ACFA AND MEASURABILITY

MARK RYTEN AND IVAN TOMAŠIĆ

Abstract. We show that definable sets of finite S_1-rank in algebraically closed fields with an automorphism can be measured.

1. Introduction

A *difference field* is a pair (K, σ) consisting of a field K and a distinguished automorphism σ of K. Important examples of such fields are algebraic closures $\bar{\mathbb{F}}_p$ of finite fields, equipped with a power of the Frobenius automorphism $\phi_q : x \mapsto x^q$ (for q a power of p). We will denote the pair $(\bar{\mathbb{F}}_p, \phi_q)$ by K_q.

The fundamental work of Ax [1] showed that *pseudofinite* fields (infinite models of the theory of finite fields) can be characterised as fields F which are perfect, quasifinite ($\mathrm{Gal}(\bar{F}/F) \cong \hat{\mathbb{Z}}$) and pseudo-algebraically closed (every geometrically irreducible variety over F has an F-rational point). Moreover, every pseudofinite field is elementarily equivalent to an ultraproduct of finite fields.

It has been a fruitful idea in mathematics to consider the finite field $\mathbb{F}_q$ as the fixed field of ϕ_q in K_q. This was, after all, what motivated Weil's idea of a cohomological proof of his conjectures, and a stream of important results by Grothendieck and Deligne.

Knowing that the fixed field of the model companion of difference fields (ACFA) is a pseudofinite field, and having in mind Ax's results, van den Dries, Macintyre and Wood were tempted to formulate a more general conjecture: ACFA is in fact the theory of fields K_q, and every model of ACFA is elementarily equivalent to an ultraproduct of fields K_q.

Although this question is model-theoretic in nature, it soon becomes clear that the answer transcends the boundaries of mathematical disciplines and requires pushing the methods of algebraic geometry to the extreme (and beyond). Both approaches to the problem, by Macintyre [12] and Hrushovski [9], have the same basic idea, which we will try to sketch here.

It is known that the theory ACFA ([13], [2]) is axiomatised by the following axiom scheme:

(1) (K, σ) is an algebraically closed field with an automorphism σ.
(2) For every variety X over K, and every variety $W \subseteq X \times \sigma(X)$ projecting generically onto X and $\sigma(X)$, there is a point $x \in X(K)$ such that $(x, \sigma(x)) \in W$.

The fact that finite fields are asymptotically pseudo-algebraically closed is shown using the Lang-Weil estimates. In the same way, to show axiom (2) above asymptotically for fields K_q, we require some kind of a generalisation of Lang-Weil estimate

Date: September 13, 2004.
2000 *Mathematics Subject Classification.* Primary 03C60, 11G25. Secondary 03C40, 28B99.

for the number of points on a correspondence twisted by a high-enough power of Frobenius.

Deligne's conjecture, proved in [16], [4] is a result of this nature, as well as the more general fixed-point formula used by Lafforgue in his work on the Langlands programme [11]. However, due to certain properness restrictions, none of these results is general enough for our purpose. Hrushovski proves a less qualitatively precise, but more general quantitative estimate in [9], from which the 'nonstandard Frobenius' conjecture is immediate.

In a somewhat different direction, using the classical Lang-Weil and the specific quantifier elimination (where each definable set has a finite covering by a quantifier-free set), the paper [3] establishes estimates for the number of points of definable sets over finite fields. As a consequence of the uniformity in these estimates, it also assigns a dimension and measure to definable sets in pseudofinite fields. Caught in the fashion of studying measurability aspects of various structures, as well as the increasing interest in motivic integration in the model-theoretic community, the authors of the present paper have independently realised that a similar measurability phenomenon can be deduced for ACFA, using Hrushovski's twisted Lang-Weil and essentially the same form of quantifier elimination. More precisely, we get the following.

Theorem 1.1 (Main Theorem)**.** *Let $\varphi(X, Y)$ be a formula in the language of difference rings, with $X = (X_1, \ldots, X_m)$ as parametric variables and with $Y = (Y_1, \ldots, Y_n)$. Then there is a positive constant C and a finite set D of pairs (d, μ) with $d \in \mathbb{Z} \cup \{\infty\}$, $\mu \in \mathbb{Q}^+ \cup \{\infty\}$, such that in each field K_q and each $x \in K_q^m$, we have the estimate*

$$\left|\mathrm{card}(\varphi(x, K_q^n)) - \mu q^d\right| \leq C q^{d-1/2},$$

for some $(d, \mu) \in D$.

Moreover, for each $(d, \mu) \in D$ there is a difference formula $\varphi_{(d,\mu)}(X)$ such that for each K_q, the above estimate holds for $\varphi(x, K_q^n)$ with (d, μ) if and only if $K_q \models \varphi_{(d,\mu)}(x)$.

We must note here that although the framework of difference schemes developed in [9] may be more appropriate for the task at hand, we choose to use mostly elementary techniques of classical algebraic geometry together with several main results from [9] considered axiomatically. Our hope is that this approach may find a wider audience.

The organisation of the paper is as follows. In Section 2 we recall some classical results on constructibility in algebraic geometry, and prove some new lemmas which are not readily available in the literature.

In Section 3, we establish the estimates for the quantifier-free definable sets over the fields K_q, using the twisted Lang-Weil. This is the hardest part of the work, because extending the estimates to formulae with quantifiers works exactly as in [3].

In Section 4, we thus establish the Main Theorem 1.1 and use it to we define a dimension and measure for certain definable sets in a model of ACFA, and discuss the relationship of this dimension to the known rank-functions.

A word about notation and language. We use scheme-theoretic language, which is slightly unusual for a model-theoretic paper. In Section 2 this language allows slightly more general constructibility results than can be formulated in the language

of varieties. However, in sections 3 and 4, which contain our main results, everything can be formulated in the language of varieties and we try to limit referring to schemes as much as possible.

We are grateful to Ehud Hrushovski and Zoe Chatzidakis for numerous discussions. The second author was supported by EPSRC grant GR/R37388/01 and in part by a Marie Curie Fellowship.

2. Constructibility

We attempt to find a balance between the standard notation of algebraic geometry and model theory.

The structure sheaf of a scheme X is denoted $\mathcal{O}_X$, and the residue field at $x \in X$ by $\mathbf{k}(x)$. If X is an integral scheme (reduced and irreducible), the residue field of the generic point equals the function field of X. Given a scheme S, a *variety over* S is a separated and reduced scheme of finite type over S. Given schemes X and S, the set of S-valued points of X, denoted $X(S)$, is the set of all morphisms $S \to X$. When S is the spectrum of a field k we usually just write $X(k)$. We use the term *algebraic scheme* for a scheme of finite type over a field.

For the reader coming from model theory, an affine variety X over an algebraically closed field k in our language corresponds exactly to the zero set of some polynomial ideal and to the set $X(k)$ of k-valued points of X. As most of our results refer to such objects, there should be no problem with the language.

The algebraic closure of a field k is denoted by $\bar{k}$. The *geometric* properties of a scheme X over a field k refer to the properties of the scheme $X \times_k \bar{k}$ (X considered over the algebraic closure $\bar{k}$).

Families of varieties and schemes can be treated more precisely in algebraic geometry than what is usually done in model theory. Given an S-scheme $f : X \to S$ and a point $s \in S$, there is a natural map $\mathrm{Spec}(\mathbf{k}(s)) \to S$, and the fibre X_s is defined to be the fibre product $X \times_S \mathrm{Spec}(\mathbf{k}(s))$. As a topological space, it can be identified with $f^{-1}(s)$ (with topology induced from X) and it is equivalent to the usual model-theoretic treatment of families: if our family X is defined by a formula $X(Y; Z) \wedge S(Z)$, as a set, X_s is exactly the definable set obtained by substituting parameters s for the variable Z. However, the algebraic definition of X_s is richer, because we retain the structure sheaf on X_s. Even if we have a map of *varieties*, considering fibres can quickly take us away from varieties into the realm of nonreduced or nonseparated objects, as 2.10 below illustrates. This is the reason why we prefer the scheme-theoretic language, at least in this section about constructible properties.

We adopt the definitions from [5], [7]. Since we are primarily interested in applications to varieties over a field, in our consideration of constructibility we assume that all schemes are noetherian. However, many results can be generalised to arbitrary schemes of finite presentation simply by replacing 'constructible' by 'locally constructible' below. We refer the reader interested in these issues to [7], section 9.

Definition 2.1.
(1) A subset of a noetherian topological space X is *constructible*, if it is a finite union of locally closed subsets of X.
(2) A function h from a noetherian space X to a set T is *constructible* if $h^{-1}(t)$ is constructible for all $t \in T$ and empty except for finitely many values t.

Proposition 2.2. *A function $h : X \to T$ on a noetherian space is constructible if and only if for every closed irreducible $Y \subseteq X$ there exists a nonempty open $U \subseteq Y$ on which h is constant.*

Corollary 2.3. *Let X be a noetherian topological space on which every closed irreducible subset admits a generic point. If $h : X \to T$ is such that $h^{-1}(t)$ is constructible for every $t \in T$, then h is constructible.*

Definition 2.4. We say that $\mathbf{P}(X, k)$ is a *constructible property* (of algebraic schemes), if the following conditions are satisfied:

(1) If k is a field, X a scheme over k and k' is an extension of k, $\mathbf{P}(X, k)$ holds if and only if $\mathbf{P}(X \times_k k', k')$ does.
(2) Let S be an integral noetherian scheme with generic point η, $u : X \to S$ a morphism of finite type. For $s \in S$, let $X_s := u^{-1}(s) = X \times_S \operatorname{Spec}(\mathbf{k}(s))$. Let E be the set of $s \in S$ where $\mathbf{P}(X_s, \mathbf{k}(s))$ holds. Then one of the sets E, $S \setminus E$ contains a nonempty open set (and is therefore a neighbourhood of η).

It is clear that a Boolean combination of constructible properties is again a constructible property.

A similar definition to 2.4 should make sense for properties of several schemes, morphisms between schemes, or constructible subsets. In particular:

Definition 2.5. Let $\mathbf{P}(f, X, Y, k)$ be an relation. We say that $\mathbf{P}$ is a *constructible property* (of morphisms of schemes), if the following conditions are satisfied:

(1) If k is a field, $f : X \to Y$ a map of schemes over k, and k' is an extension of k, $\mathbf{P}(f, X, Y, k)$ holds if and only if $\mathbf{P}(f_{(k')}, X_{(k')}, Y_{(k')}, k')$ does.
(2) Let S be an integral noetherian scheme with generic point η, X, Y two S-schemes of finite type and $f : X \to Y$ an S-morphism. For $s \in S$, let $X_s := X \times_S \operatorname{Spec}(\mathbf{k}(s))$, $Y_s := Y \times_S \operatorname{Spec}(\mathbf{k}(s))$ and $f_s := f \times 1 : X_s \to Y_s$. Let E be the set of $s \in S$ where $\mathbf{P}(f_s, X_s, Y_s, \mathbf{k}(s))$ holds. Then one of the sets E, $S \setminus E$ is a neighbourhood of η.

The above definition is equivalent to the usual model-theoretic definition, as the following proposition ([7], 9.2.3) shows.

Proposition 2.6. *Let $\mathbf{P}$ be a constructible property of algebraic schemes (resp. of morphisms of schemes), S a scheme, X, Y S-schemes of finite type, and $f : X \to Y$ an S-morphism. Then the set E of $s \in S$ for which $\mathbf{P}(X_s, \mathbf{k}(s))$ (resp. $\mathbf{P}(f_s, X_s, Y_s, \mathbf{k}(s))$) holds is constructible. Moreover, if S is irreducible with generic point η, one of the sets E, $S \setminus E$ is a neighbourhood of η.*

The moral of the whole story of constructible properties is that the behaviour of a constructible property is "generically determined" by the generic point.

The following is an easy modification of [7], 9.3.1.

Proposition 2.7. *Let $\mathbf{P}(X, k)$ be a constructible property of algebraic schemes. Denote by $\mathbf{P}'(f, X, Y, k)$ (resp. $\mathbf{P}''(f, X, Y, k)$) the following relation: $f : X \to Y$ is a k-morphism of k-schemes such that $\mathbf{P}(f^{-1}(y), \mathbf{k}(y))$ for all $y \in Y$ (resp. for generic $y \in Y$). Then $\mathbf{P}'$ and $\mathbf{P}''$ are constructible properties of morphisms of schemes.*

Recall that a *finite* algebraic scheme X over a field k is isomorphic to $\mathrm{Spec}(A)$, where A is an artinian ring, which also happens to be a k-algebra of finite rank. This rank we shall call the *total rank* of X. The *separable rank* of X is $\sum_{x\in X}[\mathbf{k}(x):k]_{\mathrm{sep}}$, which equals the geometric number of points of X ([5], 6.4.5, 6.4.7).

Theorem 2.8. *The properties of a k-algebraic scheme X listed below are constructible:*

(1) *X is empty.*
(2) *X is finite over k.*
(3) *$\dim(X)$ belongs to a given set $\Phi \subseteq \mathbb{Z}\cup\{-\infty\}$.*
(4) *X is geometrically irreducible/reduced/integral/connected.*
(5) *number of geometric components of X belongs to some Φ;*
(6) *X is geometrically normal/regular.*
(7) *X is finite of (total, separable) rank that belongs to some Φ.*

Proof. The items (1)–(3), (4)–(5) and (6) are [7], 9.2.6, 9.7.7 and 9.9.5. For (7), the case of separable rank is included in (5). Let us sketch the proof for the case of total rank. The first property of 2.4 is [5], 6.4.6, so it remains to check the second.

Assume $f : X \to S$ is a quasifinite map with S integral noetherian with generic point η. We need to show that the rank of the fibres is constant in a neighbourhood of η. However, by localising S, we may assume that f is finite and even flat, by the generic flatness theorem ([6], 6.9.1). It is well-known that the rank is constant in that case ([15], III.10). □

Theorem 2.9. *The following properties of maps between algebraic schemes are constructible:*

(1) *surjective;*
(2) *dominant;*
(3) *separated;*
(4) *proper;*
(5) *radical;*
(6) *finite;*
(7) *quasi-finite;*
(8) *generically finite of degree (total, separable, purely inseparable) that belongs to some Φ;*
(9) *an immersion (open, closed);*
(10) *an isomorphism.*

Proof. All the properties except (8) can be found in [7] as 9.6.1. The item (8) follows from 2.7 and 2.8(7), because when $X \to Y$ is a dominant generically finite map of integral schemes, its (separable, total) degree is exactly the (separable, total) rank of the generic fibre. The purely inseparable degree is also constructible being the quotient of the total and the separable degree. □

Example 2.10. Let k be an algebraically closed field of characteristic $p > 0$, let $X = \mathbb{A}^1_k = \mathrm{Spec}(k[x])$ and let $f : X \to X$ be given by $x \to x^p$. The fibres of closed points $x \in X$ are non-reduced of rank p, and the generic fibre is integral of rank p, which coincides with the degree of f.

The following is a well-known way of treating individual schemes as fibres of families of schemes. In model theory, it corresponds to taking the canonical parameter for the variety (resp. morphism) and then writing the individual variety

(resp. morphism) as a generic element of a family over the quantifier-free type of the canonical parameter.

Lemma 2.11. *Let S and S' be irreducible varieties over $\mathbb{Z}$ (resp. $\mathbb{F}_p$) with generic points η and η'. Let X be an S-scheme of finite type and Y a separated S'-scheme of finite type. Let $f_0 : X_\eta \to Y_{\eta'}$ be a morphism. Then there exists an irreducible variety S'' of finite type over $\mathbb{Z}$ with generic point ν equipped with dominant maps to S and S' and an S''-map $f : X_{(S'')} \to Y_{(S'')}$ such that the original f_0 can be identified with f_ν.*

Proof. Let $K := \mathbf{k}(\eta)$, $K' := \mathbf{k}(\eta')$ be the residue fields at the given generic points. It follows from the assumptions and [6], 4.8.13 that there is a field of definition of f_0, denoted K'', of finite type over KK'. In the spirit of [7], 8.1, there exists a scheme S'' with function field K'', as well as an S''-map $f : X_{(S'')} \to Y_{(S'')}$ with the required properties. □

There is an intimate connection between the existence of bounds on polynomial ideals defining varieties under consideration and constructibility.

Definition 2.12. (1) The *complexity* of a variety X is the minimum (in the lexicographical ordering) of the number, as well as the degrees, of polynomials defining an open affine covering of X and the "gluing" maps between them. Similarly we can define complexity for constructible sets and for algebraic maps.

(2) We say that an algebraic-geometric operation is of *bounded complexity* if, for a given complexity n, there exists an N such that for varieties of complexity at most n the result of the operation is of complexity at most N.

Clearly, knowing that certain operations in algebraic geometry are of bounded complexity has direct consequences for constructibility. This approach was pioneered in [17] and its use of nonstandard methods is of great importance for model theory.

On the other hand, constructibility also has implications toward bounded complexity:

Proposition 2.13. *The following operations are of bounded complexity:*

(1) *taking the image of a constructible set by an algebraic map;*
(2) *taking the closure of the image of a constructible set;*
(3) *given a constructible property $\mathbf{P}$, taking the constructible set $E := \{y \in Y : \mathbf{P}(X_y, \mathbf{k}(y))\}$, for a map $X \to Y$.*

Proof. Let us prove (1) and (2) simultaneously. Let $f_i : X_i \to Y_i$ be k_i-maps and let E_i be constructible in X_i of bounded complexity. Suppose that the complexity of $f_i(X_i)$ (resp. $\overline{f_i(X_i)}$) is unbounded. By taking the ultraproduct, we get a map of ordinary varieties over the ultraproduct field K. For a model-theorist, the proof terminates in one step by using Los' theorem, because the projection of the ultraproduct constructible set will be the projection for almost all i.

Alternatively, (by 2.11), the ultraproduct map can be considered as the generic fibre of a map of S-schemes $X \to Y$ for S integral of finite type over the prime subfield with generic point η. However, if we take a constructible (resp. closed) subset Z of Y such that $Z \cap Y_\eta = f_\eta(E_\eta)$ (resp. $Z \cap Y_\eta = \overline{f_\eta(E_\eta)}$), by [7], 9.5.2 and

9.5.3, it follows that there is a dense open subset of S on which $Z_s = f_s(E_s)$ (resp. $Z_s = \overline{f_s(E_s)}$). By devissage on S we contradict the assumption of unboundedness.

For (3), let $\mathbf{P}$ be a constructible property, and assume $X_i \to Y_i$ are k_i-maps of bounded complexity and suppose E_i are the corresponding constructible sets of unbounded complexity. As above, take the ultraproduct and get the relevant map of S-schemes $X \to Y$, for S integral of finite type over the prime subfield. If we consider X as a scheme over $S \times Y$, by 2.6 we get that $E := \{(s, y) : \mathbf{P}(X_{(s,y)}, \mathbf{k}(s, y))\}$ is constructible. Then, for s in S, $E_s = \{y \in Y_s : \mathbf{P}((X_s)_y)\}$, which gives a bound on the complexity of the latter sets. □

A similar proof shows that a constructible function of varieties or maps takes only finitely many values when we bound the complexity. For example, there is a bound on the number of geometric components of varieties of bounded complexity.

3. Quantifier-free case

A *difference ring* is a ring R with a distinguished homomorphism σ. As already mentioned in the introduction, a difference field is a field K with a distinguished *automorphism* σ. The language of difference rings, apart from the usual symbols of the language of rings, contains an unary function symbol for σ, and we refer to formulae in this language as σ-formulae.

Definition 3.1. Let (K, σ) be a difference field. Let X be some variety over K and let W be a closed subvariety of $X \times \sigma(X)$. We introduce the notation for the set of fixed K-points of the correspondence W twisted by σ:

$$X^{W^\sigma}(K) := \{x \in X(K) : (x, \sigma(x)) \in W(K)\}.$$

Mostly we will apply this to the special case of fields K_q (defined in the Introduction), in which case we will denote this set by $X^{W^q}(K_q)$.

We make significant use of the following results of Hrushovski, appearing as 1.1B, 1.1 and 16.1 in [9].

Theorem 3.2. *Assume the following.*

1. *Let S and S' be reduced, irreducible, separated schemes of finite type over $\mathbb{Z}$ and let a (base change) map $\tau : S' \to S^2$ be also given. Let X be a scheme over S. View X^2 as a scheme over S^2, and let W be a (S'-) subscheme of $X^2 \times_{S^2} S'$. For L a field and $s \in S'(L)$, denote $\tau(s) = (s_1, s_2) \in S^2(L)$. We will assume that X_{s_1}, X_{s_2} and W_s are varieties and view W_s as a subvariety of $X_{s_1} \times X_{s_2}$.*
2. *We further assume that for $s \in S'$, W_s, X_{s_1}, X_{s_2} are geometrically irreducible, the projection $W_s \to X_{s_2}$ is a quasi-finite map of purely inseparable degree δ', $\dim(X_{s_1}) = \dim(X_{s_2}) = \dim(W_s) = d$, the total degree of $W_s \to X_{s_1}$ is δ.*
3. *Let $t \in S(K_q)$, $s \in S'(K_q)$ such that $\tau(s) = (t, \phi_q(t))$. In this situation, let*

$$X_t^{W_s^q}(K_q) = \{c \in X_t(K_q) : (c, \phi_q(c)) \in W_s(K_q)\}.$$

Then there exists an open ($\mathbb{Z}$ or $\mathbb{F}_p$) subscheme S'' of S' and a constant $C > 0$ such that if $s \in S''(K_q)$ with $\tau(s) = (t, \phi_q(t))$, then

$$\left|\mathrm{card}\left(X_t^{W_s^q}(K_q)\right) - \delta/\delta' q^d\right| \leq C q^{d-1/2}.$$

Since fixing the base change $S' \to S^2$ determines some of the difference type of the parameters of W, and we do not wish to develop the theory of constructibility for difference schemes for the purposes of this paper, we opt for the following, "bounded complexity" version.

Theorem 3.3. *Let X be an affine variety over K_q, and let $W \subseteq X \times X^{\phi_q}$ be an irreducible subvariety. Assume $\dim(W) = \dim(X) = d$, the map $W \to X$ is dominant of degree δ and $W \to X^{\phi_q}$ is quasifinite of purely inseparable degree δ'. There is a constant C depending on the complexity of X and W (but not on q or the parameters from K_q) such that*

$$\left|\mathrm{card}\left(X^{W^q}(K_q)\right) - \delta/\delta' q^d\right| \leq C q^{d-1/2}.$$

Theorem 3.4. *Let X be a smooth algebraic variety over a difference field (K, σ). Let $W \subseteq X \times X^\sigma$ be a geometrically reduced and irreducible subvariety with $\dim(W) = \dim(X) + e$. Assume W projects dominantly to X and X^σ. Let Z be the difference scheme described by $\{x \in X : (x, x^\sigma) \in W\}$. Then any component of Z has transformal dimension at least e.*

Remark 3.5. We leave the difference scheme properties from the theorem above undefined, because they are beyond the content of this paper. We will use the theorem to the following extent. If X and W over some K_q are as above and $e > 0$, then $X^{W^q}(K_q)$ is infinite.

Next we show how to break up an arbitrary situation into pieces which all satisfy the requirements of 3.3 or 3.4. We were subsequently informed by Zoe Chatzidakis that our procedure is a variant of the construction appearing in [8].

Lemma 3.6. *Let (K, σ) be a difference field, and let W be a subvariety of $X \times X^\sigma$. Then we can find, by operations of bounded complexity, geometrically irreducible X_i and distinct geometrically irreducible W_i, $i < n$, as well as numbers $d_i, e_i, \delta_i, \delta_i' \in \mathbb{Z} \cup \{\infty\}$, $i < n$, such that:*

(1)
$$X^{W^\sigma}(K) = \bigcup_{i<n} X_i^{W_i^\sigma}(K);$$

(2) *for every $i < n$, W_i projects dominantly onto X_i and X_i^σ;*
(3) *when $d_i := \dim(W_i) = \dim(X_i)$ then moreover $W_i \to X_i$ is generically finite of degree $\delta_i \in \mathbb{Z}$, and $W_i \to X_i^\sigma$ is quasifinite of purely inseparable degree $\delta_i' \in \mathbb{Z}$.*
(4) *when $e_i := \dim(W_i) - \dim(X_i) > 0$, X_i is smooth and, by 3.4, we stipulate $\delta_i = \infty$.*

If W and X come from families like in 3.2(1), there is a finite set $\mathcal{D}$ of sequences $\Delta = (d_i, e_i, \delta_i, \delta_i' : i < n)$ such that for every $s \in S'(K)$ there is a $\Delta \in \mathcal{D}$ such that W_s "decomposes in a Δ-way".

Moreover, for each $\Delta \in \mathcal{D}$, there is a σ-formula $\varphi_\Delta(z)$ such that $W_s \subseteq X_t \times X_{\sigma(t)}$ decomposes in a Δ-way if and only if $\varphi_\Delta(s)$.

Proof. We argue by induction on geometric number of components and dimension of W, as well as the complexity of W and X. We repeat the same procedure for all geometric components of W so we may assume that W is geometrically irreducible. Let X_1 and X_2 be closures of projections of W in X and X^σ, respectively. It is

clear that X_1 and X_2 are again geometrically irreducible and we can distinguish the following two cases.

When $X_1 \neq \sigma^{-1}(X_2)$, we replace X by $X' = X_1 \cap \sigma^{-1}(X_2)$ and W by $W' = W \cap X' \times \sigma(X')$ and we continue by induction.

Let us consider the case $X_1 = \sigma^{-1}(X_2)$. Clearly $\dim(X_1) \leq \dim(W)$. If $\dim(X_1) < \dim(W)$, we write X_1 as a disjoint union of X_o and X_s, where X_s is the singular locus (a proper closed subset). Then the sets $W \cap X_o \times \sigma(X_o)$ and $W \cap X_s \times \sigma(X_s)$ are either as required or we proceed by induction (the mixed terms $X_s \times \sigma(X_o)$ and $X_o \times \sigma(X_s)$ have no points of the form $(x, \sigma(x))$.

If $\dim(X_1) = \dim(X_2) = \dim(W)$, let $X_2' \subseteq X_2$ be open such that the map $W_\eta \to X_{\eta_2}$ is quasifinite on X_2' and let C be the (proper closed) complement of X_2' in X_2. Then W decomposes as W intersected by $\sigma^{-1}(X_2') \times X_2'$, $\sigma^{-1}(C) \times C$ and mixed terms. Mixed terms have no points of form $(x, \sigma(x))$, the first one is as required and the second one is of lower dimension and we continue by induction.

It is clear that the induction finishes in boundedly many steps since all the operations involved are of bounded complexity:

(1) cartesian products and intersections just by definition;
(2) taking geometrically irreducible components by [17];
(3) Zariski closures of images by 2.13(2);
(4) taking an open set where a generically finite morphism is quasifinite by 2.13(3) and 2.8(7).
(5) taking the geometric nonsingular locus of a variety, by 2.13(3) and 2.8(6).

Therefore, in view of 2.9, there exists the sought-after formula φ_Δ describing the situation. □

Corollary 3.7. *Let $X \to S$, $W \to S'$, $S' \to S^2$ be as in 3.2(1). Then there exists a constant $C > 0$ depending only on the complexity of X and W and a finite set D of pairs (d, μ) with $d \in \mathbb{Z} \cup \{\infty\}$, $\mu \in \mathbb{Q}^+ \cup \{\infty\}$ such that for large enough q, for $s \in S'(K_q)$ mapping onto $(t, \phi_q(t)) \in S^2(K_q)$, there exist $(d, \mu) \in D$ such that*

$$\left|\mathrm{card}\left(X_t^{W_s^q}(K_q)\right) - \mu q^d\right| \leq C q^{d-1/2}.$$

Moreover, for every (d, μ) in D, there is a σ-formula $\varphi_{(d,\mu)}(z)$ such that the above estimate holds for s if and only $(K_q, \phi_q) \models \varphi_{(d,\mu)}(s)$.

Proof. Given an $s \in S'(K_q)$, apply the previous lemma to get the 'components' W_i and X_i, $i < n$. If there is one i where $\dim(X_i) < \dim(W_i)$, the required number of points is infinite by 3.5 and no discussion is required. Thus we may suppose that $\dim(X_i) = \dim(W_i)$ for all $i < n$ and all the second projections are quasifinite.

We proceed by induction on $d := \max\{\dim(W_i) : i < n\}$. By rearranging the W_i we may assume that $\dim(W_i) = d$ for $i < m$ and $\dim(W_i) =: d_i < d$ for $m \leq i < n$. We claim that the numbers d and $\mu := \sum_{i<m} \delta_i/\delta_i'$ are as required. Indeed, if we denote by $N_{i,q}$ the generic number of counted K_q-points coming from W_i, we have:

(1) for $i < m$, $\left|N_{i,q} - (\delta_i/\delta_i')q^d\right| < C_i q^{d-1/2}$;
(2) for $m \leq i < n$, $\left|N_{i,q} - (\delta_i/\delta_i')q^d\right| < C_i q^{d-1/2}$;
(3) the number of double-counted points comes from $W_i \cap W_j$ for $i \neq j < n$, which are of dimension less than d.

It is clear that the required formulae $\varphi_{(d,\mu)}$ can be obtained by Boolean combinations of φ_Δ from 3.6. □

Corollary 3.8. *Let $\theta(X, Y)$ be a quantifier-free formula in the language of difference rings. Then there exist positive constant C such that for each $x \in K_q$ with large enough q there exist $\mu \in \mathbb{Q}^+ \cup \{\infty\}$ and $d \in \mathbb{Z} \cup \{\infty\}$ such that*

$$\left|\mathrm{card}(\theta(x, K_q)) - \mu q^d\right| \leq C q^{d-1/2}.$$

Moreover, the function $x \mapsto (d, \mu)$ is definable in the language of difference rings (and it has finitely many values). We denote by $\theta_{(d,\mu)}(X)$ the σ-formula which in each K_q (with large enough q) defines the set of x such that the above estimate holds for the pair (d, μ).

Proof. By the methods of [3], 3.5, we may assume that the formula is *positive* quantifier-free, i.e. just a system of σ-polynomial equations.

Let us describe the folklore translation of such a system into a correspondence ([13]). We may assume the system is of the following form:

$$f_i(X; Z, \sigma Z, \ldots, \sigma^m Z) = 0, \text{ for } i < n,$$

where X is a tuple of parametric variables. The solutions of this system are clearly in bijection with the solutions of the system

$$\begin{aligned} f_i(X; Y_0, \ldots, Y_m) &= 0, \quad i < n \\ Y_{j+1} &= \sigma Y_j, \quad j < m. \end{aligned}$$

Let $Y = (Y_0, \ldots, Y_{m-1})$, and denote by $\tilde{f}_i$ the polynomials such that $\tilde{f}_i(X, Y, Y') = f_i(X, Y, Y'_{m-1})$, for $i < n$. If we let $S' = \mathbb{A}^k$, where k is the length of the parametric variable X, and if we let W be the S'-variety defined by polynomials $\tilde{f}_i$, for a given $x \in S'$, the solutions to the system above is in bijection with the set

$$\{y \in \mathbb{A}^m : (y, \sigma(y)) \in W_x\}.$$

Thus we have obtained a correspondence $W \to S'$ equipped with two projections into the affine space $X := \mathbb{A}^m$ (over say $S = \mathrm{Spec}(\text{prime subfield})$). This brings us into the setup of the previous corollary. □

Remark 3.9. If we had a refinement of 3.4, which guaranteed that the transformal dimensions are exactly e, our considerations would allow extracting even the transformal dimension as a definable invariant, although the interesting case for us is when it is 0, when we get some form of the total dimension and measure.

4. Main theorem and applications

Using the particular form of quantifier elimination for ACFA ([2], 1.6, 1.8), together with the fact that ACFA is the theory of fields K_q ([9]), we obtain the following.

Fact 4.1. *Every formula $\varphi(X, Y)$ (X parameter variables) in the language of difference rings is equivalent, uniformly for all fields K_q, to a disjunction of formulae of the form*

$$\exists T \theta(X, Y, T),$$

where T is a single variable, θ is quantifier-free, and there is a number e such that for every K_q, and all $x \in K_q^m$ and $y \in K_q^n$, the number of $t \in K_q$ with $\theta(x, y, t)$ is at most e.

This is exactly the form of quantifier elimination needed to axiomatically transfer the proof of [3], 3.7 to our context, using our result 3.8 for quantifier-free formulae. Thus we may consider our Main Theorem 1.1 proved.

Now we are ready to interpret the numbers d and μ as an appropriate kind of *dimension* and *measure* in a model of $ACFA$.

Let $\varphi(X,Y)$ be a formula, and let C, D be as in the theorem above. Then, for all fields K_q with sufficiently large q, and for every tuple $x \in K_q^n$, there exists a unique pair $(d,\mu) \in D$ with $|\operatorname{card}(\varphi(x,K_q^n)) - \mu q^d| \leq Cq^{d-(1/2)}$. Hence, there exists a unique pair $(d,\mu) \in D$ such that $K_q \models \varphi_{(d,\mu)}(x)$. Therefore, by the main result of [9], the same will be true in a model of ACFA as well.

Definition 4.2. If S is a set definable in a model K of ACFA by the formula $\varphi(x,Y)$ for $x \in K^n$, then we define the pair $(d(S),\mu(S))$ to be the unique pair $(d,\mu) \in D$ such that $K \models \varphi_{(d,\mu)}(x)$.

Proposition 4.3. *Let K be a model of ACFA.*

(1) *For a definable set S, $d(S) = 0$ if and only if S is finite.*
(2) *If S and T are disjoint definable sets, then*

$$\mu(S \cup T) = \begin{cases} \mu(S) + \mu(T) & \text{if } d(S) = d(T), \\ \mu(S) & \text{if } d(S) > d(T), \\ \mu(T) & \text{if } d(S) < d(T). \end{cases}$$

(3) *Let $f : S \to T$ be a definable function. If for all $a \in T$, $d(f^{-1}(a)) = d$ then $d(S) = d(T) + d$. If additionally for all $a \in T$, $\mu(f^{-1}(a)) = m$, then $\mu(S) = m\mu(T)$.*
(4) *(The S_1-property). Assume that $d(\varphi(Y)) = n$. For any formula $\psi(X,Y)$, there is no infinite sequence $(a_i)_{i\in I}$ such that for all $i \in I$, $d(\varphi(Y) \wedge \psi(a_i,Y)) = n$ and for all $i \neq j \in I$, $d(\varphi(Y) \wedge \psi(a_i,Y) \wedge \psi(a_j,Y)) < n$.*

Proof. The properties (1)–(3) are obtained by arguing over fields K_q for large q by straightforward counting arguments. For the property (4), suppose there is such an infinite family. Then $\mu(\varphi(Y)) \geq \sum_i \mu(\varphi(Y) \wedge \psi(a_i,Y))$, which is a contradiction, because all the numbers in the sum belong to a finite set of positive rational numbers. □

Remark 4.4. As already remarked in 7.13 of [2], any definable rank satisfying the properties above, if finite, will bound the S_1 and therefore SU-rank. So we can argue that we have obtained a measurability result for formulae of finite S_1-rank in ACFA.

The function $\deg_\sigma$ from loc. cit. satisfies these properties, and by careful analysis of what we have done, we get:

Proposition 4.5. *Let S be a definable set in a saturated model K of ACFA, defined over a (small) set A. The rank d defined above is equal to*

$$\sup\{\deg_\sigma(x/\operatorname{acl}_\sigma(A)) : x \in S\}.$$

Proof. It is easily seen that the set defined using X and W of dimension d like in 3.3 has $\deg_\sigma$ exactly d.

Thus, d and $\deg_\sigma$ agree on quantifier-free σ-sets. Moreover, since both behave well with respect to finite covers, they coincide for all definable sets. □

Remark 4.6. Let K be a model of ACFA and let $S \subseteq K^n$ be a definable set. By $\mathrm{Def}(S)$ we denote the set of all definable subsets of S. The μ from above induces a finitely additive measure μ_S on $\mathrm{Def}(S)$ by:

$$\mu_S(T) := \begin{cases} \mu(T)/\mu(S) & \text{if } d(T) = d(S), \\ 0 & \text{if } d(T) < d(S). \end{cases}$$

Remark 4.7. To tie in our results with those of [3], suppose (K, σ) is a model of $ACFA$. It is well-known ([13], [2]) that the fixed fields F_k of σ^k are pseudofinite fields. Thus, by [3], each F_k has an appropriate dimension/measure pair (d_k, μ_k).

Clearly, if $S \subseteq K^n$ is a set definable in the language of rings, $(d_k(S), \mu_k(S))$ coincides with our $(d(S \cap F_k^n), \mu(S \cap F_k^n))$ from 4.2.

Remark 4.8 (Stable finite dimensional reducts of ACFA are locally modular). The measurability of the finite dimensional part of ACFA in 4.6 clearly implies the following notion of unimodularity in the sense of Hrushovski.

Let A and B be finite-dimensional definable sets in ACFA. Let f_1 and f_2 be definable surjections from A onto B, with constant finite fibre sizes $k_1, k_2 \in \mathbb{N}$ respectively. Then $k_1 = k_2$.

Now let $\mathcal{R}$ be a finite dimensional stable reduct in ACFA. Since ACFA is supersimple, $\mathcal{R}$ is superstable of finite rank. Furthermore, $\mathcal{R}$ must also be Hrushovski unimodular. Then, by the main result of [10], all the minimal types of $\mathcal{R}$ are locally modular.

Remark 4.9 (Finite simple groups). Macintyre and Hrushovski both remarked that one can interpret asymptotic twisted simple groups of Lie type (${}^2B_2$, ${}^2G_2$, ${}^2F_4$) inside ACFA. The first author has made this concrete in upcoming work; he shows that the families of finite simple group of the above type are uniformly bi-interpretable with families of finite difference fields. The latter appear asymptotically as definable sets inside models of ACFA. Using [9] the asymptotic theories of the above families of finite simple groups are determined. Furthermore, for any collection of finite simple groups of Lie type (twisted or untwisted), uniform estimates in the same form as those in 1.1 are obtained for any family of sets definable in the language of groups.

References

[1] James Ax. The elementary theory of finite fields. *Annals of Mathematics (2)*, 88:239–271, 1968.

[2] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Transactions of the American Mathematical Society*, 351(8):2997–3071, 1999.

[3] Zoé Chatzidakis, Lou van den Dries, and Angus Macintyre. Definable sets over finite fields. *Journal für die reine und angewandte Mathematik*, 427:107–135, 1992.

[4] Kazuhiro Fujiwara. Rigid geometry, Lefschetz-Verdier trace formula and Deligne's conjecture. *Invent. Math.*, 127(3):489–533, 1997.

[5] A. Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[6] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. *Inst. Hautes Études Sci. Publ. Math.*, (24):231, 1965.

[7] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. *Inst. Hautes Études Sci. Publ. Math.*, (28):255, 1966.

[8] Ehud Hrushovski. The Manin-Mumford conjecture and the model theory of difference fields. *Annals of Pure and Applied Logic*, 112(1):43–115, 2001.

[9] Ehud Hrushovski. The elementary theory of the Frobenius automorphism. Submitted, 2004.

[10] Ehud Hrushovski Unimodular minimal theories *Journal of the London Mathematical Society*, Ser. 2, 46, 385-396,1992.
[11] Laurent Lafforgue. Chtoucas de Drinfeld et correspondance de Langlands. *Invent. Math.*, 147(1):1–241, 2002.
[12] Angus Macintyre. Nonstandard Frobenius. In preparation.
[13] Angus Macintyre. Generic automorphisms of fields. *Annals of Pure and Applied Logic*, 88(2-3):165–180, 1997. Joint AILA-KGS Model Theory Meeting (Florence, 1995).
[14] Angus Macintyre. Weil cohomology and model theory. In Angus Macintyre, editor, *Connections between Model Theory and Algebraic and Analytic Geometry*, volume 6 of *Quaderni di matematica*. Seconda Università di Napoli, 2000.
[15] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, expanded edition, 1999. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.
[16] Richard Pink. On the calculation of local terms in the Lefschetz-Verdier trace formula and its application to a conjecture of Deligne. *Annals of Mathematics. Second Series*, 135(3):483–525, 1992.
[17] L. van den Dries and K. Schmidt. Bounds in the theory of polynomial rings over fields. A nonstandard approach. *Inventiones Mathematicae*, 76(1):77–91, 1984.

Mark Ryten, School of Mathematics, University of Leeds, Leeds LS2 9JT, United Kingdom
E-mail address: mjryten@amsta.leeds.ac.uk

Ivan Tomašić, Institut Girard Desargues, Université Lyon I, 69622 Villeurbanne cedex, France
E-mail address: tomasic@igd.univ-lyon1.fr