Characterisation of pseudo-finite fields and decidability of Psf

Eric Osterkamp

Seminar *Model Theory of Pseudofinite Structures*

5 May 2021

Preliminaries

Notation 1.

- $\mathcal{L}$ the language of Rings
- T_f theory of all finite fields
- Psf theory of pseudo-finite fields
- T_{prime} theory of all prime fields
- Psf_0 theory of pseudo-finite fields of characteristic 0

Goals today:

- Characterise pseudo-finite fields.
- Further investigate Psf to expand tool set.
- Sketch decidability of Psf.

Characterisation

- We want to show pseudofinite fields are exactly the infinite models of T_f.
- Alongside: Pseudofinite fields of characteristic 0 are exactly the infinite models of T_{prime}.
- Most of the work has already been done.

Starting off with the easy direction.

Lemma 2.

1. Any infinite model of T_f is elementarily equivalent to a non-principal ultraproduct of finite fields.
2. Any infinite model of T_{prime} is elementarily equivalent to a non-principal ultra-product of prime fields.

Proof:

- We show 1.
- Let $M \models T_f$ be infinite, and let I be the set of all sentences true in M.
- If $\phi \in I$, then $\neg\phi \notin T_f$, i.e. there exists some finite field M_ϕ such that $M_\phi \models \phi$.
- For each $\psi \in I$ let

$$X_\psi := \{\phi \in I \mid M_\phi \models \psi\}.$$

- The set $\mathcal{B} := \{X_\psi \mid \psi \in I\}$ is a filter base.
- By Zorn's Lemma we can extend $\mathcal{B}$ to an Ultrafilter $\mathcal{U}$ on I.
- Then by Łoś's theorem

$$M \equiv \prod_{\phi \in I} M_\phi/\mathcal{U}.$$

- Clearly non-principal. □

We have shown the following in the second talk.

Theorem 3.

Let $\mathcal{Q}$ be the set of all prime powers, and let $\mathcal{U}$ be a non-principal ultrafilter on $\mathcal{Q}$. Then the field $F^* = \prod_{q \in \mathcal{Q}} \mathbb{F}_q / \mathcal{U}$ is a pseudo-finite field.

But we are mostly interested in its proof. In particular we can apply this proof to the ultraproduct constructed in the proof of Lemma 2.

Theorem 4.

Any infinite model of T_f or T_{prime} is a pseudo-finite field.

Proof:

- By Lemma 2 and the proof of Theorem 3.

□

One direction done. The following result is immediate by Łoś's theorem.

Lemma 5.

1. A non-principal ultraproduct of finite fields is a model of T_f.
2. A non-principal ultraproduct of prime fields is a model of T_{prime}.

The following notion was noted during the last talk.

Definition 6.

- If K is a field, and $k_0 \subseteq K$ the prime field of K, then the *(field of) absolute numbers* of K is the field $k_0^{\text{alg}} \cap K$.
- We write $Abs(K)$ to denote the field of absolute numbers of K.

Before we can apply the main result from the last talk and finish up the characterisation we need the following Lemma.

Lemma 7.

Let $k_0 = \mathbb{F}_p$ or $k_0 = \mathbb{Q}$, and let $E \subseteq k_0^{\text{alg}}$ have at most one extension of each degree. Then there is an ultraproduct F^* of finite fields such that

$$Abs(F^*) \cong E.$$

When the characteristic of E is 0, then F^* can be chosen to be an ultraproduct of prime fields.

Proof:
Case 1 (E is finite of characteristic p):

- Let $q := |E|$, and $\mathcal{U}$ be an arbitrary non-principal ultrafilter on $\mathcal{P}$.

$$F^* := \prod_{m \in \mathcal{P}} \mathbb{F}_{q^m}/\mathcal{U}.$$

- By Łoś's theorem F^* has characteristic p, F^* contains a copy of $\mathbb{F}_q$, and F^* does not contain any copys of $\mathbb{F}_{q^d}$ for $1 < d \in \mathbb{N}$.

Case 2 (E is infinite of characteristic p):

- Let $(n_i)_{i\in\mathbb{N}}$ such that
$$\mathbb{F}_{p^{n_i}} = E \cap \mathbb{F}_{p^{i!}}.$$
- $n_i \mid (n_{i+1})$ for each $i \in \mathbb{N}$.
- Let $\mathcal{U}$ be an arbitrary non-principal ultrafilter on $\mathbb{N}$, and set
$$F^* := \prod_{i\in\mathbb{N}} \mathbb{F}_{p^{n_i}} /\mathcal{U}.$$
- $char(F^*) = p$.
- If $\mathbb{F}_{p^d} \subseteq E$, then $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{n_i}}$ for all $i \geq d$, and F^* contains a copy of $\mathbb{F}_{p^d}$
- If $\mathbb{F}_{p^d} \not\subseteq E$, then $\mathbb{F}_{p^d} \not\subseteq \mathbb{F}_{p^{n_i}}$ for all $i \in \mathbb{N}$, and F^* does not contain a copy of $\mathbb{F}_{p^d}$.
- Note by construction
$$E = \bigcup_{i\in\mathbb{N}} \mathbb{F}_{p^{n_i}}.$$

Case 3 (E is of characteristic 0):

- We write $\mathbb{Q}^{\text{alg}}$ as the union of an increasing chain L_n, $n \in \mathbb{N}$, of finite Galois extensions of $\mathbb{Q}$.
- For each n let
$$E_n := L_n \cap E.$$
- Let $I(n)$ be the set of subfields of L_n which properly contain E_n.
- Choose some generator α of E_n over $\mathbb{Q}$, and let $f_n(T)$ be its (monic!) minimal polynomial over $\mathbb{Q}$.
- For each $M \in I(n)$ choose a generator β_M of M over $\mathbb{Q}$, and let $g_M(T)$ be its minimal polynomial over $\mathbb{Q}$.
- Set
$$g_n(T) := \prod_{M \in I(n)} g_M(T).$$

- Consider
$$\theta_n := \exists t.f_n(t) \doteq 0 \wedge \forall t.g_n(t) \neq 0.$$
- For any field E' of characteristic 0 with prime field K, and K^{alg} written as a union of an increasing chain $L'_n \cong L_n$, $n \in \mathbb{N}$, of finite Galois extensions of K
$$E' \models \bigwedge_{i=0}^{n} \theta_i \implies E' \cap L'_n \cong E_n.$$
- Now consider the sets
$$A_n := \{p \in \mathcal{P} \mid \mathbb{F}_p \models \bigwedge_{i=0}^{n} \theta_i\}.$$

Claim:

For all $n \in \mathbb{N}$ the set A_n is infinite.

For the proof the of claim we will need the following result.

Corollary 8 (Tchebotarev).

Let $f_0(T), ..., f_m(T), g(T) \in \mathbb{Z}[T]$, T a single variable. Let L be the Galois extension of $\mathbb{Q}$ obtained by adjoining all roots of the polynomials $f_i(T)$, $i \in \{0, ..., m\}$, and $g(T)$. Assume there is a subfield E of L such that $Gal(L/E)$ is cyclic and

$$E \models \bigwedge_{i=0}^{m} \exists t.f_i(t) \doteq 0 \wedge \forall t.g(t) \neq 0.$$

Then the set of prime numbers p such that

$$\mathbb{F}_p \models \bigwedge_{i=0}^{m} \exists t.f_i(t) \doteq 0 \wedge \forall t.g(t) \neq 0.$$

is infinite.

Proof of Claim:

- Fix some arbitrary $n \in \mathbb{N}$, and let

$$g(T) := \prod_{i=0}^{n} g_n(T).$$

- There exist $f_0'(T), f_1'(T), ..., f_n'(T), g'(T) \in \mathbb{Z}[T]$ such that

$$f_i(t) = 0 \Leftrightarrow f_i'(t) = 0 \text{ for } i \in \{0, ..., n\} \quad \text{and} \quad g(t) = 0 \Leftrightarrow g'(t) = 0.$$

- The Galois extension of $\mathbb{Q}$ obtained by adjoining all roots of the polynomials $f_i'(T)$, $i \in \{1, ..., n\}$, and $g'(T)$ equals L_n.
- Since $E_n \models \theta_i$ for $i \in \{0, ..., n\}$,

$$E_n \models \bigwedge_{i=0}^{n} \exists t. f_i'(t) \doteq 0 \wedge \forall t. g'(t) \not\doteq 0.$$

We need the following result from Galois theory to show the group $Gal(L_n/E_n)$ is cyclic.

Lemma 9.

Let F be a perfect field with at most one extension of every degree, and L an algebraic extension of F of degree m. Then

$$Gal(L/F) \cong \mathbb{Z}/m\mathbb{Z}.$$

- Since L_nE is an algebraic extension of E, the Lemma implies $Gal(L_nE/E)$ is cyclic.
- Thus $Gal(L_nE_n/E_n) = Gal(L_n/E_n)$ is cyclic.
- We are done by Tchebotarev. □(Claim)

- We have shown: For all $n \in \mathbb{N}$ the set A_n is infinite.
- The set
$$\mathcal{A} := \{A_n \mid n \in \mathbb{N}\}$$
is a filter base.
- Extend to a non-principal ultrafilter $\mathcal{U}$ on $\mathcal{P}$.
- For each n by Łoś's theorem
$$F^* := \prod_{p \in \mathcal{P}} \mathbb{F}_p/\mathcal{U} \models \bigwedge_{i=0}^{n} \theta_i.$$
- We have shown: For any field E' of characteristic 0 with prime field K, and K^{alg} written as a union of an increasing chain $L'_n \cong L_n$, $n \in \mathbb{N}$, of finite Galois extensions of K
$$E' \models \bigwedge_{i=0}^{n} \theta_i \implies E' \cap L'_n \cong E_n.$$

Recall the main result from last talk.

Theorem 10.

Let E and F be pseudo-finite fields. Then

$$E \equiv F \iff Abs(E) \cong Abs(F).$$

Bringing it together.

Theorem 11.

1. The pseudo-finite fields are exactly the infinite models of T_f.
2. The pseudo-finite fields of characteristic 0 are exactly the infinite models of T_{prime}.

Proof:

- Again we just show 1.

- It suffices to show if F is a pseudo-finite field, then there exists an ultraproduct F^* of finite fields such that

$$F^* \equiv F.$$

- But by Theorem 10 this is equivalent to showing the existence of an ultraproduct F^* of finite fields such that

$$Abs(F^*) \cong Abs(F).$$

- So let k_0 denote the prime field of F.
- Since F is a pseudo-finite field, $Abs(F)$ has at most one extension of every degree.
- Since $Abs(F) \subseteq k_0^{alg}$, we are done by Lemma 7.

□

Consequences

- Every finite field can be equipped with a measure.
- The ultraproduct of these measures might define something interesting on a pseudo-finite field F.
- We will see how it works in the next two talks.
- In preparation we further investigate Psf.
- The developed tools will also enable us to show decidabilty of Psf.

Psf

We are interested in quantifier reduction and model completeness.

Theorem 12 (Quantifier reduction).

Modulo the theory Psf any formula $\varphi(\overline{x})$ is equivalent to a Boolean combination of formulas of the form

$$\exists t.f(\overline{x}, t) \doteq 0,$$

where $f(\overline{X}, T) \in \mathbb{Z}[\overline{X}, T]$.

For the proof we do need two more results.

Firstly a known result from model theory.

Lemma 13.

Let T be a theory, and $\varphi(\overline{x})$ a formula such that $T \cup \{\exists \overline{x}.\varphi(\overline{x})\}$ is consistent. Let Δ be a set of formulas in the variables $\overline{x}$ which is closed under disjunctions. The following conditions are equivalent:

1. There are formulas $\psi_1(\overline{x}), ..., \psi_m(\overline{x}) \in \Delta$ such that

$$T \vdash \forall \overline{x}.[\varphi(\overline{x}) \leftrightarrow (\psi_1(\overline{x}) \wedge ... \wedge \psi_m(\overline{x}))].$$

2. Whenever A and B are models of T, and $\overline{a}, \overline{b}$ are tuples in A, B respectively, if $A \models \varphi(\overline{a})$ and every formula $\psi(\overline{x}) \in \Delta$ which is satisfied by $\overline{a}$ in A is also satisfied by $\overline{b}$ in B, then $B \models \varphi(\overline{b})$.

For the proof of Theorem 12 we want to show the second condition.

Secondly we can obtain a more general version of a result from the last talk. We omit the proof by request.

Theorem 14.

Let E and F be pseudo-finite fields, and K_1 a subfield of E and K_2 a subfield of F. Assume we have an isomorphism ψ between K_1 and K_2. Then

$$(E, a)_{a \in K_1} \equiv (F, \psi(a))_{a \in K_1} \iff \text{there is } \psi' \supseteq \psi \text{ such that } \psi'(E \cap K_1^{alg}) = F \cap K_2^{alg}.$$

This will find application in the proof of the second condition.

Proof of Theorem 12:

- Fix some arbitrary formula $\varphi(\overline{x})$.
- If $\mathrm{Psf} \cup \{\exists \overline{x}.\varphi(\overline{x})\}$ is inconsistent, then $\varphi(\overline{x})$ is equivalent modulo Psf to $\exists t.1 \doteq 0$.
- So assume $\mathrm{Psf} \cup \{\exists \overline{x}.\varphi(\overline{x})\}$ is consistent.
- Let E, F be pseudo-finite fields, and Δ the set of Boolean combinations of formulas of the form $\exists t.f(\overline{x}, t) \doteq 0$, where $f(\overline{X}, T) \in \mathbb{Z}[\overline{X}, T]$.
- Δ is closed under disjunctions.

Claim:

If $E \models \varphi(\overline{a})$ for $\overline{a} \in E$, and if for some $\overline{b} \in F$ every formula $\psi(\overline{x}) \in \Delta$ which is satisfied by $\overline{a}$ in E is also satisfied by $\overline{b}$ in F, then $F \models \varphi(\overline{b})$.

Proof of Claim:

- Since $\exists t.p \doteq 0 \in \Delta$, E and F have isomorphic prime subfields k_E and k_F respectively.

- Since $\overline{a}$ and $\overline{b}$ satisfy the same equations over $\mathbb{Z}$, there exists an isomorphism ψ between (the subrings) $k_E[\overline{a}]$ and $k_F[\overline{b}]$.
- We can extend ψ to an isomorphism ψ' between (the subfields) $k_E(\overline{a})$ and $k_F(\overline{b})$.
- But for any $f(\overline{a}, T) \in k_E[\overline{a}][T]$

$$E \models \exists t.f(\overline{a}, t) \doteq 0 \iff F \models \exists t.f(\overline{b}, t) \doteq 0.$$

- Thus we can extend ψ' to an isomorphism

$$\psi'' : E \cap k_E(\overline{a})^{\text{alg}} \to F \cap k_E(\overline{b})^{\text{alg}}.$$

- Now the claim follows by Theorem 14. □(Claim)
- Since $\varphi(\overline{x})$ was arbitrary, by the Claim and Lemma 13 we are done. □

Definition 15 (Model completeness).

We call a theory T *model complete* if for all models M_1 and M_2 of T

$$M_1 \subseteq M_2 \implies M_1 \prec M_2.$$

Consider the following.

Definition 16 (Psf_c).

We set

$$\mathcal{L}_c := \mathcal{L} \cup \{c_{i,n} \mid 2 \leq n \in \mathbb{N}, 1 \leq i \leq n\}.$$

The $\mathcal{L}_c$-theory Psf_c is obtained by adding to the theory Psf for each n an axiom stating the irreducibility of the polynomial

$$X^n + \sum_{i=1}^{n} c_{i,n} X^{n-i}.$$

Lemma 17.

Every pseudo-finite field expands to a model of Psf_c.

- Let F be a pseudo-finite field.
- For each $n \in \mathbb{N}$ let α_n be a generator of the unique extension of degree n, and $f_n(T)$ be its (monic!) minimal polynomial

$$T^n + \sum_{i=1}^{n} y_{i,n} T^{n-i}.$$

- Set $c_{i,n} := y_{i,n}$. □

Recall the following result from last talk.

Corollary 18.

Let $E \subseteq F$ be pseudo-finite fields. Then

$$E \prec F \iff E^{\mathrm{alg}} \cap F = E.$$

Theorem 19 (Model completeness).

The theory Psf_c is model complete.

Proof:

- Let $E \subseteq F$ be models of Psf_c, and fix an arbitrary algebraic extension L of E of degree n.
- L is generated over E by a solution of the equation

$$X^n + \sum_{i=1}^{n} c_{i,n} X^{n-i} \doteq 0.$$

- But since $F \models \mathrm{Psf}_c$, this polynomial is irreducible over F, i.e. $L \cap F = E$.
- Since L was chosen arbitrarily,

$$E^{\mathrm{alg}} \cap F = E.$$

We will see the following result being used for the definition of a measure on pseudo-finite fields. It is not necessary for said definition, but it does shine in its application.

Theorem 20.

Let F be a pseudo-finite field, and $S \subseteq F^n$ be definable. Then there is an algebraic set $W \subseteq F^{n+m}$ such that, if $\pi : F^{n+m} \to F^n$ is the natural projection, then $\pi(W) = S$, and for each $y \in S$ the fiber $\pi^{-1}(y) \cap W$ is finite.

Proof:

- Let S be $\emptyset$-definable by an $\mathcal{L}$-formula $\varphi(\overline{x})$.
- Expand F to a model of Psf_c.
- By model completeness there exists an existential $\mathcal{L}_c$-formula $\psi(\overline{x})$ such that $\varphi(\overline{x})$ is equivalent to $\psi(\overline{x})$ modulo Psf_c.
- Since any inequation $x \neq 0$ is equivalent to $\exists y.xy \doteq 1$ modulo the theory of fields, we may assume $\psi(\overline{x})$ to be positive.
- By Boolean logic some algebraic set $W \in F^{n+m}$ such that $\pi(W) = S$ exists.
- We need to show W can be chosen such that the second statement is met.

Claim.

The formula $\varphi(\overline{x})$ is equivalent modulo Psf_c to a conjunction of disjunctions of positive existential formulas $\exists \overline{y}.\psi_i(\overline{x},\overline{y})$ where for any parameters $\overline{a} \in F$ the set of elements satisfying $\psi_i(\overline{x},\overline{a}) \doteq 0$ is finite.

- If we show the claim, we are done. Indeed, consider

$$\exists \overline{y}.f_0(\overline{x},\overline{y}) \doteq \ldots \doteq f_k(\overline{x},\overline{y}) \doteq 0 \text{ and } \exists \overline{z}.g_0(\overline{x},\overline{z}) \doteq \ldots \doteq g_l(\overline{x},\overline{z}) \doteq 0.$$

- Their conjunction is logically equivalent to

$$\exists \overline{y},\overline{z}.f_0(\overline{x},\overline{y}) \doteq \ldots \doteq f_k(\overline{x},\overline{y}) \doteq g_0(\overline{x},\overline{z}) \doteq \ldots \doteq g_l(\overline{x},\overline{z}) \doteq 0.$$

- Their disjunction is equivalent modulo the theory of fields to

$$\exists \overline{y},\overline{z}. \bigwedge_{i,j} f_i(\overline{x},\overline{y})g_j(\overline{x},\overline{z}) \doteq 0.$$

Proof of Claim:

- S is definable by a Boolean combination of formulas

$$\exists t.f(\overline{x}, t) \doteq 0,$$

  where $f(\overline{X}, T) \in \mathbb{Z}[\overline{X}, T]$.
- S is definable by a conjunction of disjunctions of $\mathcal{L}$-formulas φ_i.

Case 1 ($\varphi_i(\overline{x}) = \exists t.f(\overline{x}, t) \doteq 0$):

- For some $\overline{x} \in F^n$ the polynomial $f(\overline{x}, T)$ might be constantly 0.
- Write $f(\overline{X}, T) = \sum_j f_j(\overline{X})T^j$.
- $\varphi_i(\overline{x})$ is equivalent to

$$\bigwedge_j f_j(\overline{x}) \doteq 0 \quad \vee \quad \exists t, u. \left(f(\overline{x}, t) \doteq 0 \wedge \prod_j (f_j(\overline{x}) \cdot u) - 1 \doteq 0 \right).$$

Case 2 ($\varphi_i(\overline{x}) = \forall t.f(\overline{x}, t) \neq \dot{0}$):

- As in Case 1 we have to catch the case where $f(\overline{x}, T)$ is constant for some $\overline{x} \in F^n$.
- Express its constant coefficient is invertible and every other coefficient equals 0.
- Assume $f(\overline{x}, T)$ is not constant, and let k be the degree of $f(\overline{x}, T)$ in T.
- F does not contain a root of this polynomial if and only if the Galois extension L of F of degree $k!$ the polynomial $f(\overline{x}, T)$ can be written

$$\prod_{l=1}^{k}(T - a_l),$$

  where $a_l \notin F$.
- Second talk: Existence of an existential formula $\rho(\overline{x})$ expressing this utilising the interpretation of L in F. Interprete L in F using the constants $(c_{i,n})_{n \leq k!}$. □(Claim)

- Let S be definable by some $\varphi(\overline{x}, \overline{a})$, where $|\overline{x}| = n, |\overline{a}| = l$ for some constants $\overline{a} \in F$, and $\varphi(\overline{x}, \overline{y})$ is without parameters.
- Let S' denote the set defined by $\varphi(\overline{x}, \overline{y})$.
- There exists an algebraic set $W \subseteq F^{n+l+m}$ such that, if $\pi : F^{n+l+m} \to F^{n+l}$ is the natural projection, then $\pi(W) = S'$, and for each $y \in S'$ the fiber $\pi^{-1}(y) \cap W$ is finite.
- The fibre $W_{\overline{a}}$ of W over $\overline{a}$ fullfills the requirements of the algebraic set.

□

Decidability

We tackle decidability. A consequence of the first section is the following.

Corollary 21.

$$\mathrm{Psf} \subseteq \mathrm{Psf}_0 \subseteq T_{\mathrm{prime}} \quad \text{and} \quad \mathrm{Psf} \subseteq T_f \subseteq T_{\mathrm{prime}}.$$

We will utilise it sketching the proof of the following.

Theorem 22.

The following theories are decidable.

1. Psf_0.
2. Psf.
3. T_f.
4. T_{prime}.

Sketch of the proof:

- We have to show there is an algorithm which decides, given a sentence θ, whether it is true in all pseudo-finite fields or not.
- The second talk introduced an algorithm to axiomatise Psf.
- Recall the following introduced in the second talk.

Theorem 23 (Hermann).

1. There is a constant $A = A(n, d)$ such that for every field F, polynomials $f_1, ..., f_m, g \in F[\overline{X}]_{\leq d}$, if g belongs to the ideal of $F[\overline{X}]$ generated by $f_1, ..., f_m$, then there are $h_1, ..., h_m \in F[\overline{X}]_{\leq A}$ such that $g = \Sigma_{i=1}^{m} f_i h_i$.
2. There is a constant $D = D(n, d)$ such that for every field F and ideal I of $F[X]$ generated by elements of $F[X]_{\leq d}$, if I is not prime, then there are $g, h \in F[X]_{\leq D}$ such that $gh \in I$ but $g, h \notin I$.

- The algorithm relied on these constants.

- These constants are effectively computable, and thus each axiom in the scheme.
- Interesting: There is a more efficient way to compute the PAC axioms utilising the following result.

Theorem 24.

Let L be an algebraic extension of an infinite field K. Suppose every plane curve defined over K has an L-rational point. Then L is PAC.

Axiom 25 (PAC).

Every polynomial in $K[x, y]$ which is irreducible in $K^{\text{alg}}[x, y]$ has a zero in K^2.

- If f is not irreducible, then $f = gh$ with g and h having smaller total degree than f.
- The bound for polynomials we have to check is hence bounded by the degree of f.

- Either way, we have an enumeration of a set Γ consisting of axioms for the theory Psf.
- Hence we can produce an enumeration of the set of all proofs made using axioms of Γ.
- Hence we can produce an enumeration of Psf (by completeness).
- Similarly we have an enumeration for axioms of the theory Psf_0 $\Gamma_0 = \Gamma \cup \{p \neq \dot{0} \mid p \text{ prime}\}$, and of Psf_0.
- Fix some arbitrary $\mathcal{L}$-sentence θ.
- If θ is in Psf or Psf_0, then we will find it in these respective enumerations.
- Let $(\psi_n)_{n\in\mathbb{N}}$ be an enumeration of all $\mathcal{L}$-sentences which are Boolean combinations of the form

$$\exists t.f(t) \doteq \dot{0},$$

where $f(T) \in \mathbb{Z}[T]$.

- Then $\Gamma \vdash \theta \leftrightarrow \psi_n$ for some n by quantifier reduction.
- Thus $\theta \leftrightarrow \psi_n \in \mathrm{Psf}$, and we can effectively find it.
- It suffices to decide if ψ_n holds or does not hold in arbitrary pseudo-finite fields.
- But since every witness to ψ_n is algebraic over the prime field, the truth of ψ_n only depends on $Abs(F)$.
- Hence to show the truth of ψ_n in any pseudo-finite field it suffices to show for any prime field k, and any $E \subseteq k^{\mathrm{alg}}$ with at most one algebraic extension of any degree

$$E \models \psi_n.$$

Now recall the following.

Theorem 26 (Lang-Weil).

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

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

In particular, if $q > C^2$, then any variety V as above will have a rational point in $\mathbb{F}_q$.

1. We decide whether θ holds in Psf_0 or not:
   - ψ_n is equivalent to a disjunction of sentences of the form

$$\bigwedge_i \exists t.f_i(t) \doteq 0 \wedge \forall t.g(t) \not\doteq 0,$$

     where $f_i(T), g(T) \in \mathbb{Z}[T]$ for all i.
   - Let L be the extension of $\mathbb{Q}$ generated by all roots of polynomials in ψ_n.
   - By Galois theory ψ_n holds in some $E \subseteq L$ such that $Gal(L/E)$ is cyclic if and only if it holds in some $E' \subseteq \mathbb{Q}^{\mathrm{alg}}$ such that $Gal(\mathbb{Q}^{\mathrm{alg}}/E')$ is cyclic.
   - But the computation of $Gal(L/\mathbb{Q})$ and the subfields E of L such that $Gal(L/E)$ is cyclic is effective.
   - Moreover, deciding whether or not ψ_n is true in all subfields E of L such that $Gal(L/E)$ is cyclic is effective.

2. We decide whether θ holds in Psf or not:
   - We can procede as in 1., and if $\psi_n \notin \mathrm{Psf}_0$, then $\psi_n \notin \mathrm{Psf}$.
   - Assume $\psi_n \in \mathrm{Psf}_0$.
   - Then ψ_n is provable from Γ_0, and its proof uses finitely many axioms stating the characteristic is not p.
   - Thus there exists a constant C_2 such that ψ_n holds in all pseudo-finite fields of characteristic $p' > C_2$.
   - For a fixed p let $\mathbb{F}_{p^m}$ be the extension generated by all roots of polynomials appearing in ψ_n.
   - In a similar argument to 1. it suffices to check whether ψ_n is true in $\mathbb{F}_{p^b}$ or not for all b dividing m.

3. We decide whether θ holds in T_f or not:
   - We can procede as in 2., and if $\psi_n \notin \mathrm{Psf}$, then $\psi_n \notin T_f$.
   - So let $\psi_n \in \mathrm{Psf}$.
   - Then θ can be proven from Γ by finitely many axioms stating PAC.
   - Thus by Lang-Weil we can effectively compute a constant C_3 such that

     $$T_f \cup \{\text{there are at least } C_3 \text{ elements}\}$$

     proves θ.
   - Checking whether θ holds in the (finitely many) fields of size $< C_3$ is decidable.

4. We decide whether θ holds in T_{prime} or not:
   - We can procede as in 1., and if $\psi_n \notin \text{Psf}_0$, then $\psi_n \notin T_{\text{prime}}$.
   - So let $\theta \in \text{Psf}_0$.
   - Then θ can be proven from Γ_0 by a finite amount of axioms stating the characteristic is not p, and PAC.
   - Hence by Lang-Weil we can effectively compute a constant C_4 such that
   $$T_{\text{prime}} \cup \{p \neq 0 \mid p < C_4\}$$
   proves θ.
   - Checking whether θ holds in the finitely many prime fields of size $< C_4$ is decidable.

□