Characterisation of pseudo-finite fields and decidability of Psf

Introduction

In this talk we will apply the main result from the last talk. We will first establish the characterisation of the pseudo-finite fields as the infinite models of the theory T_f of all finite fields. This result motivates the following talks and in preparation we will further investigate Psf. Closing we will sketch the proof of the decidability of Psf, Psf_0, T_f, and T_{prime}.

Preliminaries

Notation 1. Throughout we work in the language $\mathcal{L}$ of Rings. We denote by T_f the theory of all finite fields, by T_{prime} the theory of all prime fields, by Psf the theory of pseudo-finite fields, and by Psf_0 the theory of pseudo-finite fields of characteristic 0.

Characterisation of pseudo-finite fields

We want to show pseudofinite fields are exactly the infinite models of T_f. And we will show a strong result alongside: Pseudofinite fields of characteristic 0 are exactly the infinite models of T_{prime}.

Lemma 2 ([Cha05, Example 1.29])**.**

(i) Any infinite model of T_f is elementarily equivalent to a non-principal ultraproduct of finite fields.

(ii) Any infinite model of T_{prime} is elementarily equivalent to a non-principal ultraproduct of prime fields.

Proof. We show (i). 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

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

Then the set $\mathcal{B} \coloneqq \{X_\psi \mid \psi \in I\}$ is a filter base. Indeed, for each $\psi \in I$ the set X_ψ is non-empty by construction, and if $X_{\varphi_1}, X_{\varphi_2} \in \mathcal{B}$, then by the closure under finite conjunctions of I

$$X_{\varphi_1 \wedge \varphi_2} \in \mathcal{B} \quad \text{and} \quad X_{\varphi_1 \wedge \varphi_2} \subseteq X_{\varphi_1} \cap X_{\varphi_2}.$$

By Zorn's Lemma we can extend $\mathcal{B}$ to an Ultrafilter $\mathcal{U}$ on I. Then

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

by Łoś's theorem. Since a principal ultraproduct of finite fields is finite, the ultraproduct is non-principal. □

Recall (the proof of) the following result from the second talk.

Theorem 3 ([Cha05, Theorem 6.4])**.** *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.*

Lemma 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. □

We tackle the other direction. The following result is immediate by Łoś's theorem.

Lemma 5.

(i) A non-principal ultraproduct of finite fields is a model of T_f.

(ii) A non-principal ultraproduct of prime fields is a model of T_{prime}.

Now we need to do some work.

Definition 6 (Field of absolute numbers)**.** 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.

Lemma 7 ([Cha09, Theorem 4.10]). *Let $k_0 = \mathbb{F}_p$ or $k_0 = \mathbb{Q}$, and let $E \subseteq k_0^{alg}$ 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 infinite of characteristic p). Let $(n_i)_{i\in\mathbb{N}}$ such that

$$\mathbb{F}_{p^{n_i}} = E \cap \mathbb{F}_{p^{i!}}.$$

Then $n_i \mid (n_{i+1})$ for each $i \in \mathbb{N}$. Let $\mathcal{U}$ be an arbitrary non-principal ultrafilter on $\mathbb{N}$, and set

$$F^* \coloneqq \prod_{i\in\mathbb{N}} \mathbb{F}_{p^{n_i}}/\mathcal{U}.$$

Claim 1. *$Abs(F^*) \cong E$.*

Proof of Claim. By Łoś's theorem $char(F^*) = p$. Let $d \in \mathbb{N}$. 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 $\mathbb{F}_{p^d}$ by Łoś's theorem. 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 $\mathbb{F}_{p^d}$ by Łoś's theorem. Since

$$E = \bigcup_{i\in\mathbb{N}} \mathbb{F}_{p^{n_i}},$$

we are done. □

Case 2 (E is finite of characteristic p). Let $q \coloneqq |E|$, and $\mathcal{U}$ be an arbitrary non-principal ultrafilter on $\mathcal{P}$. We set

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

Then 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 $1 < d \in \mathbb{N}$. Hence $Abs(F^*) \cong E$.

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

$$E_n \coloneqq L_n \cap E,$$

and let $I(n)$ be the (finite!) set of subfields of L_n which properly contain E_n. We will find a sentence which describes 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

$$g_n(T) \coloneqq \prod_{M\in I(n)} g_M(T).$$

Consider

$$\theta_n \coloneqq \exists t.f_n(t) \doteq 0 \wedge \forall t.g_n(t) \neq 0.$$

Claim 2. *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*

$$E' \models \bigwedge_{i=0}^{n} \theta_i \implies E' \cap L'_n \cong E_n.$$

Proof of Claim. By construction. □

Now consider the sets

$$A_n := \{p \in \mathcal{P} \mid \mathbb{F}_p \models \bigwedge_{i=0}^{n} \theta_i\}.$$

Claim 3. *For all $n \in \mathbb{N}$ the set A_n is infinite.*

We will make use of the following consequence of Tchebotarev's Theorem.

Corollary 8. *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 $n \in \mathbb{N}$. 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

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

and 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 $i \in \{0, ..., n\}$,

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

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

Lemma 9 ([Cha09, Comment 3.6])**.** *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, Lemma 9 implies $Gal(L_nE/E)$ is cyclic. Thus $Gal(L_nE_n/E_n) = Gal(L_n/E_n)$ is cyclic. Now the Claim follows by Corollary 8. □

Since $A_{n-1} \subseteq A_n$ for $n \in \mathbb{N} - \{0\}$, by Claim 3 the set

$$\mathcal{A} \coloneqq \{A_n \mid n \in \mathbb{N}\}$$

is a filter base, and can be extended to a non-principal ultrafilter $\mathcal{U}$ on $\mathcal{P}$. For each n by Łoś's theorem

$$F^* \coloneqq \prod_{p \in \mathcal{P}} \mathbb{F}_p/\mathcal{U} \models \bigwedge_{i=0}^{n} \theta_i.$$

By Claim 2: $Abs(F^*) \cong E$.

□

Recall the main result from last talk.

Theorem 10 ([Cha05, Theorem 6.14])**.** *Let E and F be pseudo-finite fields. Then*

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

Theorem 11 ([Cha05, Theorem 6.18])**.**

(i) The pseudo-finite fields are exactly the infinite models of T_f.

(ii) The pseudo-finite fields of characteristic 0 are exactly the infinite models of T_{prime}.

Proof. We show (i). By Lemma 4 and Lemma 5 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

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

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

"This implies every pseudo-finite field elementarily embeds into an ultraproduct of finite fields. Now, every finite field can be equipped with a measure (the counting measure), and one would think that the ultraproduct of these measures might define something interesting on a pseudo-finite field F. It turns out that this is the case", and we will see next talk how it works. In preparation we will further investigate Psf.

Psf

We are interested in quantifier reduction and model completeness.

Theorem 12 ([Cha05, Theorem 6.15])**.** *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 $f(\overline{X},T) \in \mathbb{Z}[\overline{X},T]$.

The proof requires two results. Firstly a known result from model theory.

Lemma 13 ([Cha05, Corollary 1.4])**.** *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:*

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

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

(ii) 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 $B \models \varphi(\overline{b})$.

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

Theorem 14 ([Cha05, Theorem 6.13'])**.** *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*

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

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 $f(\overline{X},T) \in \mathbb{Z}[\overline{X},T]$. Then 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 the same characteristic. Thus 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 $k_F[\overline{b}]$, and 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

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

Now the claim follows by Theorem 14. □

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

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

Definition 16 (Psf_c)**.** We set

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

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 ([Cha09, Theorem 5.3])**.** *Every pseudo-finite field expands to a model of Psf_c.*

Proof. 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

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

Then set $c_{i,n} \coloneqq y_{i,n}$. □

Recall the following result from last talk.

Corollary 18 ([Cha05, Corollary 6.12])**.** *Let $E \subseteq F$ be pseudo-finite fields. Then*

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

Theorem 19 ([Cha05, Theorem 6.16])**.** *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. Then 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,

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

By Corollary 18 model completeness of Psf_c follows. □

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 ([Cha05, Theorem 6.17])**.** *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 $\varphi(\overline{x})$. By Lemma 17 we can 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. Hence 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.*

Proof of Claim. By Theorem 12 the set S is definable by a Boolean combination of formulas

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

where $f(\overline{X}, T) \in \mathbb{Z}[\overline{X}, T]$. By Boolean logic 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 $f(\overline{X}, T) = \sum_j f_j(\overline{X})T^j$. Then $\varphi_i(\overline{x})$ 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 ($\varphi_i(\overline{x}) = \forall t.f(\overline{x}, t) \neq 0$)**.** As in Case 1 we have to catch the case where $f(\overline{x}, T)$ is constant for some $\overline{x} \in F^n$, i.e. its constant coefficient is invertible and every other coefficient equals 0. So assume $f(\overline{x}, T)$ is not constant, and let k be the degree of $f(\overline{x}, T)$ in T. Then F does not contain a root of this polynomial if and only if adding a root of this polynomial defines a proper extension of F 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 $a_l \notin F$. But we have already seen the existence of an existential formula $\rho(\overline{x})$ expressing this in the second talk utilising the interpretation of L in F. If we interprete L in F using the constants $(c_{i,n})_{n \leq k!}$, then we are done.

By Boolean logic the Claim follows. □

We note for two formulas

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

their conjunction is logically equivalent to

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

and their disjunction is equivalent modulo the theory of fields to

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

Then we are done by the Claim.

For the general case let the set 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 $\varphi(\overline{x}, \overline{y})$. By the $\emptyset$-definable case 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. Then the fibre $W_{\overline{a}}$ of W over $\overline{a}$ fullfills the requirements of the algebraic set. □

On decidability

Corollary 21.

$$Psf \subseteq Psf_0 \subseteq T_{prime} \quad and \quad Psf \subseteq T_f \subseteq T_{prime}.$$

Proof. Immediate by Theorem 11. □

Theorem 22. *The following theories are decidable.*

(i) Psf_0.

(ii) Psf.

(iii) T_f.

(iv) T_{prime}.

Sketch of 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. Recall this result introduced in the second talk.

Theorem 23 (Hermann, [Cha05, Theorem 5.2])**.**

(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 introduced to axiomatise Psf in the second talk relied on these constants, and while those are effectively computable, and thus each axiom in the scheme, we can make it more efficient utilising the following.

Theorem 24 ([FJ08, Theorem 11.2.3])**.** *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.*

A consequence is the axiom stating PAC for a field K becomes the following.

Axiom 25. 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, and we can produce an enumeration of the set of all proofs made using axioms of Γ. As a direct consequence of the completeness theorem, we can thus produce an enumeration of Psf. Similarly we have an enumeration for axioms of the theory Psf_0 $\Gamma_0 = \Gamma \cup \{p \neq 0 \mid p \text{ prime}\}$, 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. Since our algorithm needs to terminate, we have to show $\theta \notin \text{Psf}$ and $\theta \notin \text{Psf}_0$ is effectively computable.

Let $(\psi_n)_{n\in\mathbb{N}}$ be an enumeration of all $\mathcal{L}$-sentences which are Boolean combinations of the form

$$\exists t.f(t) \doteq 0,$$

where $f(T) \in \mathbb{Z}[T]$. Then $\Gamma \vdash \theta \leftrightarrow \psi_n$ for some n by Theorem 12. 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 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 $\mathbb{F}_q$.

(i). By Boolean logic and Theorem 12 the $\mathcal{L}$-sentence 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. Then the computation of $Gal(L/\mathbb{Q})$ and the subfields E of L such that $Gal(L/E)$ is cyclic is effective. Thus we can decide whether or not ψ_n is true in all subfields E of L such that $Gal(L/E)$ is cyclic.
Since 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, we have decided whether $\psi_n \in \mathrm{Psf}_0$ or not.

(ii). We can procede as in (i). If $\psi_n \notin \mathrm{Psf}_0$, then $\psi_n \notin \mathrm{Psf}$ by Corollary 21. So let $\psi_n \in \mathrm{Psf}_0$. 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 $p' > C_2$. Fix such a p.
Let $\mathbb{F}_{p^m}$ be the extension generated by all roots of polynomials appearing in ψ_n. In a similar argument to (i) it suffices to check whether $\mathbb{F}_{p^l} \models \psi_n$ for all l dividing m.

(iii). We can procede as in (ii). If $\psi_n \notin \mathrm{Psf}$, then $\psi_n \notin T_f$ by Corollary 21. 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.

(iv). We can procede as in (i). If $\psi_n \notin \mathrm{Psf}_0$, then $\psi_n \notin T_{\mathrm{prime}}$ by Corollary 21. So let $\theta \in \mathrm{Psf}_0$. 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

$$T_{\mathrm{prime}} \cup \{p \neq 0 \mid p < C_4\}$$

proves θ. Checking whether θ holds in the finitely many prime fields of size $< C_4$ is decidable.

□

References

[Ax68] James Ax, "The Elementary Theory of Finite Fields", *Annals of Mathematics* 88.2 (1968), pp. 239–271.

[Bos13] Siegfried Bosch, *Algebra*, 8th ed., Springer Spektrum, 2013.

[Cha05] Zoé Chatzidakis, *Notes on the model theory of finite and pseudo-finite fields*, Course Notes, Nov. 2005.

[Cha09] Zoé Chatzidakis, *Notes on the model theory of finite and pseudo-finite fields*, Course Notes, Apr. 2009.

[CDM92] Zoé Chatzidakis, Lou van den Dries, and Angus Macintyre, "Definable sets over finite fields.", *Journal für die reine und angewandte Mathematik* 427 (1992), pp. 107–136.

[FJ08] Michael D. Fried and Moshe Jarden, *Field Arithmetic*, 3rd ed., Springer, Berlin, Heidelberg, 2008.

[TZ12] Katrin Tent and Martin Ziegler, *A Course in Model Theory*, Lecture Notes in Logic, Cambridge University Press, 2012.