Independence in (unbounded) PAC fields, and imaginaries

Zoé Chatzidakis*(CNRS - Université Paris 7)

30 June 2008
Around Classification Theory, Leeds

1 Definition and some early results

Definition 1.1. A *pseudo-algebraically closed* field (*PAC*), is a field F such that every absolutely irreducible variety defined over F, has an F-rational point.

Recall that an irreducible variety over F is defined as the zero-set of a prime ideal in a polynomial ring over F; if this prime ideal generates a prime ideal in the polynomial ring over the algebraic closure F^{alg} of F, then the variety is absolutely irreducible. The property of being PAC is first-order axiomatisable.

1.2. A bit of history PAC fields first appeared in the work of Ax [A] in the late 60's on pseudo-finite fields. Recall that a pseudo-finite field is an infinite model of the thepry of finite fields. The axiomatisation of their theory is given by expressing in a first order way the fact that the field F is

– PAC,

– perfect, i.e., if F is of positive characteristic p, then every element of F has a p-th root in F,

– and its absolute Galois group, $\mathrm{Aut}(F^{alg}/F) = \mathcal{G}(F)$, is isomorphic to $\hat{Z} = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z}$, the profinite completion of $\mathbb{Z}$.

Ax's results in particular implied the decidability of the theory of pseudo-finite fields, as well as a good description of definable sets and of the completions.

Later results on PAC fields dealt with relaxing the conditions on the Galois group, and really paved the road for the subsequent developments; first appeared results analogous to those of Ax for e-free PAC fields (Jarden and Kiehne [JK]), and ω-free PAC fields (Jarden [J]). The final word came in the work of Cherlin, Van den Dries and Macintyre, (unfortunately still unpublished, but see [CDM]) which completely described the elementary invariants of PAC fields. In order to do that, they introduced an ω-sorted logic, in which one can speak about profinite groups in a first-order way. Results in that direction were also obtained by Ershov, see [E1] and [E2]. More details on the logic of profinite groups below 2.1.

*partially supported by MRTN-CT-2004-512234 and by ANR-06-BLAN-0183

1.3. Some definitions on Galois groups. Recall that a field is called *bounded* if for any integer n, it has only finitely many Galois extensions of degree n.

Given a free group $F(X)$ on a set X, one can form the *free profinite group* on X has follows: consider the family $\mathcal{N}$ of normal subgroups N of $F(X)$ which are of finite index and contain almost all the elements of X, and define

$$\hat{F}(X) = \lim_{N \in \mathcal{N}} F(X)/N.$$

When $|X| = e \in \omega$, one usually writes $\hat{F}_e$, and when $|X| = \aleph_0$, one writes $\hat{F}_\omega$.

A field F is *e-free* if its absolute Galois group is isomorphic to $\hat{F}_e$, and *ω-free* if it has an elementary substructure with absolute Galois group isomorphic to $\hat{F}_\omega$.

1.4. More history. At almost the same time, Duret ([Du]) proved the first result with a stability theoretic flavour on PAC fields: he showed that if a PAC field is not separably closed, then it has the independence property. [Recall that a field F is *separably closed* if any irreducible polynomial $f(X)$ over F is of the form $X^{p^n} - a$ for some integer n and element a of F.]

Then came a finer description of definable sets in pseudo-finite fields ([ChDM]), which in particular showed that pseudo-finite fields did not have the strict order property. Later work by Hrushovski (manuscript in 1991, published in [H]) developped the theory of S1-rank for bounded PAC fields, showed that they satisfy the independence theorem and eliminate imaginaries (provided one adds enough constants to the language). His results led to the observation that any complete theory of pseudo-finite fields is supersimple of SU-rank 1: these were the first examples of fields with a supersimple theory.

Other results: Pillay and Poizat ([PP]) showed that fields with a good notion of rank are perfect and bounded. Jarden ([J]) and Chatzidakis and Hrushovski ([CH]) showed that perfect PAC fields are *algebraically bounded.* Algebraic boundedness is a notion introduced by Van den Dries [vdD], and which implies in particular, that taking the algebraic dimension of the Zariski closure of a definable set, gives a good notion of dimension on definable sets.

There is also a good description of the algebraic closure ([CP]): if F is a PAC field, and $A \subset F$, then A is algebraically closed in the sense of the theory of F if and only if F/A is a regular extension (in characteristic 0, this simply means that $A^{alg} \cap F = A$).

2 Elementary invariants: the results of Cherlin, Van den Dries and Macintyre

All results in this section are from [CDM]. See also Ershov's papers [E1] amd [E2].

2.1. Galois groups and their complete systems. Let F be a field. Then its absolute Galois group, $\mathcal{G}(F)$, is a profinite group,

$$\mathcal{G}(F) \simeq \lim_{\leftarrow} \mathcal{G}al(L/F),$$

where L ranges over the set of all finite Galois extensions of F, and if $L \subset M$, one considers the natural restrictions map $\mathcal{G}al(M/F) \to \mathcal{G}al(L/K)$. $\mathcal{G}(F)$ is therefore a topological group, and is completely determined by the *complete system* of its finite quotients and the restriction maps between them. We define the complete system of $\mathcal{G}(F)$, noted by $S\mathcal{G}(F)$, by

$$S\mathcal{G}(F) = \biguplus \mathcal{G}al(L/F).$$

We assign to elements of $S\mathcal{G}(F)$ *sorts* indexed by the positive integers: $\sigma \in \mathcal{G}al(L/F)$ is of sort n if and only if $[L : F] \leq n$. We put on $S\mathcal{G}(F)$ an $\mathcal{L}_G$-structure, (with sorts the positive integers), in such a way that $S\mathcal{G}(F)$ can be viewed as a modular lattice, each node of the lattice being a finite group; and we put enough information to have the group law on each node, as well as the projection maps between nodes. This procedure works for arbitrary profinite groups, and the complete systems of profinite groups then form an elementary class in this language. [It is however unknown whether the class of complete systems arising from absolute Galois groups is elementary: the only thing we know is that it is closed under ultraproducts.]

A *subsystem* of $S\mathcal{G}(F)$ then corresponds, by duality, to a quotient of $\mathcal{G}(F)$, i.e., by Galois theory, to $\mathcal{G}al(M/F)$ for some (maybe infinite) Galois extension of F.

2.2. Interpretation of finite field extensions. Let F be a field, and L a finite algebraic extension of F, with $L = F(\alpha)$ for some element α. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be the minimal (monic) polynomial of α over F. One can then define on F^n, uniformly in the tuple $(a_1, \ldots, a_n)$, a multiplication law $\odot$, such that

$$(b_0, \ldots, b_{n-1}) \mapsto \sum_{i=0}^{n-1} b_i\alpha^i$$

defines an isomorphism between $(F^n, +, \odot)$ and $(L, +, \cdot)$ (the addition on F^n being the natural F-vector space addition). The uniformity implies that one can quantify over all algebraic extensions of degree $\leq n$.

Note that it is then an elementary property of $(a_1, \ldots, a_n)$ that the extension L is Galois over F (simply say that $f(X)$ has n distinct roots in L). An element σ of $\mathcal{G}al(L/F)$ is then an automorphism of F^n which commutes with $\odot$.

From these simple remarks, it follows easily that, given an $\mathcal{L}_G$-sentence θ, one can produce a sentence θ^* of the langage of fields, such that in any field F,

$$S\mathcal{G}(F) \models \theta \iff F \models \theta^*.$$

2.3. Comments (1) This logic is the strongest logic of absolute Galois groups of fields which is interpretable in the field.

(2) The tuple $(a_1, \ldots, a_n)$ is then a code for the extension $L = F(\alpha)$. Consider the set S of n-tuples $(a_1, \ldots, a_n) \in F^n$ such that the polynomial $X^n + \sum_{i=0}^{n-1} a_{n-i}X^i$ is the minimal polynomial of a generator of a Galois extension of F; then one has a definable equivalence relation on S: $(a_1, \ldots, a_n) \sim (b_1, \ldots, b_n)$ if and only if the extension of F obtained by adjoining a root of $X^n + \sum_{i=0}^{n-1} a_{n-i}X^i$ contains all the roots of $X^n + \sum_{i=0}^{n-1} b_{n-i}X^i$. One can therefore think of finite Galois extensions of F as imaginary elements. Similarly, if $\sigma \in \mathcal{G}al(L/F)$, then the conjugacy class of σ belongs to $\mathrm{dcl}^{eq}(F)$.

2.4. Theorem. Let K_1 and K_2 be PAC fields, containing a common subfield E, and such that the extensions K_1/E and K_2/E are regular. Assume that $[K_1 : K_1^p] = [K_2 : K_2^p]$. Then

$$K_1 \equiv_E K_2 \iff S\mathcal{G}(K_1) \equiv_{S\mathcal{G}(E)} S\mathcal{G}(K_2).$$

Comments. (1) Recall that K_1/E regular implies that the restriction map $\mathcal{G}(K_1) \to \mathcal{G}(E)$ is onto; it then induces, by duality, an inclusion $S\mathcal{G}(E) \to S\mathcal{G}(K_1)$. There is a version of this result which does not assume the extensions to be regular: one then requires the existence of some $\varphi \in \mathcal{G}(E)$ such that $\varphi(E^{alg} \cap K_1) = E^{alg} \cap K_2$, and such that the induced automorphism Φ of $S\mathcal{G}(E)$, defines a partial elementary map $S\mathcal{G}(K_1) \to S\mathcal{G}(K_2)$.

(2) The left-to-right implication always holds.

(3) One can show that the theory of graphs is interpretable in the $\mathcal{L}_G$-theory of systems of absolute Galois groups of PAC fields ([E2], [CDM]). It then follows that the theory of PAC fields is undecidable. Similarly, if $\mathcal{C}$ is a class of PAC fields such that the associated class of complete systems has a decidable theory, then $\mathcal{C}$ has a decidable theory. The class of Frobenius fields is such an example, see [HL]

3 More stability flavoured results

The results of the previous section already showed that the Galois groups were sole responsible for complicated behaviour of PAC fields. Below, we first discuss two simple examples:

3.1. Back to bounded PAC fields. Let F be a bounded PAC field. Then for each n, $S\mathcal{G}(F)$ has only finitely many elements of sort n. Thus, the complete system of a bounded absolute Galois group is the equivalent of a "finite structure" - no surprise it behaves well.

If K_1 is bounded, and $K_1 \prec K_2$, then $K_1^s K_2 = K_2^s$, where K_i^s denotes the separable closure of K_i.

3.2. A nice theory of unbounded PAC. Among the nice possible absolute Galois groups, is $\hat{F}_\omega$, see 2.1 for the definition. A PAC field such that $S\mathcal{G}(F) \equiv S\hat{F}_\omega$, is called an ω-free PAC field.

Some properties (see [CDM]): Th$(S\hat{F}_\omega)$ is $\aleph_0$-categorical and ω-stable. $S\hat{F}_\omega$ has good homogeneity properties, which give a relative elimination of quantifiers, a good description of definable sets and of types. It also yields a simple description of definable sets in ω-free PAC fields: they are definable by Boolean combinations of formulas with only one quantifier (see [J]).

3.3. Algebraic closure, dividing. If F is a field, and $A \subset F$, then $A = \mathrm{acl}(A)$ (A is algebraically closed in the sense of Th(F)) implies that the extension F/A is regular. (For PAC fields, this condition is also sufficient, see [CP].)

Assume that $F_0 \subset A, B$ are algebraically closed subsets of F, with $F_0 \prec F$. If $tp(A/B)$ does not divide over F_0, then A and B are independent over F_0 in the sense of Th(F^s), and

$F \cap A^s B^s = AB$. One can show, using Galois theory, that the second condition corresponds to:

$$S\mathcal{G}(A) \cap S\mathcal{G}(B) = S\mathcal{G}(F_0),$$

and is therefore quite a natural condition.

3.4. Example. Let F be a PAC field of characteristic $\neq 2$, and assume that $[F^\times : F^{\times^2}]$ is infinite. I.e., $\mathcal{G}(F)$ has infinitely many quotients isomorphic to $\mathbb{Z}/2\mathbb{Z}$. As remarked before, each quadratic extension of F can be thought of as an imaginary of F. If $a, b \in F$ are non-squares, their square roots generate the same Galois extension if and only if ab^{-1} is a square. This defines an equivalence relation on the set of non-squares of F.

3.5. Local dividing, tree property This is one of the tools that was used to show that the local character of dividing fails for unbounded PAC fields. Indeed, one can show (see [C1]) that if F is unbounded PAC, then for all $\kappa \geq \aleph_0$ there exists sets $E_0 \subset E_1$ of cardinality κ, and a 1-type p over E, such that if $E_0 \subset E_1 \subset E$ is such that p does not fork over E, then $|E_1 \setminus E_0| = \kappa$. Essentially the same proof shows that the theory of an unbounded PAC is not rosy.

Essentially the same construction shows that the theory of an unbounded PAC field has the tree property of the second kind. Here is the proof when F is ω-free, of characteristic $\neq 2$: let a_i, $i \in \mathbb{N}$, be distinct elements of F, b_j, $j \in \mathbb{N}$, elements of $F^\times$ in distinct cosets of $F^{\times^2}$, and consider the formula $\varphi(x, y, z)$ expressing that $(x + y)z^{-1}$ is a non-zero square. Then, for any i, the set $\{\varphi(x, a_i, b_j) \mid j \in \mathbb{N}\}$ is 2-inconsistent, since for $j_1 \neq j_2$, $b_{j_1} b_{j_2}^{-1}$ is not a square. On the other hand, for any $f : \mathbb{N} \to \mathbb{N}$, the set $\{\varphi(x, a_i, b_{f(i)}) \mid i \in \mathbb{N}\}$ is consistent, by basic properties of ω-free PAC fields, and since the Galois extensions $F(\sqrt{x + a_i})$ of $F(x)$ are linearly disjoint (as a family).

3.6. Three notions of independence. Paragraph 3.3 suggests three notions of independence: let $C \subset A, B$ be algebraically closed subsets of an ω-free PAC field F. Say that A and B are $*$-independent over C, where $* \in \{I, II, III\}$, if A and B are independent over C in the sense of $\mathrm{Th}(F^s)$, and if

I. $F \cap A^s B^s = AB$. This notion is symmetric, but not transitive.

II. If $C \subset D = \mathrm{acl}(D) \subset B$, then $F \cap (AD)^s B^s = \mathrm{acl}(AD)B$. This notion is the transitive closure of I: if $B \subset D \subset C$, then $A \downarrow_C B$ implies $A \downarrow_D B$.

III. $F \cap (AB)^s = AB$. This notion is symmetric and transitive.

None of the three notions has the local property. Notion I (and II) can be generalized to arbitrary PAC fields by replacing $F \cap A^s B^s = AB$ (i.e., $S\mathcal{G}(A) \cap S\mathcal{G}(B) = S\mathcal{G}(C)$) by: $tp(S\mathcal{G}(A)/S\mathcal{G}(B))$ does not fork over $S\mathcal{G}(C)$. Notion III is however particular to ω-free PAC fields. Note that if $A = \mathrm{acl}(A) \subset B$, then any type over A has a unique non-III-forking extension to B.

3.7. Independence theorem ([C2]). Let F be an ω-free PAC field of **characteristic** 0. It then satisfies the independence theorem over any algebraically closed set, for any of the three independence relations given above. I.e.: let E, A, B, C_1, C_2 be algebraically closed subsets of an ω-free PAC field, with E containing a p-basis of F if $[F : F^p] < \infty$. Assume that $tp(C_1/E) = tp(C_2/E)$, and that $C_1 \mathop{\smile\hspace{-0.9em}\mid}^{*} EA$, $C_2 \mathop{\smile\hspace{-0.9em}\mid}^{*}_{E} B$, where $* \in \{I, II, III\}$, and A and B are independent over E in the sense of $\mathrm{Th}(F^s)$. Then there is C realising $tp(C_1/A) \cup tp(C_2/B)$ and such that $C \mathop{\smile\hspace{-0.9em}\mid}^{*}_{E} AB$.

Comments There is also a dual version for type II-forking (i.e., $A \mathop{\smile\hspace{-0.9em}\mid}^{II}_{E} C_1$, $B \mathop{\smile\hspace{-0.9em}\mid}^{II}_{E} C_2$ and $(AB) \mathop{\smile\hspace{-0.9em}\mid}^{II}_{E} C$.). The type I-version generalizes to arbitrary bounded PAC fields, modulo the generalisation given in the previous paragraph.

It turns out that II-independence coincides with non-forking in the case of ω-free PAC fields. The Independence theorem is therefore in agreement with the results that a non-simple theory has the tree property of the first or of the second kind ([S]), and that theories with the tree property of the first kind do not satisfy the independence theorem ([K]).

3.8. A few more stability theoretic results ([C3]). As suggested by the enumeration of results I gave, one can show that properties such as NSOP$_n$ for $n \geq 3$ hold of a PAC field F if and only if they hold for its absolute Galois group. As the theory of $S\hat{F}_\omega$ is ω-stable, this in particular implies that ω-free PAC fields have NSOP$_3$. I believe that they also have NSOP$_1$, but some details need to be checked.

References

[A] J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968), 239 – 271.

[C1] Z. Chatzidakis, Simplicity and Independence for Pseudo-algebraically closed fields, in: Models and Computability, S.B. Cooper, J.K. Truss Ed., London Math. Soc. Lect. Notes Series 259, Cambridge University Press, Cambridge 1999, 41 – 61.

[C2] Z. Chatzidakis, Properties of forking in ω-free pseudo-algebraically closed fields, J. of Symb. Logic 67 Nr 3 (2002), 957 – 996.

[C3] Z. Chatzidakis, Amalgamation of types in pseudo-algebraically closed fields and applications, in preparation.

[ChDM] Z. Chatzidakis, L. van den Dries, A. Macintyre, Definable sets over finite fields, J. reine u. ang. Math. 427 (1992), 107 – 135.

[CH] Z. Chatzidakis, E. Hrushovski, *Perfect pseudo-algebraically closed fields are algebraically bounded*, J. of Algebra 271 (2004), 627 – 637.

[CP] Z. Chatzidakis, A. Pillay, Generic structures and simple theories, Ann. Pure Applied Logic 95 (1998), 71 – 92.

[CDM] G. Cherlin, L. van den Dries, A. Macintyre, Decidability and Undecidability Theorems for PAC-Fields, Bull. AMS 4 (1981), 101-104. Full proofs in a 1982 preprint.

[vdD] L. van den Dries, Dimension of definable sets, algebraic boundedness and henselian fields, Annals of Pure and Applied Logic 45 (1989), 189 – 209.

[Du] J. -L. Duret, Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendance, in: Model theory of Algebra and Arithmetic, Pacholski et al. ed., Springer Lecture Notes 834 (1980), 135 –157.

[E1] Ju. L. Ershov, Regularly closed fields, Soviet Math. Doklady 21 (1980), 510 –512.

[E2] Ju. L. Ershov, Undecidability of regularly closed fields, Alg. and Log. 20 (1981), 257 – 260.

[HL] D. Haran, A. Lubotzky, Embedding covers and the theory of Frobenius fields, Israel J. of Math. 41 (1982), 181 –202.

[H] E. Hrushovski, Pseudo-finite fields and related structures, in: Model Theory and Applications, ed. by L. Bélair et al., Quaderni di Matematica Vol. 11, Aracne, Rome, 2003, 151 – 212.

[J] M. Jarden, Algebraic dimension over Frobenius fields Forum Math. 6 (1994), 43-63.

[JK] M. Jarden, U. Kiehne, The elementary theory of algebraic fields of finite corank, Inv. Math. 30 (1975), 275 –294.

[K] B. Kim, Simplicity, and stability in there, J. Symb. Logic 66 Nr 2 (2001), 822 – 836.

[J] M. Jarden, The elementary theory of ω-free Ax fields, Inv. Math. 38 (1976), 187 – 206.

[PP] A. Pillay, B. Poizat, Corps et chirurgie, J. of Symb. Logic vol. 60 (1995), 528 – 533.

[S] S. Shelah, Simple unstable theories, Ann. P. Appl. Logic 19 (1980), 177 – 203.