ALGEBRAIC DIMENSION OVER FROBENIUS FIELDS

by

Moshe Jarden*, Tel Aviv University

Abstract

We prove that each perfect Frobenius field is algebraically bounded and hence has a dimension function in the sense of v.d. Dries on the collection of all definable sets. Given a definable set S over $\mathbb{Q}$ (resp. $\mathbb{F}_p$) we can effectively determine for each $k \in \{-\infty, 0, 1, \ldots\}$ whether there exists a perfect Frobenius field M of characteristic 0 (resp., of characteristic p) such that the dimension of $S(M)$ is k. Our method of proof and decision procedure is based on Galois Stratification.

Forum **6** (1994), 43–63

* This work was partially supported by a grant from the G.I.F., the German–Israeli Foundation for Scientific Research and Development, Tel Aviv University. It was partially done while the author visited the Institute for Experimental Mathematics in Essen.

Introduction

Consider a field K and an algebraic subset A of $\mathbb{A}^n$ defined by polynomials $f_1, \ldots, f_m \in K[\mathbf{X}]$, with $\mathbf{X} = (X_1, \ldots, X_n)$. For each extension M of K let $A(M)$ denote the set of M-rational points of A. Denote the algebraic closure of K by $\widetilde{K}$. Each $g \in \widetilde{K}[\mathbf{X}]$ defines a **polynomial function** on $A(\widetilde{K})$ whose value in a point $\mathbf{a} \in A(\widetilde{K})$ is $g(\mathbf{a})$. In particular, let x_i be the function which the variable X_i defines. Let $\mathbf{x} = (x_1, \ldots, x_n)$. Then $\widetilde{K}[A] = \widetilde{K}[\mathbf{x}]$ is the **coordinate ring** of A. The map $X_i \mapsto x_i$, $i = 1, \ldots, n$, extends to a $\widetilde{K}$-epimorphism $\widetilde{K}[\mathbf{X}] \to \widetilde{K}[A]$ whose kernel is, by Hilbert's Nullstellensatz, the radical of the ideal generated by $f_1, \ldots, f_m$. If A is irreducible over $\widetilde{K}$, then $\widetilde{K}[A]$ is an integral domain and the **dimension** of A (which is usually denoted by $\dim(A)$) is the transcendence degree of $\widetilde{K}(A)$ over $\widetilde{K}$. It is the maximal number of elements of $\widetilde{K}[A]$ which are algebraically independent over $\widetilde{K}$. If A decomposes into a union of irreducible varieties $A = V_1 \cup \cdots \cup V_r$, then $\dim(A) = \max\{\dim(V_1), \ldots, \dim(V_m)\}$. It is also the maximal number of elements of $\widetilde{K}[A]$ which are algebraically independent. Here we say that $g_1, \ldots, g_r \in \widetilde{K}[A]$ are **algebraically independent** if for each nonzero polynomial $h \in K[Y_1, \ldots, Y_r]$ we have $h(g_1, \ldots, g_r) \neq 0$. In other words, there exists $a \in A(\widetilde{K})$ such that $h(g_1(\mathbf{a}), \ldots, g_r(\mathbf{a})) \neq 0$.

L. v.d. Dries [D] uses the latter definition for what he calls "algebraic dimension" of an arbitrary subset S of M^n, where M is an arbitrary field extension of K. He defines $M[S]$ as the ring of all M-valued polynomial functions on S. Then he defines algebraic independence of elements of $M[S]$ and the algebraic dimension of S as above. We denote the algebraic dimension of S by $d(S)$.

Note that if A is as above and M is an extension of K which is not algebraically closed, then $d(A(M))$ is bounded by $\dim(A)$, but may very well be smaller than it.

In particular let $\mathcal{L}$ be a first order language which expands the language of rings $\mathcal{L}(\text{ring}, K)$ with constant symbol for each element of K. Each formula $\varphi(X_1, \ldots, X_n)$ of $\mathcal{L}$ defines a set

$$S_\varphi(M) = \{\mathbf{a} \in M^n |\ \varphi(\mathbf{a}) \text{ is true in } M\}.$$

L. v.d. Dries [D] proves that if each definable subset S of M^{n+1} is "algebraically bounded" then d behaves on the collection of all definable sets as a **dimension function**:

(1a) $d(S) = -\infty$ if and only if $S = \emptyset$;

(1b) $d(\{a\}) = 0$ for each $a \in M$;

(1c) $d(M) = 1$;

(1d) $d(S_1 \cup S_2) = \max\{d(S_1), d(S_2)\}$;

(1e) $d(S^\sigma) = d(S)$ for each permutation σ of $\{1, \ldots, n\}$, where
$S^\sigma = \{(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in M^n |\ (x_1, \ldots, x_n) \in S\}$.

(1f) Let S be a definable subset of M^{n+1}. For each $\mathbf{a} \in M^n$ let $S_\mathbf{a} = \{c \in M |\ (\mathbf{a}, c) \in S\}$. For $i = 0, 1$ let $T^{(i)} = \{\mathbf{a} \in M^n |\ d(S_\mathbf{a}) = i\}$. Then $T^{(i)}$ is a definable set and $d\{(\mathbf{a}, c) \in S |\ \mathbf{a} \in T^{(i)}\} = d(T^{(i)}) + i$.

Here we say that S is **algebraically bounded** if there exist polynomials $f_1, \ldots, f_m \in M[\mathbf{X}, Y]$ such that for each $\mathbf{a} \in M^n$ for which the set $S_\mathbf{a}$ is finite and nonempty there exists j between 1 and m such that $f_j(\mathbf{a}, Y) \neq 0$ and $S_\mathbf{a} \subseteq \{c \in M |\ f_j(\mathbf{a}, c) = 0\}$.

Suppose further that $\mathcal{M}$ is a class of fields that contain K. We say that S is **uniformly bounded** on $\mathcal{M}$ if there exist polynomials $f_1, \ldots, f_m \in K[\mathbf{X}, Y]$ such that for each $M \in \mathcal{M}$ and for each $\mathbf{a} \in M^n$ for which the set $S(M)_\mathbf{a}$ is finite and nonempty there exists j between 1 and m such that $f_j(\mathbf{a}, Y) \neq 0$ and $S(M)_\mathbf{a} \subseteq \{c \in M |\ f_j(\mathbf{a}, c) = 0\}$.

In addition to algebraically closed fields, v.d. Dries proves that definable sets in real closed fields and definable sets in Henselian fields are algebraically bounded. So, in all those cases the algebraic dimension has property (1).

The goal of the present work is to prove the algebraic boundedness of definable sets over each Frobenius field M. Moreover, we prove for a K-definable set S that the dimension $d(S(M))$ is uniform in M (See (c) of the following theorem). Finally, if K is finitely generated, we establish a primitive recursive procedure to compute $d(S(M))$.

Here we say that M is **PAC** if each nonvoid absolutely irreducible variety V defined over M has an M-rational point. We denote the absolute Galois group of a field

M by $G(M)$. An **embedding problem** for $G(M)$ is a pair

$$(\alpha\colon B \to A,\ \varphi\colon G(M) \to A), \tag{2}$$

of epimorphisms of profinite groups. A **solution** of (2) is an epimorphism $\gamma\colon G(M) \to B$ such that $\alpha \circ \gamma = \varphi$. We denote the set of finite quotients of $G(M)$ by $\mathrm{Im}(G(M))$. If (2) is solvable for each $B \in \mathrm{Im}(G(M))$, then $G(M)$ has the **embedding property**. We say that M is a **Frobenius field** if M is PAC and $G(M)$ has the embedding property.

THEOREM: (a) *Let K be a field, $\varphi(X_1, \ldots, X_n, Y)$ be a formula of $\mathcal{L}(\mathrm{ring}, K)$, and $S = S_\varphi$. Then, $S(M)$ is algebraically bounded, uniformly on all perfect Frobenius fields M that contain K.*

(b) *For each perfect Frobenius field M, algebraic dimension gives a dimension function d on the collection of definable sets over M.*

(c) *In the notation of (a), there exist a finite Galois extension L of K and a finite family $\mathcal{G}$ of finite groups such that for each perfect Frobenius field M that contains K the dimension $d(S(M))$ depends only on $M \cap L$ and on $\mathrm{Im}(G(M)) \cap \mathcal{G}$.*

(d) *If K is a given finitely generated field (e.g., K is $\mathbb{Q}$ or $\mathbb{F}_p$), then we may effectively compute L and $\mathcal{G}$. In particular we can determine for each $k \in \{-\infty, 0, 1, \ldots, n\}$ whether there exists a perfect Frobenius field M which contains K such that $d(S_\varphi(M)) = k$.*

The case $n = 0$ is also allowed in the Theorem. In this case φ is a sentence. To say that φ is true in M is equivalent in this case to say that $d(S_\varphi(M)) = 0$. Thus (d) of the Theorem allows us to effectively check whether φ is true in all perfect Frobenius fields M which contains K. This is exactly the content of [FJ, Thm. 25.11].

It is therefore not surprising that the proof of (a) and (c) of the Theorem is based on the Galois stratification procedure as presented in Chapter 25 of [FJ]. So, we assume that the reader is familiar with that chapter and use its concepts without necessarily redefining it.

Finally, to prove part (d) of the theorem we assume also familiarity with the concepts and results of [FJ, Chap. 17].

1. Algebraic dimension over PAC fields.

We fix a basic field K and let $p = \mathrm{char}(K)$. Each field we consider is an extension of K. We denote the language of rings with constant symbols for each element of K by $\mathcal{L}(\mathrm{ring}, K)$.

Let M be a field extension of K. Consider a nonempty subset S of M^n. Every polynomial $f \in M[X_1, \ldots, X_n]$ defines a function from S into M, which we call an **M-polynomial function**. Denote the ring of all M-polynomial functions on S by $M[S]$. We say that $f_1, \ldots, f_m \in M[S]$ are **algebraically independent** if for each nonzero polynomial $g \in M[Y_1, \ldots, Y_m]$ there exists $\mathbf{x} \in S$ such that $g(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})) \neq 0$. Following v.d. Dries [D, Section 2], we define the **algebraic dimension** of S as the maximal number of functions in $M[S]$ which are algebraically independent. We denote this number* (which is obviously bounded by n) by $d(S)$.

As v.d. Dries remarks in [D, 2.12], the algebraic dimension of S is equal to the algebraic dimension of its Zariski closure $\overline{S}$. Thus there exist polynomials $f_1, \ldots, f_m \in M[\mathbf{X}]$ which define an M-algebraic set A and $\overline{S} = A(M) = \{\mathbf{x} \in M^n |\ f_1(\mathbf{x}) = \cdots = f_m(\mathbf{x}) = 0\}$. If M is algebraically closed, then, by Hilbert Nullstellensatz, $d(\overline{S})$ is equal to the dimension of A as is usually defined in algebraic geometry:

$$\dim(A) = \max\{\mathrm{trans.deg}_M M(\mathbf{x}) |\ \mathbf{x} \in A(\Omega)\}, \tag{1}$$

where Ω is an algebraically closed field which contains M and has infinite transcendence degree over M. If M is not algebraically closed, then $d(\overline{S}) \leq \dim(A)$. A typical example where an inequality occurs is when A is the algebraic surface defined by the equation $X^2 + Y^2 + Z^2 = 0$ over $\mathbb{Q}$. Then $\dim(A) = 2$ but $A(\mathbb{Q}) = \{(0,0,0)\}$ and hence $d(A(\mathbb{Q})) = 0$.

There is a way to compute the algebraic dimension by transcendence degree of points. Each formula $\varphi(X_1, \ldots, X_n)$ of $\mathcal{L}(\mathrm{ring}, K)$ defines a map $S = S_\varphi$ from the class of field extensions of K to the class of sets:

$$S(M) = \{\mathbf{x} \in M^n |\ \varphi(\mathbf{x}) \text{ is true in } M\}.$$

* L. v.d. Dries [D] uses the notation alg.dim for the algebraic dimension and reserves the letter d for an arbitrary dimension function.

We say that S is a K**-definable subset** of $\mathbb{A}^n$, and $S(M)$ is a K**-definable** set over M (more precisely, K**-definable subset** of M^n). Let $M^\#$ be an elementary extension of M which is $|M|^+$-saturated [S, p. 81]. Then, [D, Lemma 2.3]:

$$(2) \qquad d(S(M)) = \max\{\text{trans.deg}_M M(\mathbf{x})|\ \mathbf{x} \in S(M^\#)\}.$$

In particular consider an algebraic set A defined over a field M. The decomposition intersection procedure [FJ, Section 19.1] gives an algebraic subset A^* of A which is the union of all absolutely irreducible subvarieties of A defined over M. Moreover, each M-irreducible component of A^* is absolutely irreducible. This procedure is in particular valuable if M is PAC [FJ, p. 129].

PROPOSITION 1.1: *We have, $d(A) \leq \dim(A^*)$. If M is PAC, then $d(A) = \dim(A^*)$.*

Proof: Let $M^\#$ be an elementary extension of M which is $|M|^+$-saturated. In particular $M^\#$ is a regular extension of M. Hence each $\mathbf{x} \in A(M^\#)$ defines an absolutely irreducible variety V over M. So $V \subseteq A$ and therefore, $V \subseteq A^*$. It follows that $\text{trans.deg}_M(\mathbf{x}) = \dim(V) \leq \dim(A^*)$. Conclude from (2) that $d(A(M)) \leq \dim(A^*)$.

Now we suppose that M is PAC and prove the other direction of the latter inequality. Let $A_1^*, \ldots, A_s^*$ be the M-irreducible components of A^*. They are absolutely irreducible varieties. For each i between 1 and s the set $A_i^*(M)$ is Zariski dense in A_i^* [FJ, Prop. 10.1]. Hence, by the saturation of $M^\#$, the set $A_i^*(M^\#)$ contains a point $\mathbf{x}$ which belongs to no proper M-algebraic subset of A_i^*. Thus $\mathbf{x}$ is a generic point of A_i^*. Conclude that

$$\dim(A^*) = \max_{1 \leq i \leq s}(\dim(A_i^*)) \leq d(A(M)),$$

as contended. ∎

A subset S of M^{n+1} is said to be **algebraically bounded** if there exist polynomials $f_1, \ldots, f_r \in M[X_1, \ldots, X_n, Y]$ such that for each $\mathbf{x} \in M^n$ for which the set $S_{\mathbf{x}} = \{y \in M|\ (\mathbf{x}, y) \in S\}$ is finite there exists i between 1 and r such that $f_i(\mathbf{x}, Y) \neq 0$ and $S_{\mathbf{x}} \subseteq \{y \in M|\ f_i(\mathbf{x}, y) = 0\}$. In this case we say that the set $\{f_1, \ldots, f_r\}$ **bounds** S.

We say that a collection $\mathcal{D}$ of sets over M is **algebraically bounded**, if each subset of M^{n+1} which belongs to $\mathcal{D}$ is algebraically bounded. If this is the case, then the restriction of the algebraic dimension to $\mathcal{D}$ is what v.d. Dries calls a "dimension function" [D, 2.7]. If we add [D, 1.5] and [D, 2.5] to the definition of the dimension function which appears in the introduction of [D] we conclude:

PROPOSITION 1.2: *Suppose that each K-definable set over M is algebraically bounded. Then the following conditions hold for all K-definable sets S, S_1, S_2 over M:*

(a) $d(S) = -\infty$ *if and only if* $S = \emptyset$.

(b) $d(S) = 0$ *if and only if S is finite and nonempty.*

(c) $d(M^n) = n$ *for each positive integer n.*

(d) $d(S_1 \bigcup S_2) = \max\{d(S_1), d(S_2)\}$.

(e) $S_1 \subseteq S_2$ *implies* $d(S_1) \le d(S_2)$.

(f) *Suppose that $S \subseteq M^{m+n}$. For each $\mathbf{x} \in M^m$ let $S_\mathbf{x} = \{\mathbf{y} \in M^n | (\mathbf{x}, \mathbf{y}) \in S\}$, and for $i = 0, 1, \ldots, n$ let $T^{(i)} = \{\mathbf{x} \in M^m |\ d(S_x) = i\}$. Then $T^{(i)}$ is K-definable and $d\big(\{(\mathbf{x}, \mathbf{y}) \in S |\ \mathbf{x} \in T^{(i)}\}\big) = d(T^{(i)}) + i$.*

(g) *If $S \subseteq M^m$ and $f\colon S \to M^n$ is a function whose graph is K-definable, then $d(f(S)) \le d(S)$. In particular $d(f(S)) = d(S)$ if f is injective.*

(h) *Under the assumptions of (g) let $0 \le i \le m$. Then $B^{(i)} = \{\mathbf{y} \in A^n |\ d(f^{-1}(y)) = i\}$ is K-definable and $d(f^{-1}(B^{(i)})) = d(B^{(i)}) + i$.*

(i) $d(S_1 \times S_2) = d(S_1) + d(S_2)$.

COROLLARY 1.3: *Under the assumptions of Proposition 1.2 let S be a K-definable subset of M. If S is infinite, then $d(S) = 1$.*

Proof: By Proposition 1.2(c),(e), $d(S) \le d(M) = 1$. Hence, by Proposition 1.2(a),(b), $d(S) = 1$. ∎

2. Algebraic boundedness of Galois sets.

The goal of this section is to prove that for each perfect Frobenius field M, algebraic dimension defines a dimension function on the definable sets over M. Our main tool in the proof is Galois Stratification as developed in [FJ, Chap. 25]. It is interesting to note that although the elementary theory of perfect PAC fields is undecidable [FJ, Cor. 22.24] some ingredients of Galois Stratification go through for perfect PAC fields. This goes far enough to prove that if M is a perfect PAC field, then each subset of M^{n+1} which is defined by a quantifier free Galois formula is algebraically bounded.*

Let $\mathcal{A} = \langle A, C_i/A_i \rangle_{i\in I}$ be a normal stratification of a K-constructible set A in $\mathbb{A}^{n+m}$ over K [FJ, Sec. 25.3]. Consider a family $\mathcal{H}$ of finite groups and an expansion

$$\mathcal{A}(\mathcal{H}) = \langle \mathbb{A}^{n+m}, C_i/A_i, \mathrm{Con}(A_i, \mathcal{H}) \rangle_{i\in I}$$

of $\mathcal{A}$ to a Galois stratification with respect to $\mathcal{H}$. In particular each $H \in \mathrm{Con}(A_i, \mathcal{H})$ belongs to $\mathcal{H}$. If $\mathcal{H}'$ is another family of finite groups which contains (an isomorphic copy) of each $H \in \mathrm{Con}(A_i, \mathcal{H})$, then $\mathcal{A}(\mathcal{H}') = \mathcal{A}(\mathcal{H})$. In the latter case we write $\mathrm{Con}(\mathcal{A}(\mathcal{H})) \subseteq \mathcal{H}'$. Each m-tuple of quantifiers $Q_1, \ldots, Q_m$ defines a **Galois formula** $\theta(\mathbf{X})$ with respect to $\mathcal{H}$:

$$(Q_1Y_1)\cdots(Q_mY_m)[\mathrm{Ar}(\mathbf{X}, \mathbf{Y}) \subseteq \mathrm{Con}(\mathcal{A}(\mathcal{H}))], \tag{1}$$

where $\mathbf{X} = (X_1, \ldots, X_n)$ and $\mathbf{Y} = (Y_1, \ldots, Y_m)$.

As in Section 1, θ defines a map $S = S_\theta$ from the class of all extensions M of K to the class of sets:

$$S(M) = \{\mathbf{x} \in M^n |\ \theta(\mathbf{x}) \text{ is true in } M\}.$$

(See [FJ, Sec. 25.4] for the interpretation of "$\theta(\mathbf{x})$ is true in M"). We say that S is a **K-Galois set in** $\mathbb{A}^n$ and that $S(M)$ is a **K-Galois subset** of M^n. If θ is quantifier free (i.e., $m = 0$), then we also say that $\mathcal{A}(\mathcal{H})$ **defines** $S = S_{\mathcal{A}(\mathcal{H})}$ and $S(M) = S_{\mathcal{A}(\mathcal{H})}(M)$.

* The author is indebted to Dan Haran for calling his attention to the possibility of partially extending the results to PAC fields.

REMARK 2.1: *Identification of definable sets and Galois sets.* Remark 25.8 of [FJ] associates a Galois formula $\theta(\mathbf{X})$ to each formula $\varphi(\mathbf{X})$ of $\mathcal{L}(\mathrm{ring}, K)$ such that if M is an extension of K and $\mathbf{a} \in M^n$, then $M \models \varphi(\mathbf{a})$ if and only if $M \models \theta(\mathbf{a})$. Moreover, $\theta(X)$ has the same prefix of quantifiers as $\varphi(X)$ and is defined by a stratification $\mathcal{A}(\mathcal{H})$ where $\mathcal{H} = \{1\}$.

Conversely, let $\theta(\mathbf{X})$ be a Galois formula over K with respect to the stratification $\mathcal{A}(\mathcal{H})$ given by (1). We construct a formula $\varphi(\mathbf{X})$ which is equivalent to $\theta(\mathbf{X})$ over each field M that contains K.

It suffices to carry out the construction only for quantifier free formula. That is $\theta(\mathbf{X})$ is the formula $\mathrm{Ar}(\mathbf{X}) \subseteq \mathrm{Con}(\mathcal{A}(\mathcal{H}))$, where $\mathcal{A}(\mathcal{H}) = \langle A, C_i/A_i, \mathrm{Con}(A_i, \mathcal{H})\rangle_{i\in I}$ is a Galois stratification over K with respect to $\mathcal{H}$, and A is a K-constructible subset of $\mathbb{A}^n$.

For each extension M of K and each $\mathbf{a} \in M^n$ the statement $M \models \theta(\mathbf{a})$ is equivalent to the disjoint disjunction of the statements

$$(2) \qquad \mathbf{a} \in A_i \quad \wedge \quad \mathrm{Ar}(A_i, M, \mathbf{a}) \subseteq \mathrm{Con}(A_i, \mathcal{H}).$$

So, we may assume that $A = A_i$ and let $C = C_i$.

Also, $\mathrm{Con}(A_i, \mathcal{H}) = \mathrm{Con}_j(A, \mathcal{H})$ is the disjoint union of finitely many conjugacy classes $\mathrm{Con}_j(A, \mathcal{H})$ of subgroups of $\mathcal{G}(C/A)$. The statement $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}(A, \mathcal{H})$ is equivalent to the disjoint disjunction of the statements $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}_j(A, \mathcal{H})$. So, assume without loss that $\mathrm{Con}(A, \mathcal{H})$ consists of all conjugates of a certain subgroup H of $\mathcal{G}(C/A)$.

Let E (resp., F) be the quotient field of $K[A]$ (resp., C). Let $y_0, y_1, \ldots, y_s$ be elements of C such that $E(y_0)$ is the fixed field of H in F and $K(y_1), \ldots, K(y_s)$ is a list of all proper extensions of $E(y_0)$ in F. Replacing $\mathcal{A}(\mathcal{H})$ by a finer stratification, if necessary, we may assume that $K[A, y_0]/K[A]$ is a ring cover and that $y_1, \ldots, y_s$ are integral over $K[A]$. Let $K[A] = K[\mathbf{x}, g(\mathbf{x})^{-1}]$, where $\mathbf{x}$ is a generic point of A and $g \in K[\mathbf{X}]$ a polynomial that vanishes at no point of A. Choose monic polynomials $f_j(\mathbf{x}, Y) \in K[A][Y]$ which are irreducible over E and such that $f_j(\mathbf{x}, y_j) = 0$. Then, for each extension M of K and each $\mathbf{a} \in M^n$, statement (2) is equivalent over M to the following statement of $\mathcal{L}(\mathrm{ring}, K)$:

$$\mathbf{a} \in A \quad \wedge \quad (\exists Y)[f_0(\mathbf{a}, Y) = 0] \quad \wedge \quad \bigwedge_{j=1}^{s} \neg(\exists Y)[f_j(\mathbf{a}, Y) \neq 0]. \quad \blacksquare$$

Chapter 25 of [FJ] shows how to eliminate quantifiers from Galois formulas over Frobenius fields. Thus, if M is a perfect Frobenius field which contains K, and S is a K-Galois formula with θ given by (1), then there exists a quantifier free K-Galois formula θ', such that $S(M) = S_{\theta'}(M)$. Proposition 23.2 of [FJ] expresses the main property of Frobenius fields which makes the elimination of quantifiers procedure of [FJ, Chap. 25] (also called the **stratification procedure**) work. It turns out that a stronger form of the latter Proposition holds even for a PAC field, once a certain embedding problem is solvable.

LEMMA 2.2: *Let M be a PAC field. Let S/R be a Galois cover of rings which is finitely generated and regular over M. Let F/E be the corresponding Galois cover of the quotient fields, and suppose that E is transcendental over M. Denote the algebraic closure of M in F by N. Let H be a subgroup of $\mathcal{G}(F/E)$ which belongs to $\mathrm{Im}(G(M))$ such that $\mathrm{res}_N H = \mathcal{G}(N/M)$.*

(a) *If the embedding problem*

$$(3) \qquad (\mathrm{res}_N\colon H \to \mathcal{G}(N/M),\ \mathrm{res}_N\colon G(M) \to \mathcal{G}(N/M))$$

is solvable (i.e., there exists an epimorphism $\gamma\colon G(M) \to H$ such that $\gamma(\sigma)x = \sigma x$ for all $\sigma \in G(M)$ and $x \in N$), then there exist infinitely many M-homomorphisms $\varphi\colon S \to M_s$ such that

(4a) $\varphi(R) = M$ and $D(\varphi) = H$, and

(4b) if $p = \mathrm{char}(M) > 0$, $m \le [M : M^p]$ and $y_1, \ldots, y_m \in R$ are p-independent over E^p, then $\varphi(y_1), \ldots, \varphi(y_m)$ are p-independent over M^p.

(b) *If embedding problem (3) is unsolvable, then there exists no M-homomorphism $\varphi\colon S \to K_s$ such that (4a) holds.*

(c) *If M is a Frobenius field, then (3) is solvable, and hence there exist infinitely many φ such that (4) holds.*

Proof: Suppose first that embedding problem (3) is solvable. Then the proof of [FJ, Prop. 23.2] gives an M-homomorphism $\varphi\colon S \to K_s$ such that (4) holds. We repeat this proof for the convenience of the reader.

Let E' be the fixed field of H in F. Since E is a regular extension of M and N is the algebraic closure of M in F, the extension F/N is regular. Since $\mathrm{res}_N H = \mathcal{G}(N/M)$, we have $N \cap E' = M$. By assumption M has a Galois extension P which contains N for which there exists an isomorphism $h\colon \mathcal{G}(P/M) \to \mathcal{G}(F/E')$ such that $h(\sigma)x = \sigma x$ for each $\sigma \in \mathcal{G}(P/M)$ and $x \in N$. Restriction maps $\mathcal{G}(PE'/E')$ isomorphically onto $\mathcal{G}(P/M)$. Let $F' = PF$. It is a Galois extension of E' and $\mathcal{G}(F'/E')$ is isomorphic to the group

$$\{(\sigma_1, \sigma_2) \in \mathcal{G}(P/M) \times \mathcal{G}(F/E') |\ \mathrm{res}_N \sigma_1 = \mathrm{res}_N \sigma_2\}.$$

Consider the subgroup

$$\Delta = \{\sigma \in \mathcal{G}(F'/E') |\ \mathrm{res}_F \sigma = h(\mathrm{res}_P \sigma)\}$$

and let D be the fixed field of Δ in F'. It satisfies $\Delta \cap \mathcal{G}(F'/F) = 1$ and $\Delta \cap \mathcal{G}(F'/PE') = 1$. Also, $\Delta \cdot \mathcal{G}(F'/F) = \mathcal{G}(F'/E')$. Indeed, let σ be an element of $\mathcal{G}(F'/E')$. Let τ_1 be the unique element of $\mathcal{G}(P/M)$ such that $h(\tau_1) = \mathrm{res}_F \sigma$. Since $\mathrm{res}_N h(\tau_1) = \mathrm{res}_N \tau_1$, there exists $\tau \in \mathcal{G}(F'/E')$ such that $\mathrm{res}_P \tau = \tau_1$ and $\mathrm{res}_F \tau = h(\tau_1)$. So, $\sigma = \tau \cdot \tau^{-1}\sigma$ with $\tau \in \Delta$ and $\tau^{-1}\sigma \in \mathcal{G}(F'/F)$, as desired. Similarly, $\Delta \cdot \mathcal{G}(F'/PE') = \mathcal{G}(F'/E')$. By Galois correspondence, $DF = F'$, $DP = F'$, $D \cap F = E'$ and $D \cap P = M$. The latter relation implies that D is a regular extension of M. Moreover, D/M is finitely generated because F'/M is.

The integral closure U of R in D is finitely generated over R [L, p. 120], and therefore over M. Since M is PAC there exists an M-epimorphism $\psi\colon U \to M$. By [FJ, Exer. 2 of Chap. 5], the integral closure V of U in F' is $PU = P \otimes_M U$. By the same reason, $V = PS$. Thus ψ extends to an P-epimorphism $\psi'\colon V \to P$. Since $[F' : D] = [P : M]$ the decomposition group $D(\psi')$ is Δ [FJ, Lemma 5.5]. Let φ be the restriction of ψ' to S. Then $\mathcal{G}(F/E') = \mathrm{res}_F D(\psi') \le D(\varphi) \le \mathcal{G}(F/E')$. Hence $D(\varphi) = H$. This proves (4a).

If $p > 0$ and $y_1, \ldots, y_m$ are as in (4b), then, since D/E is separable, they are p-independent over D_p. Use [FJ, Prop. 10.11] to choose ψ so that $\psi(y_1), \ldots, \psi(y_m)$ are p-independent over M^p.

Now choose $x \in R$ which is transcendental over M. Suppose that $\varphi_1, \ldots, \varphi_n$ are M-homomorphisms from S into M_s which satisfy (4). Let $a_i = \varphi_i(x)$, $i = 1, \ldots, n$, and consider the ring of fractions $R' = R[(x-a_1)^{-1}, \ldots, (x-a_n)^{-1}]$ and $S' = SR'$ of R and S, respectively. Then S'/R' is a Galois cover of rings which is finitely generated and regular over M with F/E as the corresponding field cover. The argument above supplies an M-homomorphism φ': $S' \to M_s$ which satisfies (4) with R' replacing R. In particular $\varphi(x) \notin \{a_1, \ldots, a_n\}$. Denote the restriction of φ' to S by φ_{n+1}. Then $D(\varphi_{n+1}) = D(\varphi')$. Also, φ_{n+1} is different from $\varphi_1, \ldots, \varphi_n$ and satisfies (4).

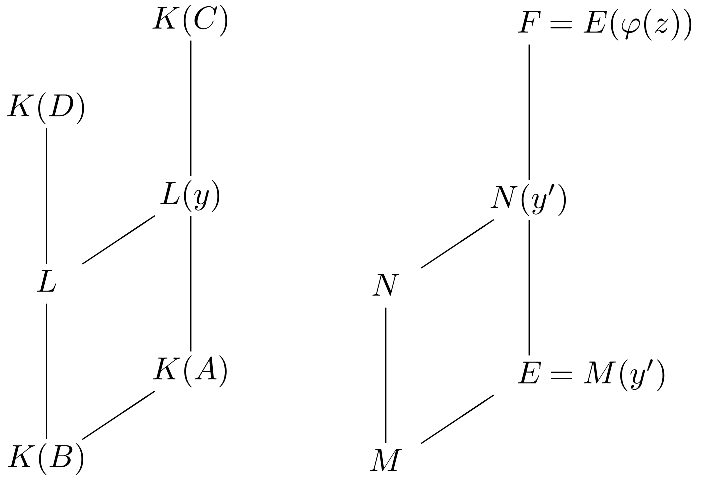
Conversely, suppose that there exists an M-homomorphism φ: $S \to M_s$ such that $\varphi(R) = M$ and $D(\varphi) = H$. Suppose without loss that the restriction of φ to N is the identity map. Then $\overline{F} = \varphi(S)$ is a Galois extension of M that contains N and φ induces an isomorphism φ^*: $\mathcal{G}(\overline{F}/M) \to H$ such that $\varphi^* \circ \alpha = \mathrm{res}_{\overline{F}/N}$, where α: $H \to \mathcal{G}(N/M)$ is the restriction map. The map $\mathrm{res}_{M_s/\overline{F}} \circ \varphi^*$ solves embedding problem (3). ∎

The core of the stratification procedure is [FJ, Lemmas 25.2 and 25.4]. We mix these results with a certain strengthening into Lemma 2.3. Here, as in those lemmas, we use π for the projection of an $(n+1)$-tuple in $\mathbb{A}^{n+1}$ on the first n coordinates. From now on, we assume familiarity with the technique of Galois stratification as presented in [FJ, Chap. 25]. However, there are two concepts that we redefine:

Let $(C/A,\ D/B)$ be a pair of Galois ring/set covers over K such that $A \subseteq \mathbb{A}^{n+1}$, $B \subseteq \mathbb{A}^n$ and $\pi(A) = B$. Let $\mathbf{x}$ be a generic point of B over K. Let z be a primitive element for the ring cover $C/K[A]$. Let $(\mathbf{x}, y)$ be a generic point of A over K. We say that $(C/A,\ D/B)$ is **specialization compatible** if the following conditions holds:

(5a) If $\dim(A) = \dim(B)$, then $K[A]$ is an integral extension of $K[B]$ and the maximal separable extension of $K(B)$ in $K(C)$ is contained in $K(D)$.

(5b) If $\dim(A) = \dim(B) + 1$, then $K(D)$ contains the algebraic closure L of $K(B)$ in $K(C)$ and $D \cap L/B$ is a ring cover. Also, for each field extension M of K, for each transcendental element y' over M and each K-homomorphism φ: $D \to \widetilde{M(y')}$ such that $\varphi(\mathbf{x}) \in B'(M)$ and $\varphi(y) = y'$ we have $[K(C) : L(y)] = [F : N(y')]$ and N is the algebraic closure of M in F. Here $N = M(\varphi(D \cap L))$ and $F = M(y', \varphi(z))$.



Note that (5a) does not appear in the definition of “specialization compatible” on page 406 of [FJ]. However, this is the condition which is required in [FJ, Lemma 25.4]. That part of (5b) which requires that N is the algebraic closure of M in F follows from the proof of [FJ, Lemma 25.1] but does not appear in that lemma itself.

Our second remark concerns decomposition groups. Let S/R be a Galois ring cover over K. Let M be a field that contains K and let S_1/R_1 be a Galois ring cover over M. Suppose that φ: $S \to S_1$ is a K-homomorphism such that $R_1 = M\varphi(R)$, and $S_1 = M\varphi(S)$. Then φ induces an isomorphism φ^* of $\mathcal{G}(S_1/R_1)$ onto the following subgroup of $\mathcal{G}(S/R)$:

$$D_M(\varphi) = \{\sigma \in \mathcal{G}(S/R) |\ (\forall u \in S)[\varphi(u) \in R_1 \text{ implies } \varphi(\sigma u) = \varphi(u)]\}.$$

For each $\tau \in \mathcal{G}(S_1/R_1)$, $\varphi^*(\tau)$ is the unique element of $D_M(\varphi)$ which satisfies

$$\varphi(\varphi^*(\tau)u) = \tau(\varphi(u)) \tag{6}$$

for all $u \in S$. Let S_2/R_2 be another Galois ring cover over M and let ψ: $S_1 \to S_2$ be an epimorphism such that $\psi(R_1) = R_2$. The defining relation (6) implies that $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Lemma 2.3: *Let $(C/A, D/B)$ be a specialization compatible pair of Galois ring/set covers over K such that $A \subseteq \mathbb{A}^{n+1}$, $B \subseteq \mathbb{A}^n$ and $\pi(A) = B$. Let* $\mathrm{Con}(A, \mathcal{H})$ *be a* *conjugacy domain of subgroups of* $\mathcal{G}(C/A)$ *belonging to a family* $\mathcal{H}$ *of finite groups. Let* $\mathcal{F} = \mathrm{Sub}(\mathcal{G}(D/B)) \cup \mathrm{Sub}(\mathcal{G}(C/A))$.

(a) *Suppose that* $\dim(A) = \dim(B)$. *Define a conjugacy domain* $\mathrm{Con}(B, \mathcal{H})$ *of subgroups of* $\mathcal{G}(C/A)$ *as in [FJ, before Lemma 25.4]. Let* M *be a perfect field that contains* K *such that* $\mathrm{Im}(G(M)) \cap \mathcal{F} \subseteq \mathcal{H}$. *Then, for each* $\mathbf{b} \in B(M)$ *such that* $\mathrm{Ar}(B, M, \mathbf{b}) \subseteq \mathrm{Con}(B, \mathcal{H})$ *the set of all* $\mathbf{a} \in A(M)$ *such that* $\pi(\mathbf{a}) = \mathbf{b}$ *and* $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}(A, \mathcal{H})$ *is finite and nonempty.*

(b) *Suppose that* $\dim(A) = \dim(B) + 1$. *Define a conjugacy domain* $\mathrm{Con}(B, \mathcal{H})$ *of subgroups of* $\mathcal{G}(C/A)$ *as in [FJ, Lemma 25.2]. Let* M *be a perfect PAC field that contains* K *such that* $\mathrm{Im}(G(M)) \cap \mathcal{F} = \mathcal{H} \cap \mathcal{F}$. *Then, for each* $\mathbf{b} \in B(M)$ *there are either infinitely many* $\mathbf{a} \in A(M)$ *such that* $\pi(\mathbf{a}) = \mathbf{b}$ *and* $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}(A, \mathcal{H})$ *or none. If* M *is Frobenius and* $\mathrm{Ar}(B, M, \mathbf{b}) \subseteq \mathrm{Con}(B, \mathcal{H})$, *then the former possibility holds.*

(c) *In both cases, if* $\mathbf{b} \in B(M)$ *and* $\mathbf{a} \in A(M)$, *then* $\pi(\mathbf{a}) = \mathbf{b}$ *and* $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}(A, \mathcal{H})$ *implies* $\mathrm{Ar}(B, M, \mathbf{b}) \subseteq \mathrm{Con}(B, \mathcal{H})$.

Proof of (a): Let $\mathbf{b}$ and M be as in (a). [FJ, Lemma 25.4] provides $\mathbf{a} \in A(M)$ such that $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}(A, \mathcal{H})$. The point $\mathbf{b}$ determines a homomorphism φ_0 of $K[B]$ into M. Each $\mathbf{a} \in A(M)$ for which $\pi(\mathbf{a}) = \mathbf{b}$ gives rise to an extension of φ_0 to a homomorphism φ of $K[A]$ into M. Since $K[A]$ is integral over $K[B]$, there are only finitely many extensions φ. Hence there are only finitely many points $\mathbf{a}$.

Proof of (b): We have to prove that if there exists an $\mathbf{a} \in A(M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}(A, , \mathcal{H})$, then there are infinitely many such points.

Assume without loss that $L = K(D)$ is the algebraic closure of $K(B)$ in $K(C)$. Let y' be a transcendental element over M. The specialization $\mathbf{x} \to \mathbf{b}$ induces a homomorphism φ_0 of $K[A] = K[\mathbf{x}, y, g(\mathbf{x}, y)^{-1}]$ into $R = M[y', g(\mathbf{b}, y')^{-1}]$, where g is a polynomial in $K[\mathbf{X}, Y]$ which vanishes at no point of A. Extend φ_0 to a homomorphism φ of $C = K[A][z]$ into $R[z']$ where $z' = \varphi(z)$ is an element of $M(y')_s$. Let $E = M(y')$ and $F = E(z')$. Then $R[z']/R$ is a regular Galois ring cover over M and F/E is the corresponding cover of fields. The specialization assumption implies that $N = M \cdot \varphi(D)$

is the algebraic closure of M in F.

Let $\mathbf{a} = (\mathbf{b}, c)$ and extend the specialization $y' \to c$ to a homomorphism ψ of $R[z']$ onto a finite Galois extension P of M which contains N such that ψ is the identity on N. Let $\lambda = \psi \circ \varphi$. By the discussion that precedes the Lemma we get a commutative diagram

$$\begin{tikzcd}
H = D_M(\lambda) \arrow[r, "\mathrm{res}"] & \varphi^*(\mathcal{G}(N/M)) \\
H' = D_M(\psi) \arrow[r, "\mathrm{res}"] \arrow[u, "\varphi^*"] & \mathcal{G}(N/M) \arrow[u, "\varphi^*"'] \\
\mathcal{G}(P/M) \arrow[r, "\mathrm{res}"] \arrow[u, "\psi^*"] & \mathcal{G}(N/M) \arrow[u, equal]
\end{tikzcd}$$

In particular $H \in \mathrm{Ar}(A, M, \mathbf{a})$ and hence

$$H \subseteq \mathrm{Con}(A, \mathcal{H}). \tag{7}$$

Moreover the embedding problem ($\mathrm{res}_N\colon H' \to \mathcal{G}(N/M)$, $\mathrm{res}_N\colon G(M) \to \mathcal{G}(N/M)$) is solvable (by $\psi^* \circ \mathrm{res}_{\tilde{K}/P}$). Since M is PAC, Lemma 2.2(a) gives infinitely many M-homomorphisms ψ_i of $R[z']$ onto a Galois extension P_i of M which contains N such that ψ_i is the identity on N, $\psi_i(R) = M$, and $D_M(\psi_i) = H'$. For each i let $c_i = \psi_i(y')$ and $\lambda_i = \varphi \circ \psi_i$. Then $\mathbf{a}_i = (\mathbf{b}, c_i) = \lambda_i(\mathbf{x}, y) \in A(M)$ and $\pi(\mathbf{a}_i) = \mathbf{b}$. Moreover, $D(\lambda_i^*) = \varphi^*(\psi_i^*(\mathcal{G}(P_i/M))) = \varphi^*(D_M(\psi_i)) = \varphi^*(H') = H$. Hence $H \in \mathrm{Ar}(A, M, \mathbf{a}_i)$. Conclude from (7) that $\mathrm{Ar}(A, M, \mathbf{a}_i) \subseteq \mathrm{Con}(A, \mathcal{H})$, as desired.

Finally if M is a Frobenius field and $\mathrm{Ar}(B, M, \mathbf{b}) \subseteq \mathrm{Con}(B, \mathcal{H})$, then [FJ, Lemma 25.2] gives a point $\mathbf{a} \in A(M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $\mathrm{Ar}(A, M, \mathbf{a}) \subseteq \mathrm{Con}(A, \mathbf{H})$. Conclude from the preceding paragraphs that there are infinitely many such points.

Proof of (c): See the first part of the proof of [FJ, Lemma 25.2] and [FJ, Lemma 25.4]. ∎

LEMMA 2.4: *Let n be a nonnegative integer, $\mathcal{C}$ a family of finite groups, A a K-constructible subset of $\mathbb{A}^{n+1}$, $B \subseteq \mathbb{A}^n$ and $\pi(A) = B$. Let $\mathcal{A}(\mathcal{C}) = \big\langle A, C_i/A_i, \mathrm{Con}(A_i, \mathcal{C})\big\rangle_{i \in I}$ be a Galois stratification of A over K.*

Then there exist K-normal basic stratifications $A = \dot\bigcup_{j \in J} \dot\bigcup_{k \in K(j)} A_{jk}$ and $B = \dot\bigcup_{j \in J} B_j$ with the following properties:

(8a) *Each A_{jk} is contained in a unique A_i and has a Galois ring cover C_{jk} which is induced by C_i/A_i; in particular $\mathcal{G}(C_{jk}/A_{jk})$ is isomorphic to a subgroup of $\mathcal{G}(C_i/A_i)$.*

(8b) *$\pi(A_{jk}) = B_j$ for each $j \in J$ and each $k \in K(j)$ and $\pi^{-1}(B_j) = \dot{\bigcup}_{k\in K(j)} A_{jk}$.*

(8c) *Each B_j is equipped with a Galois ring cover D_j.*

(8d) *The pair $(C_{jk}/A_{jk}, D_j/B_j)$ of Galois ring/set covers is specialization compatible.*

Moreover, for each family $\mathcal{H}$ of finite groups which contains $\mathrm{Con}(\mathcal{A}(\mathcal{C}))$, each $j \in J$ and each $k \in K(j)$ consider the unique $i \in I$ such that $A_{jk} \subseteq A_i$ and let $\mathrm{Con}(A_{jk},\mathcal{H})$ be the conjugacy domain of subgroups of $\mathcal{G}(C_{jk}/A_{jk})$ induced by $\mathrm{Con}(A_i,\mathcal{C})$. Then use [FJ, Lemma 25.4] if $\dim(A_{jk}) = \dim(B_j)$ (resp., [FJ, Lemma 25.2] if $\dim(A_{jk}) = \dim(B_j)+1$) to define conjugacy a domain $\mathrm{Con}_k(B_j,\mathcal{H})$ of subgroups of $\mathcal{G}(D_j/B_j)$ from $\mathrm{Con}(A_{jk},\mathcal{H})$. Define $\mathrm{Con}(B_j,\mathcal{H})$ to be $\bigcup_{k\in K(j)} \mathrm{Con}_k(B_j,\mathcal{H})$. Finally, let $\mathcal{F} = \mathrm{Sub}(\mathcal{A}) \cup \mathrm{Sub}(\mathcal{B})$.

Then, the Galois stratification $\mathcal{A}'(\mathcal{H}) = \langle A, C_{jk}/A_{jk}, \mathrm{Con}(A_{jk},\mathcal{H})\rangle_{j\in J,k\in K(j)}$ refines $\mathcal{A}(\mathcal{C})$, and $\mathcal{B} = \langle B, D_j/B_j, \mathrm{Con}(B_j,\mathcal{H})\rangle_{j\in J}$ is a Galois stratification of B over K.

Also, for every perfect field M that contains K and satisfies $\mathrm{Im}(G(M)) \cap \mathcal{F} = \mathcal{H} \cap \mathcal{F}$, we have:

(9a) *If $\mathbf{a} \in A_{jk}(M)$ satisfies $\mathrm{Ar}(A_{jk}, M, \mathbf{a}) \leq \mathrm{Con}(A_{jk},\mathcal{H})$, then $\mathbf{b} = \pi(\mathbf{a}) \in B_j(M)$ and $\mathrm{Ar}(B_j, M, \mathbf{b}) \subseteq \mathrm{Con}(B_j,\mathcal{H})$.*

(9b) *Let $\mathbf{b} \in B(M)$ such that $\mathrm{Ar}(\mathcal{B}, M, \mathbf{b}) \subseteq \mathrm{Con}(B_j,\mathcal{H})$ and let $k \in K(j)$. If $\dim(A_{jk}) = \dim(B_j)$, then the set of all $\mathbf{a} \in A_{jk}(M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $\mathrm{Ar}(A_{jk}, M, \mathbf{a}) \subseteq \mathrm{Con}(A_{jk},\mathcal{H})$ is finite and nonempty. If $\dim(A_{jk}) = \dim(B_j) + 1$ and M is PAC, then the latter set is either infinite or empty. If M is Frobenius, then the former possibility holds.*

Proof: The existence of the K-normal stratifications $\mathcal{A}'$ and $\mathcal{B}$ with the property (8) follows from the stratification lemma [FJ, 17.26] as in the beginning of the proof of [FJ, Lemma 25.6]. Condition (9) follows from Lemma 2.3. ∎

PROPOSITION 2.5: *Let n be a nonnegative integer, $\mathcal{C}$ a family of finite groups, and $\mathcal{A}(\mathcal{C}) = \langle A, C_i/A_i, \mathrm{Con}(A_i,\mathcal{C})\rangle_{i\in I}$ a Galois stratification of $\mathbb{A}^{n+1}$ over K. Let $S =$*

*$S_{\mathcal{A}(\mathcal{C})}$ be the corresponding Galois subset of $\mathbb{A}^{n+1}$. Then there exists a finite set P of polynomials with coefficients in K which bounds $S(M)$ for each perfect PAC field M which contains K and satisfies $\mathrm{Con}(\mathcal{A}(\mathcal{C})) \subseteq \mathrm{Im}(G(M))$. If K has elimination theory in the sense of [FJ, Sec. 17.2], then P can be effectively computed.**

Proof: Denote the class of all perfect PAC fields M which contain K and satisfy $\mathrm{Con}(\mathcal{A}(\mathcal{C})) \subseteq \mathrm{Im}(G(M))$ by $\mathcal{M}$. For each $M \in \mathcal{M}$

$$S(M) = \{\mathbf{a} \in M^{n+1} |\ \mathrm{Ar}(\mathcal{A}, M, \mathbf{a}) \subseteq \mathrm{Con}(\mathcal{A}(\mathcal{C}))\}.$$

Construct a normal refinement $\mathcal{A}'$ of $\mathcal{A}$ and a normal stratification $\mathcal{B}$ of $\mathbb{A}^n$ over K, as in Lemma 2.4. The rest of the proof breaks into two parts.

PART A: *The set J_0.* Let J_0 be the set of all $j \in J$ for which $\dim(A_{jk}) = \dim(B_j)$ for each $k \in K(j)$. For each $j \in J_0$ and $k \in K(j)$, the ring $K[A_{jk}]$ is integral over $K[B_j]$. The latter ring can be written as $K[B_j] = K[\mathbf{x}, g_{j,0}(\mathbf{x})^{-1}]$ where $\mathbf{x} = (x_1, \ldots, x_n)$ is a generic point of B_j over K and $g_{j,0} \in K[\mathbf{X}]$ vanishes at no point of B_j. Also there exists $y \in K[A_{jk}]$ such that $(\mathbf{x}, y)$ is a generic point of A_{jk}. In particular y satisfies an equation

$$g_{j,0}(\mathbf{x})^r y^m + g_{j,1}(\mathbf{x}) y^{m-1} + \cdots + g_{j,m}(\mathbf{x}) = 0 \tag{10}$$

where $g_{j,1}, \ldots, g_{j,m} \in K[\mathbf{X}]$, and r and m depend on j and on k. Let

$$f_{jk}(\mathbf{X}, Y) = g_{j,0}(\mathbf{X})^r Y^m + g_{j,1}(\mathbf{X}) Y^{m-1} + \cdots + g_{j,m}(\mathbf{X}),$$

and let $f_j(\mathbf{X}, Y) = \prod_{k \in K(j)} f_{jk}(\mathbf{X}, Y)$.

If K has elimination theory, then J_0 can be effectively computed and for each $j \in J_0$ the polynomial $f_j(\mathbf{X}, Y)$ can be effectively computed.

PART B: *The set $P = \{f_j(\mathbf{X}, Y) |\ j \in J_0\}$ bounds S uniformly for all $M \in \mathcal{M}$.* Indeed, let M be a field in $\mathcal{M}$ and set $\mathcal{H} = \mathrm{Im}(G(M))$. Expand $\mathcal{A}'$ and $\mathcal{B}$ to Galois stratifications $\mathcal{A}'(\mathcal{H})$ and $\mathcal{B}(\mathcal{H})$ as in Lemma 2.4. In particular,

$$S(M) = \{\mathbf{a} \in M^{n+1} |\ \mathrm{Ar}(\mathcal{A}', M, \mathbf{a}) \subseteq \mathrm{Con}(\mathcal{A}'(\mathcal{H}))\} = \dot{\bigcup_{j \in J}} \dot{\bigcup_{k \in M(j)}} S_{jk}(\mathcal{M}).$$

* *The observation that P does not depend on M is due to Dan Haran.*

where

$$S_{jk}(M) = \{\mathbf{a} \in A_{jk}(M) |\ \mathrm{Ar}(A_{jk}, M, \mathbf{a}) \subseteq \mathrm{Con}(A_{jk}, \mathcal{H})\}.$$

Let π: $\mathbb{A}^{n+1} \to \mathbb{A}^n$ is the projection on the first n coordinates. For each $j \in J$ let

$$T_j(M) = \{\mathbf{b} \in B_j(M) |\ \mathrm{Ar}(B_j, M, \mathbf{b}) \subseteq \mathrm{Con}(B_j, \mathcal{H})\}.$$

Now let $\mathbf{b}$ be a point in M^n such that $S(M)_{\mathbf{b}}$ is finite but nonempty. In particular, there exists $\mathbf{a} \in M^{n+1}$ such that $\pi(\mathbf{a}) = \mathbf{b}$ and $\mathbf{a} \in S(M)$. Let $j \in J$ and $k \in K(j)$ be the unique indices such that $\mathbf{a} \in S_{jk}(M)$. Then $\mathbf{b} \in T_j(M)$.

Claim B1: *$j \in J_0$.* Otherwise there exists $k' \in K(j)$ such that $\dim(A_{jk'}) = \dim(B_j) + 1$. In this case, by (9b), $S(M)_{\mathbf{b}}$ is either an infinite set or empty, a contradiction.

Claim B2: *$f_j(\mathbf{b}, Y) \neq 0$ and $S(M)_{\mathbf{b}} \subseteq \{c \in K |\ f_j(\mathbf{b}, c) = 0\}$.* Indeed, since $\mathbf{b} \in B_j$, we have $g_{j,0}(\mathbf{b}) \neq 0$. Hence $f_{jk}(\mathbf{b}, Y) \neq 0$ for each $k \in K(j)$ and therefore $f_j(\mathbf{b}, Y) \neq 0$.

Secondly, if $c \in S(M)_{\mathbf{b}}$, then $(\mathbf{b}, c) \in S(M)$ and therefore there exists $k \in K(j)$ such that $(\mathbf{b}, c) \in A_{jk}$. Let $(\mathbf{x}, y)$ be a generic point of A_{jk}. Then (10) implies that $f_{jk}(\mathbf{b}, c) = 0$. Hence, $f_j(\mathbf{b}, c) = 0$ as asserted.

Conclude from both claims that the set $\{f_j(\mathbf{X}, Y) |\ j \in J_0\}$ bounds S, as needed.

∎

Let $\mathcal{M}$ be a class of fields which contains the field K. We say that the **theory of $\mathcal{M}$ is algebraically bounded** if for each K definable set S in $\mathbb{A}^{n+1}$, there exists a finite set P of polynomials in $K[\mathbf{X}, Y]$ such that for each $M \in \mathcal{M}$ and each $\mathbf{b} \in M^n$ for which $S(M)_{\mathbf{b}}$ is finite and nonempty there exists $f \in P$ such that $f(\mathbf{b}, Y) \neq 0$ and $S(M)_{\mathbf{b}} \subseteq \{c \in M |\ f(\mathbf{b}, c) = 0\}$. If P can be effectively computed from S, then we say that the theory of $\mathcal{M}$ is **effectively algebraically bounded**.

Denote the class of all perfect Frobenius fields that contain K by $\mathrm{Frob}(K)$. For a family $\mathcal{C}$ of finite groups denote the class of all perfect Frobenius fields that contain K and satisfy $\mathrm{Im}(G(M)) \subseteq \mathcal{C}$ by $\mathrm{Frob}(K, \mathcal{C})$.

THEOREM 2.6: *The theory of* Frob(K) *is algebraically bounded. If K has elimination theory, then* Frob(K) *is effectively algebraically bounded.*

Proof: Let S be a K-definable subset of $\mathbb{A}^{n+1}$. By Remark 2.1 there exists a Galois formula $\theta(X_1, \ldots, X_n, Y)$ over K with respect to the family $\mathcal{C} = \{1\}$ which defines S. The elimination procedure which is summarized in [FJ, Prop. 25.9] proves that θ is equivalent over each $M \in \mathrm{Frob}(K)$ to a quantifier free formula $\theta'(X_1, \ldots, X_n, Y)^*$. The formula θ' depends on the intersection of $\mathrm{Im}(G(M))$ with a certain finite family $\mathcal{S}$ of finite groups. However, the normal stratification which underlies θ' depends only on the normal stratification which underlies θ and hence only on S. By Proposition 2.5, there exists a finite set P of polynomials with coefficients in K which bounds $S(M) = S_{\theta'}(M)$ for each $M \in \mathrm{Frob}(K)$. Conclude that the theory of Frob(K) is algebraically bounded.

Finally, if K has elimination theory, then both θ' and P can be effectively computed. Hence, the theory of Frob(K) is effectively algebraically bounded. ∎

EXAMPLES 2.7: *Free groups.* Let $\widehat{F}_m$ be the free profinite group on m generators, where $1 \le m \le \aleph_0$. Then $\widehat{F}_m$ is projective and has the embedding property [FJ, Example 20.13 and Lemma 23.7]. A field M with $G(M) \cong \widehat{F}_m$ is said to be m-**free**. Thus each m-free PAC field is Frobenius. By Theorem 2.6 the theory of m-free perfect PAC fields of fixed characteristic is effectively algebraically bounded.

A perfect 1-free PAC field is also called **pseudo finite**. These fields are the models of the theory of all elementary statements which are true in almost all fields $\mathbb{F}_p$ [FJ, Lemma 18.25]. Thus the elementary theory of pseudo finite fields is effectively algebraically bounded.

Chatzidakis, v.d. Dries and Macintyre [CDM, Cor. 5.7] use ultraproducts to prove a stronger result: *"The elementary theory of finite fields is algebraically bounded"*. Of course, this result could have also been achieved by Galois Stratification over $\mathbb{Z}$ as in [FJ, Section 26.2]. This method would have also make the result effective. ∎

Combine Theorem 2.6 and Proposition 1.2:

* This is the only point in the proof where it fails for perfect PAC fields

THEOREM 2.8: *Let M be a perfect Frobenius field which contains K. Then algebraic dimension defines a dimension function on the collection of all K-definable sets over M. Thus, all K-definable sets over M, S, S_1, S_2 satisfy conditions (a)–(i) of Proposition 1.2.*

PROBLEM 2.9: Is each definable subset over a perfect PAC field algebraically bounded?

3. Calculation of dimension of definable sets.

The stratification procedure allows us not only to establish the algebraic dimension of definable sets over a Frobenius field M as a dimension function $d = d_M$ but also to prove that d_M is uniform in M in some sense. More precisely, let K be our fixed base field. Then, for each definable set S over K there exists a finite family of finite groups $\mathcal{G}$ and a finite Galois extension L of K such that $d(S(M))$ is determined by $\mathrm{Im}(G(M)) \cap \mathcal{G}$ and by $M \cap L$. If K has elimination theory in the sense of [FJ, Chap. 17] (e.g., K is a given finitely generated field over its prime field), then $\mathcal{G}$ and L are effectively computable.

LEMMA 3.1: *Let n be a nonnegative integer, $\mathcal{C}$ a family of finite groups, A a K-constructible subset of $\mathbb{A}^{n+1}$, and $\mathcal{A}(\mathcal{C})$ a Galois stratification of A over K. Denote the K-Galois subset of $\mathbb{A}^{n+1}$ which $\mathcal{A}(\mathcal{C})$ defines by S. As in Section 2, let π be the projection of $\mathbb{A}^{n+1}$ on the first n coordinates and let $B = \pi(A)$.*

Then there exist a partition $B = B^{(0)} \mathbin{\dot\cup} B^{(1)}$ into K-constructible sets and K-normal basic stratification $\mathcal{B}^{(0)}$ and $\mathcal{B}^{(1)}$ of $B^{(0)}$ and $B^{(1)}$, respectively, which do not depend on $\mathcal{C}$, (set $\mathcal{F} = \mathrm{Sub}(\mathcal{A}) \cup \mathrm{Sub}(\mathcal{B}^{(0)}) \cup \mathrm{Sub}(\mathcal{B}^{(1)})$), with the following property:

For each family $\mathcal{H}$ of finite groups which contains $\mathrm{Con}(\mathcal{A}(\mathcal{C}))$, the normal stratification $\mathcal{B}^{(0)}$ and $\mathcal{B}^{(1)}$ can be expanded to Galois stratifications $\mathcal{B}^{(0)}(\mathcal{H})$ and $\mathcal{B}^{(1)}(\mathcal{H})$, respectively, such that for each perfect Frobenius field M which contains K and satisfies $\mathrm{Im}(G(M)) \cap \mathcal{F} = \mathcal{H} \cap \mathcal{F}$ we have

$$d(S(M)) = \max\{d(T^{(0)}(M)),\, d(T^{(1)}(M)) + 1\},$$

where $T^{(\varepsilon)}$ is the K-Galois subset of B defined by $\mathcal{B}^{(\varepsilon)}(\mathcal{H})$, $\varepsilon = 1, 2$.

Proof: For each $M \in \mathrm{Frob}(K)$ we have

$$S(M) = \{\mathbf{a} \in A(M) |\ \mathrm{Ar}(\mathcal{A}, M, \mathbf{a}) \subseteq \mathrm{Con}(\mathcal{A}(\mathcal{C}))\}.$$

Refine $\mathcal{A}$ to a K-normal stratification $\mathcal{A}'$ and construct a K-normal basic stratification $\mathcal{B}$ of A which satisfies condition (8) of Lemma 2.4. Let $\mathcal{H}$ be a family of finite groups which contains $\mathrm{Con}(\mathcal{A}(\mathcal{C}))$. Expand $\mathcal{A}'$ and $\mathcal{B}$ to Galois stratifications $\mathcal{A}'(\mathcal{H})$ and $\mathcal{B}(\mathcal{H})$, respectively, which satisfy condition (9) of Lemma 2.4. Then

$$S(M) = \{\mathbf{a} \in A(M) \mid \mathrm{Ar}(\mathcal{A}', M, \mathbf{a}) \subseteq \mathrm{Con}(\mathcal{A}', \mathcal{H})\} = \dot{\bigcup_{j\in J}} \dot{\bigcup_{k\in K(j)}} S_{jk}(M),$$

where

$$S_{jk}(M) = \{\mathbf{a} \in A_{jk}(M) \mid \mathrm{Ar}(A_{jk}, M, \mathbf{a}) \subseteq \mathrm{Con}(A_{jk}, \mathcal{H})\}.$$

Also, let $T = \dot{\bigcup}_{j\in J} T_j$, with

$$T_j(M) = \{\mathbf{b} \in B_j(M) \mid \mathrm{Ar}(B_j, M, \mathbf{b}) \subseteq \mathrm{Con}(B_j, \mathcal{H})\}.$$

Denote the set of all $j \in J$ such that $\dim(A_{jk}) = \dim(B_j)$ for all $k \in K(j)$ by J_0. Let $J_1 = J - J_0$. For each $\varepsilon \in \{0, 1\}$ let $B^{(\varepsilon)} = \bigcup_{j\in J_\varepsilon} B_j$,

$$\mathcal{B}^{(\varepsilon)}(\mathcal{H}) = \left\langle B^{(\varepsilon)}, D_j/B_j, \mathrm{Con}(B_j, \mathcal{H})\right\rangle_{j\in J_\varepsilon},$$

and $T^{(\varepsilon)} = \bigcup_{j\in J_\varepsilon} T_j$.

Consider now $M \in \mathrm{Frob}(K)$ which satisfies the relation $\mathrm{Im}(G(M)) \cap \mathcal{F} = \mathcal{H} \cap \mathcal{F}$. Let $\mathbf{b} \in B(M)$ be a point for which there exists $\mathbf{a} \in S(M)$ such that $\pi(\mathbf{a}) = \mathbf{b}$. In particular, by (9a) of Section 2, there exists a unique $j \in J$ such that $\mathbf{b} \in T_j(M)$. Hence, by (8b) of Section 2, $\pi^{-1}(\mathbf{b}) \cap S(M) = \dot{\bigcup}_{k\in K(j)} \{\mathbf{a} \in S_{jk}(M) \mid \pi(\mathbf{a}) = \mathbf{b}\}$. By Theorem 2.8, the algebraic dimension defines a dimension function d on the collection of all definable sets over M, which satisfies conditions (a)–(i) of Proposition 1.2. By Remark 2.1, the sets S and $T^{(\varepsilon)}$, $\varepsilon = 0, 1$ are definable. By (9b) of Lemma 2.4 we have:

(1a) If $j \in J_0$, then $\pi^{-1}(\mathbf{b}) \cap S(M)$ is finite and nonempty. Hence

$$S(M)_{\mathbf{b}} = \{c \in M \mid (\mathbf{b}, c) \in S(M)\}$$

is finite and nonempty. By (b) of Proposition 1.2, $d(S(M)_{\mathbf{b}}) = 0$.

(1b) If $j \in J_1$, then $\pi^{-1}(\mathbf{b}) \cap S(M)$ is infinite. Hence, $S(M)_{\mathbf{b}}$ is infinite and therefore, by Corollary 1.3, $d(S(M)_{\mathbf{b}}) = 1$.

Conclude that

$$T^{(\varepsilon)}(M) = \{\mathbf{b} \in B(M) |\ d(S(M)_{\mathbf{b}}) = \varepsilon\}, \qquad \varepsilon = 0, 1.$$

Note that $S(M) = [\pi^{-1}(T^{(0)}(M)) \cap S(M)] \cup [\pi^{-1}(T^{(1)}(M)) \cap S(M)]$. Hence, by Proposition 1.2(d) and (f),

$$d(S(M)) = \max\{d(T^{(0)}(M)),\ d(T^{(1)}(M)) + 1\}. \qquad \blacksquare$$

A repeated application of Lemma 3.1 gives an explicit formula for $d(S(M))$:

PROPOSITION 3.2: *Let n be a nonnegative integer, $\mathcal{C}$ a family of finite groups, A a constructible subset of $\mathbb{A}^n$, and $\mathcal{A}(\mathcal{C})$ a Galois stratification of A over K. Denote the K-Galois subset of $\mathbb{A}^{n+1}$ which $\mathcal{A}(\mathcal{C})$ defines by S.*

Then there exists a finite Galois extension L of K and a finite family $\mathcal{G}$ of finite groups which depend on $\mathcal{A}$ but not on $\mathcal{C}$ such that $\mathrm{Sub}(\mathcal{A}) \cup \mathrm{Sub}(\mathcal{G}(L/K)) \subseteq \mathcal{G}$ with the following property:

For each family $\mathcal{H}$ of finite groups which contains $\mathrm{Con}(\mathcal{A}(\mathcal{C}))$ and each $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n$ there exists a conjugacy domain $\mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G})$ of subgroups of $\mathcal{G}(L/K)$ such that for each perfect Frobenius field M which contains K and satisfies $\mathrm{Im}(G(M)) \cap \mathcal{G} = \mathcal{H} \cap \mathcal{G}$ we have

$$(2) \qquad d(S(M)) = \max_{\varepsilon \in \{0,1\}^n} \begin{cases} \sum_{i=1}^n \varepsilon_i & \textit{if } \mathcal{G}(L/M \cap L) \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G}) \\ -\infty & \textit{otherwise} \end{cases}$$

REMARK: Interpret the right hand side of (2) in the following way: for each $\varepsilon \in \{0,1\}^n$ for which $\mathcal{G}(L/M \cap L) \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G})$ compute $\sum_{i=1}^n \varepsilon_i$. Then take the maximum over the computed sums, or let the right hand side be $-\infty$ if no sum was computed.

Proof: Consider first the case $n = 0$. In this case $\mathbb{A}^n$ consists of the origin O only and A is either empty or $A = \{O\}$. In the first case take $L = K$, $\mathcal{G} = \{1\}$, and interpret the right hand side of (2) as $-\infty$. Since $S(M)$ is empty for each $M \in \mathrm{Frob}(K)$, $-\infty$ is indeed the right value for $d(S(M))$. If $A = \{O\}$, then $\mathcal{A}(\mathcal{C}) = \{A, C/A, \mathrm{Con}\}$, $K[A] = K$, C is a finite Galois extension L of K, and Con is a conjugacy domain of subgroups of $\mathcal{G}(L/K)$. The Artin symbol $\mathrm{Ar}(A, M, O)$ is the conjugacy class of $\mathcal{G}(L/M \cap L)$ in $\mathcal{G}(L/K)$. Hence,

$S(M) \neq \emptyset$ if and only if $\mathcal{G}(L/M \cap L) \in \mathrm{Con}$. So, if we interpret $\sum_{i=1}^{0} \varepsilon_i$ as 0, then (2) is true in this case.

Suppose therefore that $n \geq 1$. Let $\pi\colon \mathbb{A}^n \to \mathbb{A}^{n-1}$ be the projection on the first $n-1$ coordinates. Apply Lemma 3.1 to obtain a partition $B = \pi(A) = B^{(0)} \cup B^{(1)}$, and K-normal basic stratifications $\mathcal{B}^{(0)}$ and $\mathcal{B}^{(1)}$ such that the conclusion of Lemma 3.1 holds.

In particular, for each family $\mathcal{D}$ of finite groups which contains $\mathrm{Con}(\mathcal{A}(\mathcal{C}))$ the basic stratifications $\mathcal{B}^{(0)}$ and $\mathcal{B}^{(1)}$ can be expanded to Galois stratifications $\mathcal{B}^{(0)}(\mathcal{D})$ and $\mathcal{B}^{(1)}(\mathcal{D})$, respectively, such that for each $M \in \mathrm{Frob}(K)$ which satisfies $\mathrm{Im}(G(M)) \cap \mathcal{F} = \mathcal{D} \cap \mathcal{F}$ we have

$$d(S(M)) = \max\{d(T^{(0)}(M)), d(T^{(1)}(M)) + 1\} \tag{3}$$

where

$$T^{(\varepsilon_n)}(M) = \bigl\{\mathbf{b} \in B^{(\varepsilon_n)}(M) |\ \mathrm{Ar}(\mathcal{B}^{(\varepsilon_n)}, M, \mathbf{b}) \subseteq \mathrm{Con}(\mathcal{B}^{(\varepsilon_n)}(\mathcal{D}))\bigr\}, \quad \varepsilon_n = 0, 1. \tag{4}$$

Apply the induction hypothesis to $\mathcal{B}^{(\varepsilon_n)}(\mathcal{D})$ to obtain a finite Galois extension $L^{(\varepsilon_n)}$ of K and a finite family $\mathcal{G}^{(\varepsilon_n)}$ of finite groups which depend on $\mathcal{B}^{(\varepsilon_n)}$ but not on $\mathcal{D}$ such that $\mathrm{Sub}(\mathcal{B}^{(\varepsilon_n)}) \cup \mathrm{Sub}(\mathcal{G}(L/K)) \subseteq \mathcal{G}^{(\varepsilon_n)}$ with the following property:

For each family $\mathcal{H}$ of finite groups which contains $\mathrm{Con}(\mathcal{B}^{(\varepsilon_n)}(\mathcal{D}))$ and for each $\varepsilon' = (\varepsilon_1, \ldots, \varepsilon_{n-1}) \in \{0,1\}^{n-1}$ there exists a conjugacy domain $\mathrm{Con}_{\varepsilon'}(L^{(\varepsilon_n)}/K, \mathcal{H} \cap \mathcal{G}^{(\varepsilon_n)})$ such that for each $M \in \mathrm{Frob}(K)$ which satisfies $\mathrm{Im}(G(M)) \cap \mathcal{G}^{(\varepsilon_n)} = \mathcal{H} \cap \mathcal{G}^{(\varepsilon_n)}$

$$\begin{aligned} &d(T^{(\varepsilon_n)}(M)) \\ &\quad = \max_{\varepsilon' \in \{0,1\}^{n-1}} \begin{cases} \sum_{i=1}^{n-1} \varepsilon_i' & \text{if } \mathcal{G}(L^{(\varepsilon_n)}/M \cap L^{(\varepsilon_n)}) \subseteq \mathrm{Con}_{\varepsilon'}(L^{(\varepsilon_n)}/K, \mathcal{H} \cap \mathcal{G}^{(\varepsilon_n)}) \\ -\infty & \text{otherwise.} \end{cases} \end{aligned} \tag{5}$$

Let $L = L^{(0)}L^{(1)}$, $\mathcal{G} = \mathcal{F} \cup \mathcal{G}^{(0)} \cup \mathcal{G}^{(1)} \cup \mathrm{Sub}(\mathcal{G}(L/K))$. For each family $\mathcal{H}$ of finite groups which contains $\mathrm{Con}(\mathcal{A}(\mathcal{C})))$ and each $\varepsilon = (\varepsilon', \varepsilon_n) \in \{0,1\}^n$ let

$$\begin{aligned} \mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G}) = \{&H \leq \mathcal{G}(L/K) |\ H \in \mathcal{H} \\ &\text{and } \mathrm{res}_{L^{(\varepsilon_n)}}(H) \in \mathrm{Con}_{\varepsilon'}(L^{(\varepsilon_n)}/K, \mathcal{H} \cap \mathcal{G}^{(\varepsilon_n)})\}. \end{aligned}$$

To conclude the proof consider $M \in \mathrm{Frob}(K)$ for which $\mathrm{Im}(G(M)) \cap \mathcal{G} = \mathcal{H} \cap \mathcal{G}$. Let $\varepsilon = (\varepsilon', \varepsilon_n) \in \{0,1\}^n$. Then $\mathrm{Im}(G(M)) \cap \mathcal{G}^{(\varepsilon_n)} = \mathcal{H} \cap \mathcal{G}^{(\varepsilon_n)}$. Since $\mathcal{G}(L/M \cap L) \in \mathrm{Im}(G(M)) \cap \mathrm{Sub}(\mathcal{G}(L/K))$, we have $\mathcal{G}(L/M \cap L) \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G})$ if and only if $\mathcal{G}(L^{(\varepsilon_n)}/M \cap L^{(\varepsilon_n)}) \in \mathrm{Con}_{\varepsilon'}(L^{(\varepsilon_n)}/K, \mathcal{H} \cap \mathcal{G}^{(\varepsilon_n)})$. Hence, by (5)

$$(6) \qquad d(T^{(\varepsilon_n)}(M)) = \max_{\varepsilon' \in \{0,1\}^{n-1}} \begin{cases} \sum_{i=1}^{n-1} \varepsilon_i & \text{if } \mathcal{G}(L/M \cap L) \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G}) \\ -\infty & \text{otherwise.} \end{cases}$$

The combination of (3) and (6) gives (2). ∎

THEOREM 3.3: *Let S be a K-definable subset of $\mathbb{A}^n$. Then there exists a finite Galois extension L of K and a finite family $\mathcal{G}$ of finite groups which contains* $\mathrm{Sub}(\mathcal{G}(L/K))$ *with the following property:*

For each subfamily $\mathcal{H}$ of $\mathcal{G}$ which contains the trivial group and each $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n$ there exists a conjugacy domain $\mathrm{Con}_\varepsilon(L/K, \mathcal{H})$ *of subgroups of $\mathcal{G}(L/K)$ such that for each perfect Frobenius field M which contains K and satisfies* $\mathrm{Im}(G(M)) \cap \mathcal{G} = \mathcal{H}$ *we have*

$$(7) \qquad d(S(M)) = \max_{\varepsilon \in \{0,1\}^n} \begin{cases} \sum_{i=1}^{n} \varepsilon_i & \textit{if } \mathcal{G}(L/M \cap L) \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H}) \\ -\infty & \textit{otherwise} \end{cases}$$

Proof: Let $\mathcal{C}$ be the family of all finite groups. By Remark 2.1 there exists a K-Galois formula $\theta(X_1, \ldots, X_n)$ with respect to the family $\{1\}$ which defines S. Thus, for each field M which contains K,

$$S(M) = \{\mathbf{a} \in S(M) |\ M \models \theta(\mathbf{a})\}.$$

By [FJ, Prop. 25.9], there exists a finite family $\mathcal{F}$ of finite groups and a K-normal stratification $\mathcal{A}$ of $\mathbb{A}^n$ such that $\mathrm{Sub}(\mathcal{A}) \subseteq \mathcal{F}$ and for every family $\mathcal{D}$ of finite group which contains $\{1\}$, the normal stratification $\mathcal{A}$ can be expanded to a Galois stratification $\mathcal{A}(\mathcal{D})$ such that

(8) for every $M \in \mathrm{Frob}(K)$ which satisfies $\mathrm{Im}(G(M)) \cap \mathcal{F} = \mathcal{D} \cap \mathcal{F}$ we have

$$(8a) \qquad S(M) = S_{\mathcal{A}(\mathcal{D})}(M) = \{\mathbf{a} \in \mathbb{A}^n(M) |\ \mathrm{Ar}(\mathcal{A}(\mathcal{D}), M, \mathbf{b}) \subseteq \mathrm{Con}(\mathcal{A}(\mathcal{D})\}.$$

Proposition 3.2 gives a Galois extension L of K and a finite family $\mathcal{G}$ of finite groups which depends on $\mathcal{A}$ but not on $\mathcal{D}$ such that $\mathrm{Sub}(\mathcal{A}) \cup \mathrm{Sub}(\mathcal{G}(L/K)) \subseteq \mathcal{G}$ with the following property: For each family $\mathcal{H}$ of finite groups which contains $\mathrm{Con}(\mathcal{A}(\mathcal{D}))$ and each $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n$ there exists a conjugacy domain $\mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G})$ of subgroups of $\mathcal{G}(L/K)$ such that

(9) for each $M \in \mathrm{Frob}(K)$ and satisfies $\mathrm{Im}(G(M)) \cap \mathcal{G} = \mathcal{H} \cap \mathcal{G}$ we have

$$(9a) \quad d(S_{\mathcal{A}(\mathcal{D})}(M)) = \max_{\varepsilon \in \{0,1\}^n} \begin{cases} \sum_{i=1}^n \varepsilon_i & \text{if } \mathcal{G}(L/M \cap L) \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H} \cap \mathcal{G}) \\ -\infty & \text{otherwise} \end{cases}$$

Add $\mathcal{F}$ to $\mathcal{G}$, if necessary, to assume that $\mathcal{F} \subseteq \mathcal{G}$. Let $\mathcal{H}$ be a subfamily of $\mathcal{G}$ which contains $\{1\}$. Let $\mathcal{D} = \mathcal{F} \cap \mathcal{H}$. Expand $\mathcal{A}$ to a K-Galois stratification $\mathcal{A}(\mathcal{D})$ such that (8) holds. In particular $\mathrm{Con}(\mathcal{A}(\mathcal{D})) \subseteq \mathcal{H}$. Hence, for each $\varepsilon \in \{0,1\}^n$ there exists a conjugacy domain $\mathrm{Con}_\varepsilon(L/K, \mathcal{H})$ of subgroups of $\mathcal{G}(L/K)$ such that (9) holds. If $M \in \mathrm{Frob}(K)$ satisfies $\mathrm{Im}(G(M)) \cap \mathcal{G} = \mathcal{H}$, then (9a) holds and $\mathrm{Im}(G(M)) \cap \mathcal{F} = \mathcal{D}$. Hence (8a) holds. Conclude that (7) is true. ∎

If the field K has elimination theory and the K-definable set S is given, then all objects whose existence were proved so far in this section can be effectively computed. This allows us to use (7) for certain decision problems:

THEOREM 3.4: *Suppose that K has elimination theory. Suppose we are given a K-definable subset S of $\mathbb{A}^n$, a primitive recursive full family of finite groups $\mathcal{C}$, and an element k of $\{-\infty, 0, 1, \ldots, n\}$. Then we can effectively decide if there exists $M \in \mathrm{Frob}(K, \mathcal{C})$ such that $d(S(M)) = k$.*

Proof: Chapter 17 of [FJ] gives an effective algorithm to compute L and $\mathcal{G}$ of Theorem 3.3. Corollary 23.19 of [FJ] allows us to effectively determine for each subfamily $\mathcal{H}$ of $\mathcal{C} \cap \mathcal{G}$ whether there exists a superprojective pro-$\mathcal{C}$ group Γ such that $\mathrm{Im}(\Gamma) \cap \mathcal{G} = \mathcal{H}$. List these subfamilies as $\mathcal{H}_1, \ldots, \mathcal{H}_m$ and let Γ_j be a superprojective pro-$\mathcal{C}$ group such that $\mathrm{Im}(\Gamma_j) \cap \mathcal{G} = \mathcal{H}_j$, $j = 1, \ldots, m$.

For each j between 1 and m and each group $H \in \mathcal{H}_j \cap \mathrm{Sub}(\mathcal{G}(L/K))$ use [FJ, Chap. 17] to compute

$$\delta(\mathcal{H}_j, H) = \max_{\varepsilon \in \{0,1\}^n} \begin{cases} \sum_{i=1}^n \varepsilon_i & \text{if } H \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H}_j) \\ -\infty & \text{otherwise} \end{cases}$$

By Theorem 3.3, $d(S(M)) = \delta(\mathcal{H}_j, H)$ for each $M \in \mathrm{Frob}(K)$ which satisfies

$$\mathrm{Im}(G(M)) \cap \mathcal{G} = \mathcal{H}_j \text{ and } \mathcal{G}(L/M \cap L) = H.$$

Recall that if $M \in \mathrm{Frob}(K)$, then $G(M)$ is superprojective [FJ, p. 355]. Hence, if $\delta(\mathcal{H}_j, H) \neq k$ for all j and H, then there exists no $M \in \mathrm{Frob}(K, \mathcal{C})$ such that $d(S(M)) = k$.

Suppose therefore that $\delta(\mathcal{H}_j, H) = k$ for some j and H. Then $H \in \mathrm{Im}(\Gamma_j)$. Hence, by [FJ, Lemma 23.4], there exists $M \in \mathrm{Frob}(K)$ such that $G(M) \cong \Gamma_j$ and $\mathcal{G}(L/M \cap L) = H$. This field satisfies $d(S(M)) = k$. ∎

Remark 3.5: *Primitive recursive decidability of* $\mathrm{Frob}(K, \mathcal{C})$. Let in particular θ be a sentence of $\mathcal{L}(\mathrm{ring}, K)$. Denote the subset of $\mathbb{A}^0$ which θ defines by S. For each M which contains K, $S(M)$ is nonempty if and only if θ is true in M. This is the case exactly if $d(S(M)) = 0$. An application of Theorem 3.4 in the case $n = 0$ allows us to effectively decide if there exists $M \in \mathrm{Frob}(K, \mathcal{C})$ such that $d(S(M)) = 0$. In other words, the elementary theory of the class $\mathrm{Frob}(K, \mathcal{C})$ is primitive recursive. So, Theorem 3.4 is a generalization of [FJ, Thm. 25.11]. ∎

Our second application of formula (7) is concerned with the Haar measure μ of $G(K)^e$ [FJ, Chap. 17]. Extend each $\sigma \in G(K)$ in the unique possible way from K_s to $\widetilde{K}$. The fixed field in $\widetilde{K}$ of $\sigma_1, \ldots, \sigma_e \in G(K)$ is denoted by $\widetilde{K}(\sigma_1, \ldots, \sigma_e)$.

Proposition 3.6: *Let K be a countable Hilbertian field (or a finite field) and e a positive integer (or $e = 1$). Then, for almost all $(\sigma_1, \ldots, \sigma_e) \in G(K)^e$ the field $\widetilde{K}(\sigma_1, \ldots, \sigma_e)$ is Frobenius and $G(\widetilde{K}(\sigma_1, \ldots, \sigma_e)) \cong \widehat{F}_e$.*

Proof: By [FJ, Thm. 18.4], for almost all $(\sigma_1, \ldots, \sigma_e) \in G(K)^e$ the field $\widetilde{K}(\sigma_1, \ldots, \sigma_e)$ is PAC and $G(\widetilde{K}(\sigma_1, \ldots, \sigma_e)) \cong \widehat{F}_e$. By [FJ, Prop. 15.31], $\widehat{F}_e$ has the embedding property. Hence, $\widetilde{K}(\sigma_1, \ldots, \sigma_e)$ is Frobenius [FJ, Def. 23.1]. ∎

Theorem 3.7: *Suppose that K is a countable Hilbertian field (or a finite field) and e is a positive integer (or $e = 1$). Let S be a K-definable subset of $\mathbb{A}^n$, $\mathcal{C}$ a full family of finite groups, and k an element of $\{-\infty, 0, 1, \ldots, n\}$. Then, the set*

$$\Sigma(K, S, e, k) = \{(\sigma_1, \ldots, \sigma_e) \in G(K)^e |\; d(S(\widetilde{K}(\sigma_1, \ldots, \sigma_e))) = k\}$$

is measurable and $\mu(\Sigma(K, S, e, k))$ is a rational number. If K has elimination theory and $\mathcal{C}$ is primitive recursive, then we can effectively compute $\mu(\Sigma(K, S, e, k))$.

Proof: Let L and $\mathcal{G}$ be as in Theorem 3.3. Consider the family $\mathcal{H}$ of all subgroups of $\mathcal{G}$ which are generated by e elements. Let $\mathrm{Con}_\varepsilon(L/K, \mathcal{H})$ be as in Theorem 3.3. Since $\mathrm{Im}(\widehat{F}_e)$ is the family of all finite groups which are generated by e elements, $\mathcal{H} = \mathrm{Im}(\widehat{F}_e) \cap \mathcal{G}$.

For each $(\bar\sigma_1, \ldots, \bar\sigma_e) \in \mathcal{G}(L/K)^e$ define

$$\delta(\bar\sigma_1, \ldots, \bar\sigma_e) = \max_{\varepsilon \in \{0,1\}^e} \begin{cases} \sum_{i=1}^n \varepsilon_i & \text{if } \langle \bar\sigma_1, \ldots, \bar\sigma_e \rangle \in \mathrm{Con}_\varepsilon(L/K, \mathcal{H}) \\ -\infty & \text{otherwise} \end{cases} \tag{10}$$

By Proposition 3.6, for almost all $(\sigma_1, \ldots, \sigma_e) \in G(K)^e$, $\widetilde{K}(\sigma_1, \ldots, \sigma_e)$ is a Frobenius field with $G(\widetilde{K}(\sigma_1, \ldots, \sigma_e)) = \langle \sigma_1, \ldots, \sigma_e \rangle \cong \widehat{F}_e$. For $\bar\sigma_i = \mathrm{res}_L \sigma_i$ we have $\mathcal{G}(L/\widetilde{K}(\sigma_1, \ldots, \sigma_e) \cap L) = \langle \bar\sigma_1, \ldots, \bar\sigma_e \rangle$. By (7), $d(\widetilde{K}(\sigma_1, \ldots, \sigma_e)(S)) = \delta(\bar\sigma_1, \ldots, \bar\sigma_e)$. Hence,

$$\mu(\Sigma(K, S, e, k)) = \frac{\#\{(\bar\sigma_1, \ldots, \bar\sigma_e) \in \mathcal{G}(L/K)^e \mid \delta(\bar\sigma_1, \ldots, \bar\sigma_e) = k\}}{[L : K]^e} \tag{11}$$

If K has elimination theory, $\mathcal{C}$ is primitive recursive and $\mathcal{A}(\mathcal{C})$ is given, then L and $\mathcal{G}$ and $\mathrm{Con}_\varepsilon(L/K, \mathcal{H})$ can be effectively computed. Also, for each $(\bar\sigma_1, \ldots, \bar\sigma_e) \in \mathcal{G}(L/K)^e$ we can effectively check whether $\langle \bar\sigma_1, \ldots, \bar\sigma_e \rangle \in \mathrm{Con}(L/K, \mathcal{H})$. Hence (10) gives an effective formula for $\delta(\bar\sigma_1, \ldots, \bar\sigma_e)$. So, we can effectively compute the right hand side of (11). ∎

References

[CDM] Z. Chatzidakis, L.v.d. Dries, A. Macintyre, *Definable sets over finite fields,* Journal für die reine und angewandte Mathematik **472** (1992), 107–135.

[D] L.P.D. v.d. Dries, *Dimension of definable sets, algebraic boundedness and Henselian fields, Annals of pure and applied logic* **45** *(1989), 189–209.*

[FJ] M.D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[L] S. Lang, *Introduction to algebraic geometry,* Interscience Publishers, New York, 1958.

[S] G.E. Sacks, *Saturated Model Theory,* Benjamin, Reading, 1972.

Moshe Jarden
School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL
e-mail: jarden@taurus.bitnet

27 December, 1998