mapsto & \pi(v) \end{array}$$

Therefore, $\mathrm{lift}_{V\to W,C}(w)$ denotes the the L-formula

$$(w \in W;\ \exists v \in V/C : \pi_2(v) = w)$$

{P:eq}

Proposition 2.6. *Every* L*-formula is equivalent (modulo* Psf_0*) to a boolean combination of formulas* $\mathrm{lift}_{V\to W,C}$.

Proof. Immi, give us a proof! ☐

{C:relev}

Corollary 2.7. R_{Psf_0} *is generated by the set of* $[\mathrm{lift}_{V\to W,C}]$.

Proof.

Claim. *Let* Σ *be a subset of* L *closed under conjunction containing* $\mathbb{A}^1$*. Then for every formula* ϕ *which is a boolean combination of elements of* Σ*, we have that:*

$$[\phi] \in \langle [\psi] : \psi \in \Sigma \rangle.$$

Proof of the Claim. Let ϕ be a boolean combination of elements of Σ. We may assume that ϕ is equivalent to $\phi_1 \wedge ... \wedge \phi_r$ where the ϕ_i's have disjoint set of variables and are conjunctions of formulas and negations of formulas in Σ. Then

$$[\phi] = [\phi_1] + ... + [\phi_r].$$

Note that any conjunction of formulas and negations of formulas in Σ is generated in R_{Psf_0} by some conjunctions of formulas in Σ: it follows by induction from that if $\theta_1(x_1, ..., x_n)$ and $\theta_2(x_1, ..., x_n)$ are two formulas in L then $[\neg\theta_1] = [\mathbb{A}^1]^n - [\theta_1]$ and $[\theta_1 \wedge \neg\theta_2] = [\theta_1] - [\theta_1 \wedge \theta_2]$.
End of the proof of the Claim.

Therefore, we need only prove that any conjunction

$$\mathrm{lift}_{V_1\to W_1,C_1}(\bar{x}) \cap \mathrm{lift}_{V_1\to W_2,C_2}(\bar{y})$$

is equivalent to a formula $\mathrm{lift}_{V\to W,C}(\bar{z})$. We may assume that $\bar{x} = \bar{y}$ and both W_1 and W_2 are subsets of $\mathbb{A}^n$. Replace them by $W = W_1 \cap W_2$ and V_1, V_2 by $\pi_1^{-1}(W)$, $\pi_2^{-1}(W)$. Thus, we may consider the conjunction

$$\mathrm{lift}_{V_1\to W,C_1}(\bar{x}) \cap \mathrm{lift}_{V_1\to W,C_2}(\bar{x})$$

Let

$$V := V_1 \times_W V_2 = \{(v_1, v_2) \in V_1 \times V_2 : \pi_1(v_1) = \pi_2(v_2)\}.$$

Note that we have the following diagram:

$$\begin{tikzcd}
 & & V_1 \times_W V_2 \arrow[dll] \arrow[dd] \arrow[drr] & & \\
V_1 \arrow[d] & & & & V_2 \arrow[d] \\
V_1/C_1 \arrow[drr] & & V/C_1 \times C_2 \arrow[d] & & V_2/C_2 \arrow[dll] \\
 & & W & &
\end{tikzcd}$$

Hence,

$$\mathrm{lift}_{V_1 \to W, C_1}(\bar{x}) \cap \mathrm{lift}_{V_1 \to W, C_2}(\bar{x}) \sim \mathrm{lift}_{V \to W, C_1 \times C_2}(\bar{x})$$

□

Therefore, it suffices to show that formulae of the form $\mathrm{lift}_{V \to W, C}$ generated in R_{Psf_0} by affine varieties over $\mathbb{Q}$.

Fix some Galois covering $(\pi : V \to W, G)$ and K a pseudo-finite field of characteristic 0.

Tkae $v \in V(\bar{K})$ with $\pi(v) \in W(K)$. Let $\alpha_v : \mathrm{Gal}(\bar{K}/K) \to G$ defined by $\alpha_v(\sigma) \cdot v = \sigma^{-1}(v)$ for $\sigma \in \mathrm{Gal}(\bar{K}/K)$. We denote by G_v the subgroup $\mathrm{Im}\,\alpha_v$ of G.

For a subgroup C of G, let

$$\phi_{V \to W, C} = \mathrm{lift}_{V \to W, C} \wedge \bigwedge_{A \subsetneq C} \neg\, \mathrm{lift}_{V \to W, A}\,.$$

{L:phiC1}

Lemma 2.8.

1. *Given $w \in W(K)$, then $w \in \phi_{V \to W, C}$ if and only if there exists $v \in \pi^{-1}(w)$ such that $G_v = C$.*

2. *For any $C_1, C_2 \subset G$, either $\phi_{V \to W, C_1}(K) \cap \phi_{V \to W, C_2}(K) = \emptyset$ or C_1 and C_2 are conjugates in G and $\phi_{V \to W, C_1}(K) = \phi_{V \to W, C_2}(K)$.*

Proof.

1. If $w \in \phi_{V \to W, C}$ then there is $v \in \pi^{-1}(w)$ such that $C \cdot v \in V/C(K)$. Thus, $G_v = \mathrm{Im}(\alpha_v) \subset C$. Moreover $G_v \cdot v \in K$, so $w \in \mathrm{lift}_{V \to W, G_v}$ and by minimality of C, $G_v = C$. For the otehr implication, let $v \in \pi^{-1}(w)$. Then G_v is the smallest subgroup of G such that $G_v \cdot v \in K$, so $w \in \phi_{V \to W, G_v}$.

2. If there is an element $w \in \phi_{V \to W, C_1}(K) \cap \phi_{V \to W, C_2}(K)$, then there are $v_1, v_2 \in \pi^{-1}(w)$ such that $G_{v_1} = C_1$ and $G_{v_2} = C_2$. Since v_1 and v_2 are in the same fiber, there is $g \in G$ such that $v_2 = g \cdot v_1$. Then for every $\sigma \in \mathrm{Gal}(\bar{K}, K)$, $\alpha_{v_2}(\sigma) = g\alpha_{v_1}(\sigma)g^{-1}$, so $C_2 = C_1^g$. Now, given $v \in V(\bar{K})$ with $C_1 \cdot v \in K$ then $C_2 \cdot g \cdot v = g \cdot C_1 \cdot v \in K$. It follows that $\phi_{V \to W, C_1}(K) = \phi_{V \to W, C_2}(K)$

□

{L:phiC2}

Lemma 2.9. *Let C be a subgroup of G and let π_1, π_2 such that*

$$\begin{array}{ccccc} V & \xrightarrow{\pi_1} & V/C & \xrightarrow{\pi_2} & W \\ v & \mapsto & C\cdot v & \mapsto & \pi(v) \end{array}$$

The map π_2 induces a map from $\phi_{V\to V/C,C}(K)$ to $\phi_{V\to W,C}(K)$ which is $\frac{|N_G(C)|}{|C|}$ to 1. Therefore,

$$[\phi_{V\to W,C}] = \frac{|C|}{|N_G(C)|}[\phi_{V\to V/C,C}].$$

Proof. First we have to prove that $\pi_2(\phi_{V\to V/C,C}) \subset \phi_{V\to W,C}$. Note that $\pi_1 : (V \to V/C, C)$ is a Galois covering. Let $v \in \pi_1^{-1}(\phi_{V\to V/C,C}(K))$. Then by Lemma 2.8, $C_v = C$. But $G_v = C_v$ so by Lemma 2.8, $\pi(v) \in \phi_{V\to W,C}(K)$.

Moreover, for any $g \in G$, $G_{g\cdot v} = G_v^g = C^g$, so $G_{g\cdot v} = C$ if and only if $g \in N_G(C)$. It follows that π_2 is $\frac{|N_G(C)|}{|C|} : 1$ on $\phi_{V\to V/C,C}(K)$. □

{L:phiC3}

Lemma 2.10. *For any subgroup C of G, $[\phi_{V\to V/C,C}]$ is generated by affine varieties.*

Proof. We proceed by induction on $|C|$. If C is trivial then $\phi_{V\to V,id} = V$. Otherwise, $V/C(K) = \bigcup_{A\subset C} \phi_{V\to V/C,A}(K)$. We may assume by Lemma 2.8 that we have a disjoint union of the form:

$$V/C(K) = \phi_{V\to V/C,C}(K) \cup \phi_{V\to V/C,A_1}(K) \cup ... \cup \phi_{V\to V/C,A_r}(K)$$

with $A_1, ..., A_r$ proper subsets of C. Then,

$$[\phi_{V\to V/C,C}] = [V/C] - ([\phi_{V\to V/C,A_1}] + ... + [\phi_{V\to V/C,A_r}])$$

So, by Lemma 2.9,

$$[\phi_{V\to V/C,C}] = [V/C] - \left(\frac{|A_1|}{|N_C(A_1)|}[\phi_{V\to V/A_1,A_1}] + ... + \frac{|A_r|}{|N_C(A_r)|}[\phi_{V\to V/A_r,A_r}]\right).$$

□

{L:relev}

Lemma 2.11. *For any subgroup C, $[\mathrm{lift}_{V\to W,C}]$ is generated by affine varieties.*

Proof. By Lemmas 2.9 and 2.10, $[\phi_{V\to W,C}]$ is generated by affine varieties. But, $\mathrm{lift}_{V\to W,C}(K) = \bigcup_{A\subset C} \phi_{V\to W,A}(K)$ and by Lemma 2.8, one can extract a disjoint union. □

Theorem 2.1 follows now from Corollary 2.7 and Lemma 2.11.

3 Model Completeness

In this section, we are mainly concerned with a relative elimination of quantifiers for formulae in the theory of pseudo-finite fields and more general, *PAC* perfect fields with bounded Galois group. This will yield a proof of 1.11

{F:modcom-exist}

Fact 3.1. Let T be a model-complete theory. Then every formula is equivalent to an existential one in T.

For that, we will consider algebraically closed fields in $\mathrm{L}_{\mathrm{rings}}$ expanded with a unary predicate to define a *PAC* . To avoid confusion, whenever we work in the expanded language, we will use the symbol #. Recall that Morley rank or Zariski dimension is definable in $\mathrm{L}_{\mathrm{rings}}$. Moreover, we have elimination of imaginaries which implies the following:

{F:EI}

Fact 3.2. Given an algebraically closed field M, a tuple $\bar{a}$ in M and $C \subset M$, then $\mathrm{tp}(\vec{a}/\operatorname{acl}(C) \cap \operatorname{dcl}(C\vec{a}))$ is stationary.

Definition 3.3. An infinite subset F of D is *PAC* if any $\mathrm{L}_{\mathrm{rings}}$-formula with parameters in F of multiplicity 1 has a realization in F.

Note 3.4. Let F a *PAC* set of M and a in $\operatorname{dcl}(F)$. Choose a formula $\phi(x, \vec{b})$ witnessing this fact with $\vec{b}$ in F. It is clear that $\phi(x, \vec{b})$ has multiplicity 1, hence a is in F.

Hence, a subset of an algebraically closed field is *PAC* in the above sense if and only if it is a perfect pseudoalgebraically closed field.

Moreover, we will assume that F has bounded Galois group in M and it will be some fixed profinite group G (Note that this is a first order condition). All the above will be axiomatized by some set of formulae $T^{\#}$.

{def:full}

Definition 3.5. Let M be a model of $T^{\#}$ and M_0 a #-substructure of M. We say that M_0 is full in M if M_0 is algebraically closed and $\operatorname{acl}(F^M) \subset \operatorname{dcl}(F^M M_0)$.

{L:full}

Lemma 3.6. *Let M_0 and M be as above. Then M_0 is full in M if and only if $M_0 \models T^{\#}$ if and only if* $\mathrm{Gal}(F^{M_0}) \sim \mathrm{Gal}(F^M)$.

Proof. Since algebraic closed fields have elimination of quantifiers, it is clear that any #-substructure is algebraically closed. We have a group homomorphism:

$$\begin{array}{rccc} \phi: & \mathrm{Gal}(F^M) & \to & \mathrm{Gal}(F^{M_0}) \\ & \sigma & & \sigma \restriction M_0 \end{array}$$

We claim that ϕ is an continous epimorphism of profinite groups. Continuity is clear since any finite extension of F^{M_0} induces a finite extension of F^M. In order to show that ϕ is surjective, we use the following basic result from stability:

Claim. *Let A, B and C be (possibly infinite) tuples with $A \underset{C}{\smile\!\!\!\!\!\!\mid} B$ such that* $\mathrm{tp}(A/C)$ *is stationary. Given a C-isomorphism $f : B \to B'$ with $A \underset{C}{\smile\!\!\!\!\!\!\mid} B'$, then f extends to a CA-isomorphism.*

Hence, given σ_0 in $\mathrm{Gal}(F^{M_0})$, we want to extend it to F^M. Given $\bar{a}$ in F^M, note that $\mathrm{Cb}(bara/F^{M_0})$ is in $\mathrm{acl}(F^{M_0}) \cap \mathrm{dcl}(F^{M_0}\bar{a}) \subset F^{M_0}$. Hence, $\mathrm{tp}(\bar{a}/F^{M_0})$ is stationary and we can extend σ to an element in $\mathrm{Gal}(F^M)$.

Therefore, ϕ is an isomorphism if and only if it is injective if and only if $\ker(\phi) = \mathrm{Gal}(\mathrm{acl}(F^M)/F^M\,\mathrm{acl}(F^{M_0}))$ is the identity, which is equivalent to M_0 being full in M.

Given n in $\mathbb{N}$, let $\mathcal{C}_n$ (*resp.* $\mathcal{C}_n^{M_0}$) be the collection of open subgroups of $\mathrm{Gal}(\mathrm{acl}(F^M)/F^M)$ (*resp.* $\mathrm{Gal}(\mathrm{acl}(F^{M_0})/F^{M_0})$) of index n. By boundness, we have that $\mathcal{C}_n$ and $\mathcal{C}_n^{M_0}$ are finite. Moreover, the map:

$$\begin{array}{ccc} \mathcal{C}_n^{M_0} & \to & \mathcal{C}_n \\ H & \to & \phi^{-1}(H) \end{array}$$

is injective. Hence, it is surjective (since both sets are finite and have the same cardinality in case $\mathrm{Gal}(\mathrm{acl}(F^M)/F^M) \simeq \mathrm{Gal}(\mathrm{acl}(F^{M_0})/F^{M_0})$). Now,

$$\phi^{-1}(\bigcap_{H\in\mathcal{C}_n^{M_0}} H) = \bigcap_{H\in\mathcal{C}_n} H$$

By profiniteness, $1 = \bigcap_{n\in\mathbb{N}} \bigcap_{H\in\mathcal{C}_n^{M_0}} H$, and likewise for $\mathrm{Gal}(\mathrm{acl}(F^M)/F^M)$. The equivalence is now clear.

□

{L:algdcl}

Lemma 3.7. *Let M be a model of $T^{\#}$ and M_0 a full substructure of M. Suppose there is some set C in M such that $F^{M_0} \subset C \subset F^M$ with $\mathrm{acl}(C) \cap F = C$. Given a finite tuple $\bar{a}$ in $\mathrm{acl}(C)$ there is some $\bar{e}$ in M_0 such that $\bar{a}$ and $\bar{e}$ are C-interdefinable.*

Proof. Observe that $(\mathrm{acl}(C), C)$ is a $\#$-substructure of M. Moreover, it is easy to see that if $M_0 \underset{full}{\subset} M$, then so is $(\mathrm{acl}(C), C) \underset{full}{\subset} M$, and by Lemma 3.6 so is $M_0 \underset{full}{\subset} \mathrm{acl}(C)$. Therefore, there exists some $\bar{c}$ in C with $\bar{a} \in \mathrm{dcl}(\bar{c}F^{M_0})$.

Note that $\mathrm{tp}(\bar{a}\bar{c}/\,\mathrm{acl}(F^{M_0}) \cap \mathrm{dcl}(F^{M_0}\bar{a}\bar{c}))$ is stationary. Choose some $\bar{e}$ in $\mathrm{acl}(F^{M_0}) \cap \mathrm{dcl}(\bar{a}C)$ which makes $\mathrm{tp}(\bar{a}\bar{c}/\bar{e})$ stationary. We need only show that $\bar{a}$ is in $\mathrm{dcl}(C\bar{e})$.

Let σ be an automorphism fixing $C\bar{e}$. Then $\sigma(\bar{a})\sigma(\bar{c}) \underset{\bar{e}}{\equiv} \bar{a}\bar{c}$. Since $\sigma(\bar{c}) = \bar{c}$, it follows that both $\sigma(\bar{a})\bar{c}$ and $\bar{a}\bar{c}$ realize the non-forking extension of the stationary type $\mathrm{tp}(\bar{a}\bar{c}/\bar{e})$ to F^{M_0}.

Hence $\sigma(\bar{a}) \underset{\bar{e}C}{\equiv} \bar{a}$. As $\bar{a}$ is in $\mathrm{dcl}(CF^{M_0}$, we have that $\sigma(\bar{a}) = \bar{a}$. □

{P:b&f}

Proposition 3.8. *Let (M_1, F_1) and (M_2, F_2) be two saturated models of $T^{\#}$ of the same cardinality, and $(\mathrm{acl}(F_0), F_0)$ a full $\#$-substructure of M_1 which also realizes $T^{\#}$ with $M_0 = \mathrm{acl}(F^{M_0})$. Given $A = \mathrm{acl}(F^A) \subset M$ and $B = \mathrm{acl}(F^B) \subset \mathcal{N}$ algebraically closed of small cardinality with $F_0 \subset F^A$ such that $f : A \to B$ is a partial $\#$-isomorphism, then f extends to an isomorphim of M_1 to M_2.*

{N:Hrwrong}

Note 3.9. In [2], the above result was stated in a different form that in fact it is not correct. We thank Martin Ziegler for pointing this and we here include his remark.

Let A be an algebraically closed set between $M_0 = \mathrm{acl}(F_0)$ and M_1. It does not follow that $A = \mathrm{acl}(F^A)$ (as stated by Hrushovski).

Proof of the Note Choose $b \in M_0 \setminus F_0$ and f and g in F independent over F^{M_0}. Define $a = bf + b^2 g$ and $A\,\mathrm{acl}(F^{M_0} a)$. We need only show that $a \notin \mathrm{acl}(F^A)$. Let b' a conjugate of b over F^{M_0} not equal to b. It follows that b and b' are F^M-conjugated. Hence, $a' = b'f' + (b')^2 g'$ is conjugated to a over F^M. If a were in $\mathrm{acl}(F^A)$, so will be a'. Hence, a' is in A. Since:

$$\begin{pmatrix} a \\ a' \end{pmatrix} = \begin{pmatrix} b & b^2 \\ b' & (b')^2 \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}$$

and the matrix has coefficients in A, it yields that f and g are in A. But this contradicts the fact that A has Morley rank 1 over F^{M_0}.

End of the proof of the Note

Proof.

We need only extend f to $\mathrm{acl}(F_1)$ and $\mathrm{acl}(F_2)$ by bach-and-forth and afterwards extend it to M_1 and M_2 as $\mathrm{L}_{\mathrm{ring}}$-isomorphism. Hence, choose some a in $F_1 \setminus A$. Let $A_1 = \mathrm{acl}(aF^A)$. Note that $A_1 = \mathrm{acl}(F^{A_1})$ by construction.

Claim. *We can extend f to $F^{A_1} \cup A$.*

Note that $p = \mathrm{tp}(F^{A_1}/F^A)$ is stationary (or rather the type of some appropriate enumeration of F^{A_1}), since $A \cap \mathrm{dcl}(F^{A_1} F^A) \subset F^A$. So $f(p)$ is also stationary and defined over F^B. By saturation and *PAC* we can realize p in F_2. Therefore, we extend f to an automorphism of $A \cup F^{A_1}$.

Claim. *f extends to an isomorphism over A_1.*

Extend f as above to an $\mathrm{L}_{\mathrm{ring}}$-isomorphism opver A_1. We need only check that the extension is again a #-isomorphism. Given α in A_1, it follows from 3.7 that α is F^{A_1}-interdefinable with some $\bar{e}$ in $\mathrm{acl}(F_0)$. Therefore, $f(\alpha)$ is F^{A_1}-interdefinable with $f(\bar{e})$ in $f(\mathrm{acl}(F_0))$. Since $f \restriction F^{A_1}$ is a #-isomorphism, it is clear that α is in F_1 if and only if $f(\alpha)$ is in F_2. $\square$

{C:elsub}

Corollary 3.10. *Let $F_0 \subset F_1$ be two perfect PAC fields with isomorphic bounded absolute Galois group. If F_0 is algebraically closed in F_1 then $F_0 \preceq F_1$.*

Note 3.11. This extends Théorème 5.11 in [3].

Proof. Note that $(\mathrm{acl}(F_0), F_0) \subset^{\#} (\mathrm{acl}(F_1), F_1)$ is full. Choose now saturated extensions $M_1 \succeq (\mathrm{acl}(F_1), F_1)$ and $M_2 \succeq (\mathrm{acl}(F_0), F_0)$ of the same cardinality. Observe that Id is a #-automorphism of $(\mathrm{acl}(F_0), F_0)$ in M_1 and M_2, which therefore extends by 3.8 to M_1 and M_2. Hence, it is now clear that $(\mathrm{acl}(F_0), F_0) \preceq (\mathrm{acl}(F_1), F_1)$. $\square$

{D:Lcts}

Definition 3.12. Consider the absolute Galois group fixed by the theory $T^{\#}$. For each n let $\tau(n)$ be the number of different extensions of degree n. Let L_c be an extension of $\mathrm{L}_{\text{rings}}$ by constants $\{c_{i,k,n}\}_{\substack{i\leq n,\, n\in N\\ k\leq\tau(n)}}$.

Given a model M of $T^{\#}$, extend F^M to a $\mathrm{L}_c^{\#}$-structure by interpreting the constant as some collection of representatives of the irreducible polyonomials of degree n giving the above extensions of degree n. This can be described by a set of formulae T_c extending $\mathrm{Th}_{\text{rings}}(F^M)$.

{L:Psfc}

Lemma 3.13. *T_c is model-complete.*

Proof. Let $(F_0, \bar{c}) \subset (F_1, \bar{c})$ be two models of T_c. We need only show that $(\mathrm{acl}(F_0), F_0) \preceq^{\#} (\mathrm{acl}(F_1), F_1)$ since $\bar{c}$ are in F_0. By 3.10 we need only show that $\mathrm{acl}(F_0) \cap F_1 = F_0$. Take α in $\mathrm{acl}(F_0) \cap F_1$. There is some polynomial of degree n described the a tuple in $\bar{c}$ with α as a root. But the polyonomial remains irreducible when considered as a polyonomial over F_1. Therefore $n = 1$ and α lies in F_0. □

{P:zoe}

Proposition 3.14. *(Proposition 5.16 in [3]) Every existential L_{ring}-formula is equivalent to a finite conjunctions of formulae of the form $\exists t f(\bar{x}, t) = 0$, where f is in $\mathbb{Z}[\bar{x}, y]$ modulo the theory of perfect PAC fields.*

{C:ftefibers}

Corollary 3.15. *Let F be a perfect PAC field with bounded absolute Galois group. Every definable set $S \subset F^n$ is the projection with finite fibers of some algebraic subset in F^{n+m}.*

Note 3.16. This is a generalization of Corollaire after 5.17 in [3], which proves hence Lemma 1.11.

Proof. We can see F as an L_c-structure. By model-completeness, the formula which defines S is equivalent to an existential formulae (remark that the parameters may come from $\bar{c}$), so we can apply Proposition 3.14 to cover it by an algebraic set defined by polynomials. A straight-forward modification yields an algebraic set in some cartesian power of F which projects onto S with finite fibers. □

4 Definable measure following Chatzidakis

4.1 Goal

We work in the language of rings. Varieties will be absolutely irreducible.

The goal is the following theorem. It says roughly that to a definable set, one can associate a dimension d and a measure μ, which approximately specify the cardinality of the set over finite fields. (d,μ) may depend on the field, but there are only finitely many possibilities.

{thm:approx}

Theorem 4.1. *Let $\phi(\bar{x},\bar{y})$ be a formula. Then there exists a constant $C>0$ and a finite set $D\subset\mathbb{N}\times\mathbb{Q}^{>0}\cup\{(0,0)\}$ such that for every finite field $\mathbb{F}_q$ and every $\bar{b}\in\mathbb{F}_q$, there is a $(d,\mu)\in D$ such that "$\phi(\mathbb{F}_q,\bar{b})$ has approximately $\mu\cdot q^d$ elements". More precisely:*

$$|\#\phi(\mathbb{F}_q,\bar{b})-\mu\cdot q^d|<C\cdot q^{d-\frac{1}{2}} \tag{4.1}$$ {eq:approx}

Moreover, for each $(d,\mu)\in D$ there is a formula $\psi_{(d,\mu)}(\bar{y})$ such that $\mathbb{F}_q\vDash\psi_{(d,\mu)}(\bar{b})$ implies (4.1) and for each $(\mathbb{F}_q,\bar{b})$, there is a $\psi_{(d,\mu)}(\bar{b})$ which is true.

Example 4.2. For $\phi(x)=x^3=1$, the set D is $\{(0,1),(0,3)\}$.

The proof will proceed in several steps, from very special formulas to very general ones.

4.2 Varieties

The theorem of Lang-Weil says:

Theorem 4.3. *For any variety V defined over a finite field, there is a constant C such that for any field $\mathbb{F}_q$ containing the parameters of V, we have*

$$|\#V(\mathbb{F}_q)-q^d|<C\cdot q^{d-\frac{1}{2}}.$$

C should not depend on the parameter of V. Is this true?

So if ϕ defines a variety, our theorem is true.

4.3 Algebraic sets

Let ϕ be a positive, quantifier free formula, let F be any field and take $\bar{b}\in F$. We would like to decompose $\phi(F,\bar{b})$ into irreducible components and take the highest dimension as dimension of ϕ and the number of components of highest dimension as measure of ϕ. However, for this to work, we need the irreducible components to be defined over F. So take the variety V defined by the polynomials of $\phi(\bar{x},\bar{b})$ and apply the following lemma:

{lemma:star}

Lemma 4.4. *Given a variety V defined over a field F, there is a variety V^* such that $V^*(F)=V(F)$ and all irreducible components ov V^* are defined over F.*

Proof. We start with the variety V and apply the following procedure:
Let $V = V_1 \cup \cdots \cup V_s$ be the decomposition of V into irreducible components.
Set $W_i := \bigcap_{\sigma \in \mathrm{Gal}} \sigma(V_i)$ and $V' := \bigcup W_i$.
Claim: $V'(F) = V(F)$.
Proof of the claim: "$\subset$" is clear. "$\supset$": If $\bar{a} \in V_i(F)$, then $\bar{a}$ is fixed by Gal, so $\sigma^{-1}(\bar{a}) \in V_i$ for any $\sigma \in \mathrm{Gal}$, so $\bar{a} \in \sigma(V_i)$, so $\bar{a} \in W_i$.

Now we apply the same procedure to V' again, until nothing changes anymore. This happens after a finite number of steps, because for each irreducible component V_i of V, either $\dim W_i < \dim V_i$ or $W_i = V_i$.

$W_i = V_i$ means that V_i is defined over F, so the final V (which we call V^* now) has indeed its irreducible components defined over F. □

Given a fixed finite field $\mathbb{F}_q$ and a fixed $a \in \mathbb{F}_q$, we get $V^* = V_1^* \cup \cdots \cup V_s^*$, and (4.1) holds for $d = \max \dim V_i^*$ and $\mu = \#\{i \mid \dim V_i^* = d\}$.

So it remains to check that for a fixed ϕ, we only get finitely many pairs (d, μ) and that the corresponding sets $S_{d,\mu}$ of (field, parameter) can be defined. We will do this using compacity: For each $(\mathbb{F}_q, \bar{b}) \in S_{d,\mu}$, we have to find a clopen neighbourhood $\theta_{q,\bar{b}}(\bar{y})$ entirely contained in $S_{d,\mu}$. (Being a neighbourhood of $(\mathbb{F}_q, \bar{b})$ means $\mathbb{F}_q \vDash \theta_{q,\bar{b}}(\bar{b})$, and being contained in $S_{d,\mu}$ means for any other $(\mathbb{F}_{q'}, \bar{b}')$ with $\mathbb{F}_{q'} \vDash \theta_{q,\bar{b}}(\bar{b}')$, equation 4.1 is true for (d, μ).) Then by compacity, finitely many of these neighbourhoods cover all (field $\times$ parameters).

Let $V^* = V_1^* \cup \cdots \cup V_s^*$ and (d, μ) be as above, let r be the maximal number of polynomials needed to define the V_i^* and let g be the maximal degree of these polynomials.

$\theta_{q,\bar{b}}(\bar{y})$ says: There exist s varieties $V_1, \ldots, V_s$ defined by polynomials at most r polynomials of degree at most g such that:

- $\bigcup V_i(\mathbb{F}_q) = \phi(\mathbb{F}_q, \bar{y})$
- $V_i \neq V_j$ for $i \neq j$
- $\dim(V_i) \leq d$.
- $\#\{i \mid \dim V_i = d\} = \mu$.

(To be able to say this, we have to be able to talk about the dimension. We also have to be able to say that an algebraic set is absolutely irreducible. Let's pretend we knew this is true.)

Obviousely, $\theta_{q,\bar{b}}(\bar{b})$ has the desired properties.

4.4 Quantifier-free sets

Replace $\neg f(\bar{x}, \bar{y}) = 0$ by $f(\bar{x}, \bar{y}) \cdot z = 1$. These two sets are in bijection.

4.5 Existential formulas with bounded fibers

Suppose $\phi(\bar{x}, \bar{y}) = \exists \bar{t}\colon \psi(\bar{x}, \bar{y}, \bar{t})$ where ψ is quantifier free and such that there is a bound N on the size of the fibers of $\psi(F) \to \phi(F)$ which is independent of F.

Define

$$\phi_{\geq n}(\bar{x}, \bar{y}) := \exists^{\geq n} \bar{t}\colon \psi(\bar{x}, \bar{y}, \bar{t}) = \underbrace{\exists \bar{t}_1 \ldots, \bar{t}_n\colon \bigwedge \psi(\bar{x}, \bar{y}, \bar{t}_i) \wedge \bigwedge \bar{t}_i \neq \bar{t}_j}_{\tilde{\psi}_{\geq n}(\bar{x}, \bar{y}, \bar{t}_1, \ldots, \bar{t}_n)}.$$

We already have our theorem for the $\tilde{\psi}_{\geq n}$ and we want to compute some (d, μ) for ϕ. In order to do that, fix a finite field $\mathbb{F}_q$ and a parameter $\bar{b} \in \mathbb{F}_q$. (To simplify notation, we will write $\#\theta$ for $\#\theta(\mathbb{F}_q, \bar{b})$ for any of our formulas.)

We take $d(\phi) = d(\psi)$ and forget all the $\tilde{\psi}_{\geq n}$ with $d(\tilde{\psi}_{\geq n}) < d(\psi)$. (So let's now pretend all $d(\tilde{\psi}_{\geq n})$ are equal.)

If the size of the fiber of $\psi \to \phi$ over a given point is m, then the size if the fiber of $\tilde{\psi}_{\geq n} \to \phi$ is $\frac{m!}{(m-n)!}$ if $m \geq n$ and 0 otherwise.

In particular, we have

$$\#\tilde{\psi}_{\geq n} = n! \cdot \#\phi_{=n} + \frac{(n+1)!}{1!} \#\phi_{=n+1} + \cdots + \frac{N!}{(N-n)!} \#\phi_{=N}$$

So we have expressed the cardinalities of the $\tilde{\psi}_{\geq n}$ in the cardinalities of the $\phi_{=m}$ using a triangular matrix with non-zero entries on the diagonal. This matrix is invertible over $\mathbb{Q}$, so we can finally express the cardinality of $\phi = \phi_{=1} \vee \cdots \vee \phi_{=N}$ in the cardinalities of the $\tilde{\psi}_{\geq n}$. We use this expression to compute $\mu(\phi)$ out of the $\mu(\tilde{\psi}_{\geq n})$. It is clear that for this μ, equation (4.1) holds.

Finally note that $d(\phi)$ and $\mu(\phi)$ only depends on the $\mu(\tilde{\psi}_{\geq n})$ but not on the specific field $\mathbb{F}_q$ and parameter $\bar{b}$, so we only get finitely many $(d(\phi), \mu(\phi))$, and these can be defined using the formulas that define the $(d(\tilde{\psi}_{\geq n}), \mu(\tilde{\psi}_{\geq n}))$.

4.6 General formulas

Any formula is, modulo the theory of pseudo-finite fields, equivalent to one treated in the previous section. Being equivalent modulo the theory of pseudo-finite fields means being equivalent in all but finitely many fields. This is enough to prove our theorem.

5 Теорема о полноте Чеботарева

In section we aim to study Cebotarev's proof of its density theorem in the case of function fields over a finite field to see later its relations with Hrushovski's approach to the measure for pseudo-finite fields. Basic algebraic number theory is required. We refer to [1] for further reading.

Let us fix some notation: R and S will denote integral domains, K and L fields, and p, q, $\mathfrak{p}$, $\mathfrak{q}$ prime ideals.

Consider the following diagramme:

$$\begin{array}{ccc} S & \longrightarrow & L \\ \uparrow & & \uparrow \\ R & \longrightarrow & K \end{array}$$

with L/K a finite Galois extension of group G, R an integrally closed subring in K and S the integral closure of R in L. Remember that a ring extension A/B is integral if for every x in A there exists a monic polynomial in $B[X]$ having x as a root.

Given a prime ideal p in R, Nagayama's Lemma ensures the existence of some $\mathfrak{p}$ in Spec_S *lying over* p (i.e. $\mathfrak{p} \cap R = p$). It is easy to see that $G = \mathrm{Gal}(L/K)$ fixes S setwise, so G acts on the set of prime ideals over p. Given such an ideal $\mathfrak{p}$, let $D_\mathfrak{p}$ be the set of elements in G fixing $\mathfrak{p}$. Observe that $D_{\mathfrak{p}^\sigma} = \sigma D_\mathfrak{p} \sigma^{-1}$.

Claim. *G acts transitively on the set of primes over p*

Proof. Let $\mathfrak{p}$ and $\mathfrak{q}$ be two such primes and suppose that for no σ in G $\mathfrak{p}$ is mapped to $\mathfrak{q}$. By localising over p we may assume that S/R is an integral extension of local rings. Remark that in this case p is maximal if and only if $\mathfrak{p}$ is (and simlilarly for $\mathfrak{q}$). Therefore, both $\mathfrak{p}$ and $\mathfrak{q}$ are maximal ideals. By assumption,

$$\mathfrak{p}^\sigma \neq \mathfrak{q}^\tau$$

for all σ and τ in G. By maximality, we have that $S = \mathfrak{p}^\sigma + \mathfrak{q}^\tau$. It follows from the chinese remainder theorem that there is some x in S with

$$\begin{aligned} x &\equiv 0 \mod \mathfrak{p}^\sigma\, \forall \sigma \in G \\ x &\equiv 1 \mod \mathfrak{q}^\tau\, \forall \tau \in G \end{aligned}$$

Compute now the norm of x relative to L/K. It follows that $N_{L/K}(x)$ is in $S \cap \mathfrak{p} = p$ but not in $\mathfrak{q}$. This yields the desired contradiction. □

Let p and $\mathfrak{p}$ be as above and define $L_0 = \mathrm{Fix}(D_\mathfrak{p})$. Let $S_0 = S \cap L_0$ be the algebraic closure of R in L_0. Observe that $\mathfrak{p}_0 = \mathfrak{p} \cap S_0$ lies over p. Let $\mathfrak{p} = \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the distinct primes of S lying over p (with $n = |G/D_\mathfrak{p}|$). Observe that $\mathfrak{p}$ is the unique prime lying over $\mathfrak{p}_0$: If there was another one, then it differs from $\mathfrak{p}$ by a Gal(L/L_0)-conjugate, which by definition fixes $\mathfrak{p}$. Furthermore, L_0 is the smallest such subfield of L with the above property.

Define now $\bar{K}$ (*resp.* $\bar{L}$) to be the fraction field of R/p (*resp.* $S/\mathfrak{p}$) and consider the following group homomorphism:

$$\begin{array}{ccc} D_{\mathfrak{p}} & \xrightarrow{\phi} & Aut(\bar{L}/\bar{K}) \\ \sigma & \longrightarrow & \bar{\sigma} \end{array}$$

where $\bar{\sigma}$ is the automorphism obtained from extending $\sigma \restriction S$ to $S/\mathfrak{p}$ and $\bar{L}$.

Let $I_{\mathfrak{p}}$ be the kernel of ϕ, i.e. $I_{\mathfrak{p}} = \{\sigma$ in G such that $\forall x \in S\ x^{\sigma} \equiv x \mod \mathfrak{p}\}$.

Proposition 5.1. *$\bar{L}/\bar{K}$ is normal and ϕ is a surjective map. Moreover, if $\bar{L}/\bar{K}$ is separable with $[\bar{L} : \bar{K}] = [L : L_0]$, then ϕ is an isomorphism.* {P:liftgal}

Proof. First, we show that $R/p = S_0/\mathfrak{p}_0$, which implies that the fraction field of $S_0/\mathfrak{p}_0$ is also $\bar{K}$. Let x in S. We need only show that there is some a in R with $x \equiv a \mod \mathfrak{p}_0$. Choose some system of representatives $Id = \sigma_1, \ldots, \sigma_n$ of $G/D_{\mathfrak{p}}$. Note that for $i \geq 2$, $\mathfrak{p} \neq \mathfrak{p}^{\sigma_i}$. Therefore, $\mathfrak{p}_0^{\sigma_i} = \mathfrak{p}^{\sigma_i} \cap L_0 \neq \mathfrak{p}_0$. By a similar reasoning as in the previous claim, we find some element y in S with

$$\begin{aligned} y &\equiv x \mod \mathfrak{p}_0 \\ y &\equiv 1 \mod \mathfrak{p}_0^{\sigma_i}\ i \geq 2 \end{aligned}$$

Again, $a = N_{L_0/K}(y)$ is in R and is congruent with $x \mod \mathfrak{p}_0$.

After localisation on p, we may assume that p and $\mathfrak{p}$ are maximal ideals. Let now $barx$ be in $\bar{L}$ and choose some preimage x in S. Consider f to be its irreducible polynomial over L_0. By integrality of the extension, we may assume that f has coefficients on S_0. Since L/K is Galois, let $x = x_1, \ldots, x_r$ be the roots of f in L. By considering the restriction modulo $\mathfrak{p}_0$ we observe that $\bar{x}$ is root of a polynomial over $\bar{K}$ with all roots in $\bar{L}$. So the extension $\bar{l}/\bar{K}$ is normal. Moreover, $[barK(\bar{x}) : \bar{K}] \leq \deg f \leq [L : L_0]$.

It follows from the above that the maximal separable extension E of $\bar{K}$ in $\bar{L}$ satisfies $[E : \bar{K}] \leq [L : L_0]$ (by the primitive element theorem). Note that Gal$(E/\bar{K})$ determines Gal$(\bar{L}/\bar{K})$, and the former is determined by the restriction modulo $\mathfrak{p}$ of the K-conjugates of x. Hence, ϕ is surjective.

If now $E = \bar{L}$ and $[\bar{L} : \bar{K}] = [L : L_0]$, then all inequalities above turned into equalities, so ϕ must be injective. $\square$

Now we want to study when it is the case that the conditions in Proposition 5.1 hold, i.e. when it is the case that $\bar{L} : \bar{K}$ is separable and $[\bar{L} : \bar{K}] = [L : L_0]$.

Let $L : K$ be separable and finite. By the primitive element theorem, there exists some α in L such that $L = K(\alpha)$. Let $f = \sum_{i=0}^{n} a_i X^i$ be its minimal polynomial. After multiplying by some factor, we may assume that f is in $R[X]$ (possible f is no longer monic). Note that $a_n^{n-1} f$ has an n^{th}-power as leading coefficient. After a suitable change of variables, we may assume that f is in $R[X]$ and monic.

Hence, we may assume that $L = K(\alpha)$, where α is integral over R and its irreducible polynomial f is defined over R. Let $\alpha_1, \ldots, \alpha_n$ be all its conjugates in $\bar{K}^{\text{sep}}$. Define the discriminant of f as

$$d = \operatorname{Disc}(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (\alpha_i - \alpha_j)$$

Note that d is in $K \cap S = R$ and $d \neq 0$ by separability.

{L:unit}

Lemma 5.2. *If d is a unity in R then $S = R[\alpha]$.*

Proof. We need only prove that $S \subset R[\alpha]$. Let β be in S. Since β is in L, we can find $a_0, \ldots, a_r$ in K such that

$$\beta = \sum_{i=0}^{r} a_i \alpha^i$$

Hence it suffices to show that the a_i's lie in R. Let $\sigma_1, \ldots, \sigma_n$ be all the embeddings of $K(\alpha)$ in $\bar{K}^{\text{sep}}$. We have that

$$\sigma_j(\beta) = \sum_{i=0}^{r} a_i \alpha_j^i$$

The above equations give a matrix with determinant d. Therefore, if d is a unit, we can solve β in terms of the α_j's by Cramer's rule. And since all quantitieslie in R so does β. $\square$

{D:galcover}

Definition 5.3. A diagramme

$$\begin{array}{ccc} R[\alpha] & \longrightarrow & K(\alpha) \\ \uparrow & & \uparrow \\ R & \longrightarrow & K \end{array}$$

is a galois cover if the extension $K(\alpha) : K$ is Galois and if $\operatorname{Disc}(f)$ is a unit in R.

{L:unitdisc}

Lemma 5.4. *Let*

$$\begin{array}{ccc} S & \longrightarrow & K(\alpha) \\ \uparrow & & \uparrow \\ R & \longrightarrow & K \end{array}$$

be given. Given p in $\operatorname{Spec}(R)$ *and $\mathfrak{P}$ over p in* $\operatorname{Spec}(S)$*, if* $\operatorname{Disc}(f)$ *does not belong to p, then $\bar{L} : \bar{K}$ is separable and $[\bar{L} : \bar{K}] = [L : L_0]$.*

We do not give the proof of the above lemma since it is not relevant for our purposes.

Hence, given the following:

$$\begin{array}{ccc} S & \longrightarrow & K(\alpha) \\ \uparrow & & \uparrow \\ R & \longrightarrow & K \end{array}$$

choose f monic in $R[X]$ irreducible with α as a root and let d be its discriminant. Consider the following diagramme:

$$\begin{array}{ccccc} S & \longrightarrow & R_1[\alpha] & \longrightarrow & K(\alpha) \\ \uparrow & & \uparrow & & \uparrow \\ R & \longrightarrow & R_1 & \longrightarrow & K \end{array} \tag{5.1}$$ {eq:localize}

where R_1 is the localisation of R at $\{d^n\}_{n\in\mathbb{Z}}$. So $R_1 \to R_1[\alpha]$ is a Galois cover. Since there is only a finite number of primes dividing (d) in case R is a Dedekind domain, we have only lost information about the behaviour of the epimorphism described in 5.1 for finitely many primes in $\mathrm{Spec}(R)$.

From now on, K will be a global field, i.e. a finite, separable extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$, and R will be the corresponding ring of integers, i.e. the integral closure of $\mathbb{Z}$ resp. $\mathbb{F}_q[t]$ in K. In particular, R is a Dedekind domain, and all prime ideals are maximal... with exception of the zero ideal. From now on, we will ignore that one.

In addition, L will be a Galois extension of K and, as usual, S will be the integral closure of R in L. Denote the Galois group of L/K by G. To underline our addiction to other languages, from now on prime ideals of R will be called ñ and prime ideals of S will be called ç.

To be able to state the theorem of Chebotarev, we need some more definitions:

Definition 5.5. For a prime ideal $\tilde{n} \in \mathrm{Spec}(R)$, let $N\tilde{n}$ denote the number of elements of the residue field $K_{\tilde{n}}$.

Note that $K_{\tilde{n}}$ is finite: ñ is maximal (Remember that we don't consider the zero ideal), so it lies over a maximal ideal p of $\mathbb{Z}$ resp. $\mathbb{F}_p[t]$. The residue field $\mathbb{Z}/p$ resp. $\mathbb{F}_q[t]/p$ is finite and $R/\tilde{n}$ is a finite extension of that field.

Definition 5.6. Let A be a subset of $\mathrm{Spec}(R)$. If the limit

$$\delta(A) := \lim_{s\to 1^+} \frac{\sum_{\tilde{n}\in A} N\tilde{n}^{-s}}{\sum_{\tilde{n}\in \mathrm{Spec}\, R} N\tilde{n}^{-s}}$$

exists, it is called the *Dirichlet densitiy* of A.

The last thing we need to define to be able to state the theorem is the Artin symbol. Suppose ç is an unramified extension of ñ. So in particular, $D_{ç} \cong$

$\mathrm{Gal}(L_ç/K_ç)$. Let *Frob* $\in \mathrm{Gal}(L_ç/K_ç)$ be the frobenius element, i.e. $x \mapsto x^{q'}$ if $K_ç \cong \mathbb{F}_{q'}$. (Btw: $q' = N$ñ.)

Define $[\frac{L/K}{ç}]$ to be the image of *Frob* in G. This has several nice properties:

- $[\frac{L/K}{ç}]$ is uniquely determined by:

$$\forall x \in L\colon [\frac{L/K}{ç}]x \equiv x^{q'} \mod ç.$$

- If K' is another field between K and L, K'/K being Galois, then

$$[\frac{L/K}{ç}] \restriction_{K'} = [\frac{K'/K}{ç \cap K'}].$$

- If $\sigma \in G$, then

$$[\frac{L/K}{\sigma(ç)}] = \sigma[\frac{L/K}{ç}]\sigma^{-1}.$$

By the last property, for different ideals ç over ñ, all $[\frac{L/K}{ç}]$ lie in the same conjugacy class of G. So we can define:

Definition 5.7. The Artin symbol of an ideal ñ is defined by $(\frac{L/K}{ñ}) = [\frac{L/K}{ç}]^G$.

And now, finally (drum roll):

Theorem 5.8 (Chebotarev density theorem). *Let $\mathcal{C}$ be a conjugacy class in G. Then the Dirichlet densitiy of $\left\{\tilde{n} \in \operatorname{Spec} R \mid (\frac{L/K}{\tilde{n}}) = \mathcal{C}\right\}$ exists and is equal to $\frac{|C|}{|G|}$.*

Note 5.9. The Artin symbol was only defined in the unramified case. However, we saw that there are only finitely many ramified prime ideals, and the Dirichlet densitiy doesn't depend on finitely many elements. So the theorem makes sense. (To be more precise, one would have to replace R by a localized ring R_1 as in 5.1.)

And our reason for doing all this is the following:

{C:non-empty}

Corollary 5.10. $\left\{\tilde{n} \in \operatorname{Spec} R \mid (\frac{L/K}{\tilde{n}}) = \mathcal{C}\right\}$ *is not empty.*

6 Uniqueness of Hrushovki's measure

{S:non-empty}

In this section, we will use the techniques exhibited in the proof of Corollary 5.10 in the case of function fields over a finite field to prove the following result:

{T:non-empty}

Theorem 6.1. *Let K a perfect PAC field with cyclic absolute Galois group, V an absolutely irreducible variety defined over K and $V \to W$ a Galois cover. Given a conjugation class $C \subset G$ of order $n < \omega$, then $X(V \to W, C) \neq \emptyset$ if and only if* $\mathrm{Gal}(K)$ *has a quotient of order n.*

Recall that given a Galois cover $V \to W$, we defined in 1.12 the set

$$X(V \to W, C) = \{w \in W(K) \,|\, \mathrm{Artin}(w) \in C\}.$$

Proof. Assume that $\mathrm{Gal}(K)$ has a quotient of order n and let $V \to W$ be as above. Fix some c_0 in C of order n. By assumption and the primitive element theorem, there is some α in $\bar{K}$ such that $K(\alpha)/K$ is a cyclic extension of order n. Let p in $K[X]$ be the minimal polynomial of α. Consider the following algebraic set $U = \{x \,|\, p(x) = 0\}$. Define $V' = V \times U$. Then

$$\begin{tikzcd} V \times U \arrow[dr, "\pi_1"] & \\ & V \end{tikzcd}$$

is a Galois cover with group $\mathrm{Gal}(K(\alpha)/K)$.

Consider now the following diagramme:

$$\begin{tikzcd} V \times U \arrow[dd] \arrow[dr, "\pi_1"] & \\ & V \arrow[dl] \\ W & \end{tikzcd}$$

with the composite map. Then $V' = V \times U \to W$ is a Galois cover with group $G \times \mathrm{Gal}(K(\alpha)/K)$. Choose a generator σ of $\mathrm{Gal}(K)$ and denote by $\bar{\sigma}$ its reduction to $\mathrm{Gal}(K(\alpha)/K)$. Set $C' = \{(c, \sigma) \,|\, c \in C\}$. Note that $C' \subset G'$ is a conjugation class since $\mathrm{Gal}(K(\alpha)/K)$ is cyclic, hence abelian. Moreover, $X(V \to W, C) = X(V' \to W, C')$, since

$w \in X(V \to W, C) \Longleftrightarrow \exists\ v$ over w and $v^\sigma = c \cdot v \Longleftrightarrow \exists\ (v, \beta)$ in V' over w and $(v, \beta)^\sigma = (c, \bar{\sigma}) \cdot (v, \beta)$

Fix now some $d = (c_0, \bar{\sigma})$ in C' and define $W' = V'/\langle d \rangle$. Note that d has also order n. Hence, $V' \to W'$ is a Galois cover with group $\langle d \rangle$. Moreover,

W' is irreducible, defined over K and $\dim(W') = \dim(V')$. Show now that if $X(V' \to W', \{d\}) \neq \emptyset$ then $X(V' \to W, C') \neq \emptyset$.

GIven w' in $X(V' \to W', \{d\})$, there is some $v' \in V'$ over w' with

$$(v')^\sigma = d \cdot v'$$

Hence, $\pi(v')$ is in $X(W' \to W, C')$.

Therefore, we need only show that $X(V' \to W', \{d\}) \neq \emptyset$. We will show that $W'(K) = X(V' \to W', \{d\})$ and use the PAC property to conclude the claim. Let $w' \in W'(K)$. Choose some $v' = (v, \beta)$ over w'. The fiber over w' equals $\{(\bar{c}_0^n \cdot v, \bar{\sigma}^n \beta)\}$. Remark that $\{\bar{\sigma}^n \cdot \beta\}$ gives us back U. Since $(v')^\sigma$ lies in the fiber, we conclude that:

$$\begin{aligned} v^\sigma &= c_0 \cdot v \\ \bar{\sigma} \cdot \beta &= \bar{\sigma} \cdot \beta \end{aligned}$$

So, $(v')^\sigma = d \cdot v'$.

Suppose now that $X(V \to W, C) \neq \emptyset$. Choose w in $W(K)$ and v_0 in V over w such that $v_0^{\sigma^{-1}} = c \cdot v_0$ with $c \in C$. Define now

$$\begin{array}{ccc} \mathrm{Gal}(K) & \longrightarrow & G \\ \tau & \longrightarrow & f(\tau) \end{array}$$

such that $v_0^{\tau^{-1}} = f(\tau) \cdot v_0$. Now that f defines a continous group homomorphism (where G is equipped with the discrete topology). Moreover, $f(\sigma) = c$. Hence, we have a surjection

$$\mathrm{Gal}(K) \quad \longrightarrow \quad \langle c \rangle \simeq (\mathbb{Z}/n\mathbb{Z})$$

So $\mathrm{Gal}(K)$ has a quotient of order n. $\square$

7 Measures for procyclic groups

{S:procyclic}

In this section we hope to define a measure for a perfect PAC fields K with a procyclic galois group Gal (i.e. $Gal \subset \hat{\mathbb{Z}}$).

This measure μ must verify the following properties : let X, Y be definable sets in K.

- $\mu(X \dot{\cup} Y) = \mu(X) + \mu(Y)$.
- $\mu(X \times Y) = \mu(X) \cdot \mu(Y)$.
- if $X \overset{1:1}{\to} Y$ then $\mu(X) = \mu(Y)$.
- $\mu(X) = 1$ if X is an absolute irreducible variety.

Moreover, we would like that if $(V \to W, G)$ is a Galois cover and C a conjugation class, then $\mu(X(V \to W), C)$ depends only of C and G. So, we will try to define for a given procyclic galois group Gal, a function $\mu_G(C)$ for any finite group G and any conjugation class C such that if the measure μ given by $\mu(X(V \to W), C) := \mu_G(C)$ will be well defined and will satisfy the above properties.

Example 7.1.

- If Gal $= \hat{\mathbb{Z}}$ then $\mu_G(C) = |C|/|G|$.
- If Gal $= \{id\}$ then by Theorem 6.1, $\mu_G(C) = 0$ for $C \neq \{id\}$ and $\mu_G(\{id\}) = 1$

{exS3}

Example 7.2. Suppose that $G = S_3$.

	{id}	{(12),(13),(23)}	{(123),(132)}
$Gal = \hat{\mathbb{Z}}$	1/6	1/2	1/3
$Gal = \mathbb{Z}_2$	?	?	0
$Gal = \mathbb{Z}_3$	?	0	?

In the case of $\mathbb{Z}_2$, $\mu_{S_3}(\{(123),(132)\}) = 0$ since $\mathbb{Z}_2$ doesn't have a quotient of order 3 (Theorem 6.1). In the same way, for $\mathbb{Z}_3$, $\mu_{S_3}(\{(12),(13),(23)\}) = 0$.

Now, suppose that we have measures wich verify the above properties. The following lemmas will able us to complete Example 7.2.

{mucyclique}

Lemma 7.3. *If $G = \mathbb{Z}/m\mathbb{Z}$ then all non-zero $\mu_G(C)$ are equal.*

Proof. Consider the Galois cover $(V \to W, \mathbb{Z}/m\mathbb{Z})$:

$$\begin{array}{ccc} V = K^* & \to & W = K^* \\ a & \mapsto & a^m \end{array}.$$

Then for any $g \in Z/m\mathbb{Z}$, $X(V \to W, \{g\})$ is empty or equal to $\{ba^m : a \in K^*\}$ for a given $b \in K^*$. Thus the non-empty $X(V \to W, \{g\})$ are definably isomorphic. $\square$

Lemma 7.4. *Let $\pi : G \to G'$ be a surjective morphism and let C' be a conjugation class of G'. Then $\mu_{G'}(C') = \mu_G(\pi^{-1}(C))$.* {musurjective}

Proof. Consider the following diagram of the Galois covers $(V \to W, G)$ and $(V' to W, G')$:

$$\begin{tikzcd} V \arrow[dd, "f"'] \arrow[dr] & \\ & V' = V/\ker\pi \arrow[dl, "f'"] \\ W & \end{tikzcd}$$

Then $X(V' \to W, C') = X(V \to W, \pi^{-1}(C))$. Indeed: let $w \in W(K)$. Then $w \in X(V' \to W, C')$, if and only if there is $v' \in f'^{-1}(w)$ such that there is $c' \in C'$ with $\sigma(v') = c'v'$, if and only if there is $v \in f^{-1}(w)$ such that there is $c' \in C'$ with $\sigma(\ker\pi \cdot v) = c' \ker\pi \cdot v$, if and only if there is $v \in f^{-1}(w)$ such that there is $c \in \pi^{-1}(C)$ with $\sigma(v) = cv$, if and only if $w \in X(V \to W, \pi^{-1}(C))$. $\square$

Now, we are able to compute μ_{S_3} for $Gal = \mathbb{Z}_2$. Consider the surjective morphism : $S_3 \to \mathbb{Z}/2\mathbb{Z}$. By Lemma 7.3, $\mu_{\mathbb{Z}/2\mathbb{Z}}(0) = \mu_{\mathbb{Z}/2\mathbb{Z}}(1) = 1/2$. Thus, by Lemma 7.4, $\mu_{S_3}(\{(12),(13),(23)\}) = \mu_{\mathbb{Z}/2\mathbb{Z}}(1) = 1/2$ and $\mu_{S_3}(\{id,(123),(132)\}) = \mu_{\mathbb{Z}/2\mathbb{Z}}(0 = 1/2$.

Lemma 7.5. *Let $G_1 \subset G_2$. Let C_1 be a conjugation class of G_1 such that for any $c \in C_1$, $C_{G_2}(c) \subset G_1$. Let $C_2 := C_1^{G_2}$. Then* {muinclusion}

$$\mu_{G_1}(C_1) = \mu_{G_2}(C_2).$$

Proof.
Consider the following diagram of the Galois covers $(V \to W, G_2)$ and $(V \to W = V/G_1', G_1)$:

$$\begin{tikzcd} V \arrow[d, "f_1"'] \arrow[dr, "f_2"] & \\ W' \arrow[r, "\phi"] & W \end{tikzcd}$$

Then ϕ induces a surjective map from $X(V \to W', C_1)$ onto $X(V \to W, C_2)$: let $w \in X(V \to W, C_2)$. Then there is $v \in f_2^{-1}(w)$ and $c_2 \in C_2$ such that $\sigma(v) = c_2 v$. Since $C_2 = C_1^{G_2}$, one can choose v sucht that $c_2 \in C_1$. Then $f_1(v) = G_1 v \in W'(K)$ since $\sigma(G_1 v) = G_1 v$ and thus, $f_1(v) \in X(V \to W', C_1)$.

Claim. *Let $(V \to W, G)$ a Galois cover. Let $c \in C$ a conjugation class of G and $w \in W$ such that* Artin(w) = C *then*

$$\#\{v \in f^{-1}(w) : \sigma(v) = cv\} = |G|/|C|.$$

Proof. For any $c' = c^g \in C$, $\{v \in f^{-1}(w) : \sigma(v) = c'v\} = \{gv \in V : v \in f^{-1}(w) \& \sigma(v) = cv\}$ and so has the same cardinality than $\{v \in f^{-1}(w) : \sigma(v) = cv\}$. Since $|f^{-1}(w)| = |G|$, the claim follows. $\square$

Let $c \in C_1$, $w \in X(V \to W, C_2)$ and $w' \in X(V \to W', C_1)$. Then

$$\#\{v \in f_2^{-1}(w) : \sigma(v) = cv\} = |G_2|/|C_2|$$

and

$$\#\{v \in f_1^{-1}(w') : \sigma(v) = cv\} = |G_1|/|C_1|.$$

Thus

$$|\phi^{-1}(w)| = (|G_2|/|C_2|)(|C_1|/|G_1|) = |C_{G_2(c)}|/|C_{G_1(c)}| = 1.$$

So,

$$X(V \to W', C_1) \xrightarrow{1:1} X(V \to W, C_2).$$

$\square$

Now, we compute μ_{S_3} for $Gal = \mathbb{Z}_3$: consider $A_3 \subset S_3$. Let $C_1 = \{(123)\}$ and $C_2 = C_1^{S_3} = \{(123), (132)\}$. Note that $C_{S_3}((123)) = A_3$. By Lemma 7.5 and Lemma 7.3, $\mu_{S_3}(C_2) = \mu_{A_3}(C_1) = 1/3$.

In conclusion, we obtain the following tabular for Example 7.2:

	{id}	{(12),(13),(23)}	{(123),(132)}
$Gal = \hat{\mathbb{Z}}$	1/6	1/2	1/3
$Gal = \mathbb{Z}_2$	1/2	1/2	0
$Gal = \mathbb{Z}_3$	2/3	0	1/3

References

[1] M. Fried, M. Jarden, *Field Arithmetic*, **Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge**, vol. **11**, 2^{nd} ed, 2005.

[2] E. Hrushovski, *Pseudo-finite fields and related structures*,in Model theory and applications, Quad. Mat.,**11**, 151–212, Aracne, Rome, 2002.

[3] Z. Chatzidakis, *Théorie des modèles des corps finis et pseudo-finis*, Cours de $3^{\text{ème}}$ cycle, to be found at http://www.logique.jussieu.fr/www.zoe/