Model Theory

no. 2 vol. 2 2023

$M \nvDash T$

Remarks around the nonexistence of difference closure

Zoé Chatzidakis

msp

msp
Model Theory
Vol. 2, No. 2, 2023
https://doi.org/10.2140/mt.2023.2.405

Remarks around the nonexistence of difference closure

Zoé Chatzidakis

This paper shows that in general, difference fields do not have a difference closure. However, we introduce a stronger notion of closure (κ-closure), and show that every algebraically closed difference field K of characteristic 0, with fixed field satisfying a certain natural condition, has a κ-closure, and this closure is unique up to isomorphism over K.

Introduction

In this paper, a difference field is a field K with a distinguished automorphism σ. A difference field L is *difference closed* if every finite system of difference equations with coefficients in L which has a solution in a difference field extending L, already has a solution in L.

If K is a difference field, then a *difference closure of* K is a difference closed field containing K, and which K-embeds into every difference closed field containing K.

The algebra of difference fields was developed by Ritt, in analogy with the algebra of differential fields. It is well-known that any differential field of characteristic 0 has a differential closure, and that this differential closure is unique up to isomorphism over the field. In 2016, Michael Singer asked whether this result generalises to the context of difference fields. One of the main results of this paper is that it does not, even after imposing some natural conditions on the difference field K. We will show by two examples (Examples 1.3 and 1.4) that even the existence of a difference closure can fail.

There are several natural strengthenings of the notions of difference closed and difference closure (originating from model theory but having a natural algebraic translation), and we will show that these notions do satisfy existence and uniqueness of closure, provided we work over an algebraically closed difference field of characteristic 0 whose fixed subfield is large enough.

The theory of difference closed difference fields has been extensively studied, and is commonly denoted by ACFA. The proof of our result uses in an essential

Partially supported by ANR–13-BS01-0006 (ValCoMo), ANR–17-CE40-0026 (AGRUME) and AAPG2019 (ANR-DFG Geomod).

MSC2020: 03C50, 03C60, 03C98, 12Hxx.

Keywords: difference fields, prime models.

way the characteristic 0 hypothesis, as it allows us to use techniques of stability theory. They provide examples of structures which are stable over a predicate; see [13; 14] for definitions. The main result of the paper is as follows:

Theorem 3.14. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$, and let K be an algebraically closed difference field of characteristic* 0 *such that $F := \mathrm{Fix}(\sigma)(K)$ is pseudofinite and is κ-saturated. Then there is a κ-prime model of* ACFA *over K. Furthermore, it is unique up to isomorphism over K.*

Here is an algebraic translation of this result for $\kappa \geq \aleph_1$: Call a difference field $\mathcal{U}$ *κ-closed* if every system of $< \kappa$ difference equations over $\mathcal{U}$ which has a solution in some difference field extending $\mathcal{U}$ has a solution in $\mathcal{U}$. The field $\mathcal{U}$ is a *κ-closure* of the difference field K if it is κ-closed, contains K, and K-embeds into every κ-closed difference field containing K. Then Theorem 3.14 states, for $\kappa \geq \aleph_1$:

> *Let K be an algebraically closed difference field of characteristic* 0, *whose fixed field F is pseudofinite and such that every system of $< \kappa$ polynomial equations over F which has a solution in a regular extension of F already has a solution in F. Then K has a κ-closure, and it is unique up to K-isomorphism.*

It is unlikely that this result can be generalised to the characteristic p context, and in fact, I conjecture that unless the difference field K of characteristic $p > 0$ is of cardinality $< \kappa$ or is already κ-closed, then it does not have a κ-closure.

The paper is organised as follows. In Section 1 we discuss the problem and reformulate it in model-theoretic terms, and describe the two examples. In Section 2, we state the preliminary results we will need from difference algebra and model theory. Section 3 contains the proof of Theorem 3.14.

1. Discussion of the problems and the examples

1.1. ***Notation and conventions.*** All difference fields will be inversive, i.e., the endomorphism σ will be onto. Let K be a difference field, contained in some large difference field $\mathcal{U}$. If a is a tuple in $\mathcal{U}$, we denote by $K(a)_\sigma$ the difference field generated by a over K, i.e., the subfield $K(\sigma^i(a))_{i\in\mathbb{Z}}$ of $\mathcal{U}$. The algebraic and separable closure of a field L are denoted by L^{alg} and L^s, respectively, and $G(K)$ denotes the absolute Galois group of K, i.e., $\mathcal{G}al(K^s/K)$. If $A \subset \mathcal{U}$, then $\mathrm{acl}(A)$ denotes the smallest algebraically closed difference field containing A; it coincides with the model-theoretic algebraic closure of A for the theory ACFA [5, Proposition 1.7]. We denote by $\mathcal{L}$ the language $\{+, -, \cdot, 0, 1, \sigma\}$.

1.2. ***Translation into model-theoretic terms.*** Let K be a difference field. Recall that any complete theory extending the theory ACFA of difference closed difference fields is supersimple, unstable, of SU-rank ω, and does not eliminate quantifiers, but it eliminates imaginaries. It is extensively studied in [5]. The reason ACFA does not eliminate quantifiers is that given an automorphism σ of a field K, there may be several nonisomorphic ways of extending σ to K^{alg}. So, the first obvious obstacle to the existence of a difference closure is that, and a natural condition to impose is to assume that K is algebraically closed. There is another natural condition one needs to impose: if L is difference closed, then its fixed field

$$\mathrm{Fix}(\sigma)(L) = \{a \in L \mid \sigma(a) = a\}$$

is pseudofinite. Moreover, every pseudofinite field can occur as the fixed field of some difference closed field [1]. Thus if L is the difference closure of a difference field K, then $\mathrm{Fix}(\sigma)(L)$ must be prime over $\mathrm{Fix}(\sigma)(K)$ (for its theory in the language of rings). Duret showed in [8] that any completion of the theory of pseudofinite fields has the independence property. From his proof one extracts easily the fact that nonalgebraic types are nonisolated, and this forces us to require in case K is countable that $\mathrm{Fix}(\sigma)(K)$ be pseudofinite in order to hope to have a difference closure. The case when K is uncountable is a little more complicated, the question is addressed and solved in [3].

It is therefore reasonable to make the following two assumptions:

K is algebraically closed, *and* $\mathrm{Fix}(\sigma)(K)$ *is pseudofinite.*

But even this is not enough. To show this does not suffice, what we need to do is the following:

> *Exhibit a difference field K satisfying the above two conditions*, *and a finite system of difference equations which does not have a solution in K*, *and such that any finite strengthening of this system has several completions.*

This looks easy, since even our stable types are only superstable, not ω-stable. However, the first obvious examples do not satisfy the first condition. Here is a more involved example, taken from [5, Example 6.7]:

Example 1.3 (an example in characteristic 0). Let k be a countable pseudofinite field of characteristic 0 containing $\mathbb{Q}^{\mathrm{alg}}$, and consider $K = (k^{\mathrm{alg}}, \sigma)$, where σ is a (topological) generator of $\mathcal{G}al(K/k)$. We consider the elliptic curve J_a, with j-invariant $a \notin K$, and which is defined by

$$y^2 + xy = x^3 - \frac{36}{a-1728}x - \frac{1}{a-1728}.$$

We let A' be a cyclic subgroup of J_a of order p^2, $A = [p]A'$ and a_1 the j-invariant of the elliptic curve J_a/A, a_2 the j-invariant of the elliptic curve J_a/A'. Then the map $\mathbb{Q}^{\mathrm{alg}}(a, a_1) \to \mathbb{Q}^{\mathrm{alg}}(a_1, a_2)$ which is the identity on $\mathbb{Q}^{\mathrm{alg}}$ and sends (a, a_1) to (a_1, a_2) extends to a field automorphism of $\mathbb{Q}(a)^{\mathrm{alg}}$, which in turns extends to an automorphism of $K(a)^{\text{alg}}$ which agrees with σ on K. Let $\Phi(x, x_1, x_2)$ be the finite system of polynomial equations which describe the algebraic locus of (a, a_1, a_2) over K; in the notation of [11, Chapter 5, §3] (see in particular Theorem 5), $\Phi(x, x_1, x_2)$ can be written as

$$\Phi_{p^2}(x_2, x) = \Phi_p(x_1, x) = \Phi_p(x_2, x_1) = 0.$$

(The equation $\Phi_n(y, x) = 0$ says that y is the j-invariant of the quotient of the elliptic curve J_x with j-invariant x by a cyclic subgroup of order n.) We now consider the formula $\psi(x)$ given by $\Phi(x, \sigma(x), \sigma^2(x)) \wedge \sigma(x) \neq x$. Let b be any solution of $\psi(x)$. Note that necessarily, the kernel of the map $J_b \to J_{\sigma^n(b)}$ for $n > 0$ is cyclic of order p^n. Indeed, note that $\sigma^n(b)$ satisfies ψ for every n; hence, the kernel of the map $J_{\sigma^n(b)} \to J_{\sigma^{n+2}(b)}$ is cyclic of order p^2, and this map is the composite of the two maps $J_{\sigma^n(b)} \to J_{\sigma^{n+1}(b)}$ and $J_{\sigma^{n+1}(b)} \to J_{\sigma^{n+2}(b)}$, which both have kernel of order p. An easy induction then gives the result.

As $\sigma(b) \neq b$, we know that b is transcendental. Hence the curve J_b is not of CM-type, its endomorphism group is isomorphic to $\mathbb{Z}$, and therefore J_b is not isomorphic to any of its quotients by finite cyclic subgroups; see, e.g., [15, Section C.11]. Therefore, the elements $b, \sigma(b), \sigma^2(b), \ldots$ are all distinct, and $b \notin K$. Furthermore, the isomorphism type of $K(b)_\sigma$ over K is determined by $\Phi(b, \sigma(b), \sigma^2(b))$, because as we saw above, the kernel of the map $J_b \to J_{\sigma^n(b)}$ is cyclic of order p^n for $n > 0$ (see also the discussion at the bottom of page 3058 in [5]).

So any difference closed field containing K must contain a solution of $\psi(x)$. However, Example 6.7 of [5] shows that if b is as above, and L is any finite extension of $K(b)_\sigma$, then there are $2^{\aleph_0}$ nonisomorphic ways of extending σ to L^{alg}. Thus K does not have a difference closure.

One can build other examples along the same lines, using moduli spaces of abelian varieties.

Example 1.4 (an example in characteristic $p > 0$). Let $K = k(A)_\sigma^{\text{alg}}$, where k is a countable pseudofinite field fixed by σ, σ restricts to a generator of $\mathcal{G}al(k^{\text{alg}}/k)$, and A is the set of solutions of the equation $\sigma(x)^p - \sigma(x) + x^p = 0$ (in some countable difference closed overfield). Then in any difference closed field containing K, the set B of solutions of the equation $\sigma(x) - x^p + x = 0$ is an infinite-dimensional $\mathbb{F}_p$-vector space. However, as was shown in Example 6.5 of [5], there are $2^{|A|}$ ways of extending σ from $Kk(B)_\sigma^{\text{alg}}$ to $K(B)_\sigma^{\text{alg}}$: there is a definable nondegenerate bilinear map $q : A \times B \to \mathbb{F}_p$, which can be chosen totally arbitrarily.

In fact this example is part of a large family of examples: let f and g be additive polynomials with coefficients in a difference field K, and assume that the subgroup A of $\mathbb{G}_a$ defined by $f(x) = g(\sigma(x))$ is locally modular. Then there is a definable subgroup B of $\mathbb{G}_a$, and a definable nondegenerate bilinear map $A \times B \to \mathbb{F}_p$. As above, there is no prime model over $K(A)_\sigma$.

While we provided examples of difference fields not having a difference closure, we did not provide a procedure which, given a difference field which is not difference closed, exhibits a nonisolated type which needs to be realised. So, the following remains open:

Question 1.5. Are there any difference fields which are not difference closed but admit a difference closure?

Omar León Sánchez and Marcus Tressl introduced in [12] the notion of *large* differential fields of characteristic 0, and they showed that their (field-theoretic) algebraic closure are differentially closed, thus showing that the theory DCF_0 can have minimal prime models. One may try introducing the notion of *large* difference field, and hope for a similar result.

2. Preliminaries

Basic difference algebra.

2.1. Let $K \subset \mathcal{U}$ be difference fields. If $X = (X_1, \dots, X_n)$, the ring

$$K[X]_\sigma = K[\sigma^i(X_j)]_{1\le j\le n, i\in\mathbb{N}}$$

is called the *n-fold difference polynomial ring*. A *difference equation* is an equation of the form $f(X) = 0$ for some $f(X) \in K[X]_\sigma$.

If a is a finite tuple in $\mathcal{U}$, and L is a difference subfield of $K(a)_\sigma$ containing K, then $L = K(b)_\sigma$ for some finite tuple b [7, 5.23.18].

An element $a \in \mathcal{U}$ is *transformally algebraic* over K if it satisfies some nontrivial difference equation with parameters in K. Otherwise, it is *transformally transcendental* over K. A tuple a is *transformally algebraic over K* if all its elements are. A (maybe infinite) tuple of elements of $\mathcal{U}$ is transformally independent over K if it does not satisfy any nontrivial difference equation with coefficients in K. A *transformal transcendence basis of $\mathcal{U}$ over K* is a subset B of $\mathcal{U}$ which is transformally independent over K and maximal such; every element of K will then be transformally algebraic over $K(B)_\sigma$. We denote by $\Delta(K)$ the *transformal transcendence degree of K*, i.e., the cardinality of a transformal transcendence basis of K, and if L is a difference field containing K, by $\Delta(L/K)$ the cardinality of a transformal transcendence basis of L over K.

2.2. ***The fixed field.*** The fixed field of $\mathcal{U}$ is the field $\mathrm{Fix}(\sigma)(\mathcal{U}) := \{a \in \mathcal{U} \mid \sigma(a) = a\}$. Then $\mathrm{Fix}(\sigma)(\mathcal{U})$ and K are linearly disjoint over their intersection. (Choose n minimal such that there are $c_1, c_2, \dots, c_n \in \mathrm{Fix}(\sigma)$ and $d_1 = 1, d_2, \dots, d_n \in K$

such that $\sum_i c_i d_i = 0$; applying σ we get that $\sum c_i \sigma(d_i) = 0$, and by minimality of n, that $\sigma(d_i) = d_i$ for all i.) This implies in particular that if E is a difference subfield of K, then $E\,\mathrm{Fix}(\sigma)(\mathcal{U})$ and K are linearly disjoint over their intersection $E(\mathrm{Fix}(\sigma)(\mathcal{U}) \cap K)$. In positive characteristic, similar results hold for the other fixed fields $\mathrm{Fix}(\sigma^n\,\mathrm{Frob}^m)$.

Basic model-theoretic facts.

2.3. For references see [5]. The theory ACFA is supersimple, of SU-rank ω. It eliminates imaginaries, but does not eliminate quantifiers. The completions of ACFA are given by describing the isomorphism type of the automorphism σ of the algebraic closure of the prime field [5, Corollary 1.4].

We let $\mathcal{U}$ be a sufficiently saturated model of ACFA, and K a difference subfield of $\mathcal{U}$.

2.4. ***Types, algebraic closure, independence.*** If a is a tuple of elements of $\mathcal{U}$, then $\mathrm{tp}(a/K)$ is determined by the isomorphism type of the difference field $\mathrm{acl}(Ka) = K(a)_\sigma^{\mathrm{alg}}$ over K: a and b have the same type over K if and only if there is a K-isomorphism of difference fields $K(a)_\sigma \to K(b)_\sigma$ which sends a to b and extends to the algebraic closure of $K(a)_\sigma$ [5, Corollary 1.5]. The SU-rank of a over K, denoted by $\mathrm{SU}(a/K)$, is bounded by $\mathrm{tr.deg}(K(a)_\sigma/K)$, and is finite if and only if $\mathrm{tr.deg}(K(a)_\sigma/K)$ is finite (if and only if a is transformally algebraic over K).

Let A, B, C be subsets of $\mathcal{U}$. Then A is *independent from B over C*, denoted $A \mathrel{\unicode{x2AEB}}_C B$, if and only if the fields $\mathrm{acl}(AC)$ and $\mathrm{acl}(BC)$ are free over $\mathrm{acl}(C)$. Equivalently, if whenever a is a tuple of elements in A, then the prime σ-ideal $I_\sigma(a/\mathrm{acl}(BC)) := \{f(X) \in \mathrm{acl}(BC)[X]_\sigma \mid f(a) = 0\}$ is generated (as a σ-ideal) by its intersection with $\mathrm{acl}(C)[X]_\sigma$. Then independence coincides with nonforking, and we also say, in that case, that $\mathrm{tp}(A/BC)$ *does not fork over C*.

2.5. ***Reducts.*** For an integer $n > 0$, denote by $\mathcal{L}[n]$ the language $\{+, -, \cdot, 0, 1, \sigma^n\}$, and by $\mathcal{U}[n]$ the reduct $(\mathcal{U}, \sigma^n)$ to the language $\mathcal{L}[n]$. By [5, Corollaries to (1.12)], $\mathcal{U}[n] \models \mathrm{ACFA}$. If a is a tuple in $\mathcal{U}$, then $\mathrm{tp}(a/K)[n]$ denotes the type of a in the reduct $\mathcal{U}[n]$, and $\mathrm{qftp}(a/K)[n]$ the quantifier-free type of a in the reduct $\mathcal{U}[n]$.

2.6. ***Notions of canonical bases.*** If a is a tuple in $\mathcal{U}$, then $\mathrm{Cb}(a/K)$ denotes the smallest difference field over which $I_\sigma(a/K)$ is defined. Then $\mathrm{tp}(a/K)$ does not fork over $\mathrm{Cb}(a/K)$. Also, $\mathrm{Cb}(a/K)$ is contained in the algebraic closure over K of finitely many independent realisations of $\mathrm{tp}(a/K)$; if $K(a)_\sigma$ is a regular extension of K, then $\mathrm{Cb}(a/K)$ is contained in the difference field generated over K by finitely many independent realisations of $\mathrm{tp}(a/K)$ (see the proof of Lemma 2.13(4) in [5]). $\overline{\mathrm{Cb}}(a/K)$ denotes $\mathrm{Cb}(a/K)^{\mathrm{alg}}$. Note that a (finitary) type does not fork over some finite set.

2.7. ***The generic type.*** The *generic* 1-type is the type of a transformally transcendental element. It is axiomatised by its quantifier-free part, is definable and stationary.[1] Similarly, if V is a variety defined over the algebraically closed difference field K, then the generic type of V (which is characterised by having a realisation a with $\Delta(K(a)_\sigma/K) = \dim(V)$) is axiomatised by its quantifier-free part, is definable and stationary [5, Corollaries 2.11].

2.8. ***Orthogonality of types.*** Let p and q be (partial) types over A and B, respectively. If $A = B$, we say that p and q are *almost orthogonal* (or *weakly orthogonal*), denoted by $p \perp^a q$, if whenever a realises p and b realises q, then $a \mathop{\smile\!\!\!\!\!\!\mid}_A b$. We say that p and q are *orthogonal*, denoted by $p \perp q$, if whenever C contains $A \cup B$, and a realises p, b realises q, and $a \mathop{\smile\!\!\!\!\!\!\mid}_A C$, $b \mathop{\smile\!\!\!\!\!\!\mid}_B C$, then $a \mathop{\smile\!\!\!\!\!\!\mid}_C b$.

2.9. ***The dichotomy in characteristic 0.*** Recall that a partial type π over a set A is called *one-based*[2] if whenever $a_1, \dots, a_n$ realise π and $B \supset A$, then $(a_1 \dots a_n) \mathop{\smile\!\!\!\!\!\!\mid}_C B$, where $C = \operatorname{acl}(Aa_1, \dots, a_n) \cap \operatorname{acl}(B)$.[3]

Types of finite SU-rank are analysable in terms of types of SU-rank 1. The main result of [5] says that in characteristic 0, a type q of SU-rank 1 is either one-based, or nonorthogonal to the fixed field. Moreover, if q is one-based, then it is stable stably embedded and definable. See Theorem 4.10 in [5].

2.10. ***Stable embeddability of the fixed field.*** Recall that a subset S of $\mathcal{U}^n$, which is definable or ∞-definable, is *stably embedded* if whenever $D \subset \mathcal{U}^{nm}$ is definable with parameters from $\mathcal{U}$, then $D \cap S^m$ is definable with parameters from S. An important result of [5] (Proposition 1.11) says that the fixed field $F := \operatorname{Fix}(\sigma)$ of $\mathcal{U}$ is stably embedded: if $D \subset F^n$ is definable in the difference field $\mathcal{U}$ (with parameters from $\mathcal{U}$), then it is definable in the pure field language in F (with parameters from F). In fact, one has more: let $C = \operatorname{acl}(C) \subset \mathcal{U}$, and b a tuple in F. Then $\operatorname{tp}_F(b/C \cap F) \vdash \operatorname{tp}_{\mathcal{U}}(b/C)$; indeed, all finite σ-stable extensions of CF are contained in CF^{alg} (see Lemma 4.2 in [4]), and therefore any $(C \cap F)$-automorphism of the field F extends to a C-automorphism of the difference field $\operatorname{acl}(CF)$, since it obviously extends to a C-automorphism of CF, and the automorphism σ of CF^{alg} extends uniquely to $\operatorname{acl}(CF)$ up to isomorphism over CF^{alg} by Babbitt's theorem (see, e.g., Lemma 2.8 in [5]).

For more properties of stably embedded sets or types, see the appendix of [5].

2.11. ***More on stable stably embedded types.*** For a definition of a (partial) type being *stable stably embedded*, see Lemma 2 of the appendix of [5]. Here we use

[1] A type p over a set A is stationary if whenever $B \supset A$, then p has a unique nonforking extension to B.

[2] In [5], they are called *modular*.

[3] Here we are using the fact that any completion of ACFA eliminates imaginaries.

the following consequence: let $A = \mathrm{acl}(A)$ be algebraically closed, and suppose that $\mathrm{tp}(a/A)$ is stable stably embedded. Then $\mathrm{tp}(a/A)$ is definable (over A; see Lemma 1 in the Appendix of [5]). Also, if $B = \overline{\mathrm{Cb}}(a/A)$ and $\mathrm{tp}(a/B) \perp^a \mathrm{tp}(A/B)$, then $\mathrm{tp}(a/B) \vdash \mathrm{tp}(a/A)$; this is because $\mathrm{tp}(a/B)$ has a unique nonforking extension to any superset of the algebraically closed set B.

Definition 2.12 (internality to the fixed field). Let π be a partial type over $A \subset \mathcal{U}$, and $F = \mathrm{Fix}(\sigma)(\mathcal{U})$.

(1) π is *qf-internal to* $\mathrm{Fix}(\sigma)$ if there is some finitely generated over A difference field C such that whenever a realises π, there is a tuple b in F such that $a \in C(b)$. I.e., $a \in CF$.

(2) π is *almost internal to* $\mathrm{Fix}(\sigma)$ if there is some finitely generated over A difference field C such that whenever a realises π, there is a tuple b in F such that $a \in \mathrm{acl}(Cb)$.

Remarks 2.13. Clearly qf-internality implies almost internality. Moreover, to show qf-internality or almost internality of a (complete) type p, it is enough to do it for a particular realisation a of the type p, i.e., to find C independent from a over A such that $a \in CF$ or $a \in \mathrm{acl}(CF)$. See Lemma 5.2 in [5].

Internality or almost internality (to $\mathrm{Fix}(\sigma)$) of a type is in fact a property of its quantifier-free part.

Recall that a difference field E is linearly disjoint from F over $F \cap E$. It follows that in (1) above, the tuple b can be taken so that $C(b) = C(a)_\sigma$: take a generating tuple d of the (pure) field extension $F \cap C(a)_\sigma$ of $F \cap C$; as F is linearly disjoint from $C(a)_\sigma$ over $F \cap C(a)_\sigma$, we get that CF is linearly disjoint from $C(a)_\sigma$ over $C(d)$, i.e., that $C(a)_\sigma = C(d)$ since $a \in CF$.

Lemma 2.14. *Let* $A = \mathrm{acl}(A)$, *and assume that* $\mathrm{tp}(a/A)$ *is almost internal to* $\mathrm{Fix}(\sigma)$. *Then there is* $a' \in A(a)_\sigma$ *such that* $\mathrm{tp}(a'/A)$ *is qf-internal to* $\mathrm{Fix}(\sigma)$, $\sigma(a') \in A(a')$, *and* $a \in \mathrm{acl}(Aa')$.

Proof. By assumption there is some tuple c independent from a over A and such that $a \in \mathrm{acl}(AFc)$. Taking b in F such that $A(c,a)_\sigma \cap F = (F \cap A)(b)$, we obtain that F is linearly disjoint from $A(c,a)_\sigma$ over $(F \cap A)(b)$, and therefore that $AF(c,b)_\sigma$ and $A(c,a)_\sigma$ are linearly disjoint over $A(c,b)_\sigma$, so that $a \in \mathrm{acl}(Acb)$ (since $a \in \mathrm{acl}(AFcb)$). As c is independent from a over $A = \mathrm{acl}(A)$, it follows that $A(c,a)_\sigma = A(c,a,b)_\sigma$ is a regular extension of $A(a)_\sigma$, and therefore that $\mathrm{Cb}(b, c/A(a)_\sigma)$ is contained in the difference field generated by finitely many independent realisations of $\mathrm{tp}(b, c/A(a)_\sigma)$ (see 2.6). Again, as c is independent from a over A and b is in F, it follows that if a' is such that $\mathrm{Cb}(c, b/A(a)_\sigma) = A(a')_\sigma$, then $\mathrm{tp}(a'/A)$ is qf-internal to $\mathrm{Fix}(\sigma)$. As $b \in A(a', c)_\sigma$ and c is independent from a over A, it follows that $a \in \mathrm{acl}(Aa')$ as desired. As $A(c, a')_\sigma = A(c, b)_\sigma$

and $b \in F$, it follows that $A(c, a')_\sigma$ is finitely generated as a field extension of $A(c)_\sigma$. But as a' and c are independent over A, the same holds of the field extension $A(a')_\sigma/A$, i.e., for some n, $\sigma^n(a') \in A(a', \sigma(a'), \dots, \sigma^{n-1}(a'))$. We then replace a' by $(a', \sigma(a'), \dots, \sigma^{n-1}(a'))$. □

2.15. ***The semiminimal analysis.*** Let a be a tuple which is transformally algebraic over K. Thus $\mathrm{SU}(a/K) < \omega$. As $\mathrm{Th}(\mathcal{U})$ is supersimple, there is a sequence $a_1, \dots, a_n \in \mathrm{acl}(Ka)$ such that $a \in \mathrm{acl}(Ka_1, \dots, a_n)$, and for every $0 < i \leq n$, $\mathrm{tp}(a_i/\mathrm{acl}(Ka_1, \dots, a_{i-1}))$ is either one-based of rank 1, or almost internal to a non-one-based type of rank 1. This is a classical result in supersimple theories; for a proof in our case in characteristic 0, see Theorem 5.5 in [5]. Note that in characteristic 0, by the dichotomy of 2.9, all non-one-based types of rank 1 are nonorthogonal to $\sigma(x) = x$, and by Lemma 2.14, almost internality to $\mathrm{Fix}(\sigma)$ may be replaced by qf-internality to $\mathrm{Fix}(\sigma)$.

Definition 2.16. Let T be a completion of ACFA, M a model of T.

(1) We say that M is $\aleph_\varepsilon$*-saturated* if whenever $A \subseteq M$ is finite, then every strong 1-type over A is realised in M. Equivalently, as our theory eliminates imaginaries, if every 1-type over $\mathrm{acl}(A)$ is realised in M.

(2) Let κ be an infinite cardinal or $\aleph_\varepsilon$, and $A \subseteq M$. We say that M is κ*-prime over* A if M is κ-saturated, and A-embeds elementarily into every κ-saturated model of $\mathrm{Th}(M, a)_{a \in A}$. When $\kappa = \aleph_\varepsilon$, one also says that M is *a-prime over* A.

(3) Let κ be an infinite cardinal or $\aleph_\varepsilon$. We say that $A \subseteq M$ is *small* if $A = \mathrm{acl}(A_0)$, where A_0 is finite if we are dealing with $\aleph_\varepsilon$-saturation, and has cardinality $< \kappa$ if we are dealing with κ-saturation. We also say that $A \subseteq M$ is *very small* if $A = \mathrm{acl}(A_0)$, where A_0 is finite. Note that a (very) small set is in particular algebraically closed.

(4) Let κ be an infinite cardinal or $\aleph_\varepsilon$, and $A \subseteq M$. A type p over A is κ*-isolated* if it is implied by its restriction to some small subset of $\mathrm{acl}(A)$.

(5) We say that M is κ*-atomic over* $A \subseteq M$ if whenever a is a (finite) tuple in M, then $\mathrm{tp}(a/A)$ is κ-isolated. Recall also that M is *atomic over* A if every finite tuple realises an isolated type over A.

(6) We say that $B = \mathrm{acl}(B) \subseteq M$ is κ*-constructed over* $A \subseteq M$ if there is a sequence $(d_\alpha)_{\alpha<\mu}$ in $B \setminus A$ such that for every $\alpha < \mu$, $\mathrm{tp}(d_\alpha/\mathrm{acl}(Ad_\beta \mid \beta < \alpha))$ is κ-isolated and $B = \mathrm{acl}(Ad_\alpha \mid \alpha < \mu)$.

Remarks 2.17. (1) If κ is a regular cardinal, then κ-atomicity is transitive: if $A \subseteq B \subseteq C \subseteq M$, with B κ-atomic over A and C κ-atomic over B, then C is κ-atomic over A. This is however not necessarily true when κ is singular. However, this holds if $B = \mathrm{acl}(Ab)$ for some finite tuple b (since every finite tuple in B

realises an isolated type over Ab), or if C is atomic over B. (There are stronger statements involving cardinals $\lambda < \mathrm{cf}(\kappa)$.)

(2) If M is a κ-saturated model of T containing A and M is κ-constructed over A, then M is κ-prime over A.

(3) The property of being κ-constructed is preserved under towers and unions of chains indexed by ordinals.

2.18. ***Algebraic translation of the model-theoretic notions.*** Let us translate what the notions of saturation mean in our case. We will be dealing with either uncountable cardinals or $\aleph_\varepsilon$. Recall from 2.4 that $\mathrm{tp}(a/A)$ is entirely determined by the isomorphism type over the difference field generated by A of the difference field $\mathrm{acl}(Aa)$. So, for κ an uncountable cardinal, the κ-saturation of a model M of ACFA simply means that every system of $< \kappa$ difference equations with coefficients in M which has a solution in a difference field extending M already has a solution in M. This is what was called κ-closed in the introduction.

The notion of κ-prime over a difference subfield corresponds to being a κ-closure of that difference field.

In the case of $\aleph_\varepsilon$-saturation, the algebraic description is a little more complicated, and is better expressed in terms of embedding problems: Work inside a large model $\mathcal{U}$, and consider a submodel M of $\mathcal{U}$. Then M is $\aleph_\varepsilon$-saturated if whenever a is a finite tuple of elements of M and b an element of $\mathcal{U}$, there is an $\mathrm{acl}(a)$-embedding of $\mathrm{acl}(a, b)$ inside M.

A similar description holds for κ-saturated, with the base set a of cardinality $< \kappa$: a model M of ACFA is κ saturated if whenever $A \subset M$ is small and b is a finite tuple in some difference field $\mathcal{U}$ containing M, then there is an A-embedding of $\mathrm{acl}(Ab)$ into M. Note that $|A|$-many difference equations are necessary to describe the isomorphism type of $\mathrm{acl}(Ab)$ over A.

3. The results

Results of Hrushovski [10] show that if F is a pseudofinite field and $C \subset F$, then $\mathrm{Th}(F, c)_{c\in C}$ eliminates imaginaries if and only if the absolute Galois group of the relative algebraic closure inside F of the field generated by C is isomorphic to $\hat{\mathbb{Z}}$. It may therefore happen that $\mathrm{Th}(F)$ eliminates imaginaries in the ring language, but it may also happen that extra elements are needed, for instance if F contains $\mathbb{Q}^{\mathrm{alg}}$. The following lemma will therefore be useful when dealing with $\aleph_\varepsilon$-saturation.

Lemma 3.1. *Let F be an $\aleph_\varepsilon$-saturated pseudofinite field and a a finite tuple in F. Then there is a finitely generated subfield A of F containing a and such that*

$$G(A^{\mathrm{alg}} \cap F) \simeq \hat{\mathbb{Z}}.$$

Proof. Let k be the relative algebraic closure inside F of the subfield generated by a, and consider $k(t)$, where t is transcendental over k. Let Q_0 be the set consisting of all integers n which are either prime numbers or 4 and such that $G(k)$ does not have a quotient isomorphic to $\mathbb{Z}/n\mathbb{Z}$. If $\mathrm{char}(k) \neq 0$, we let $Q = Q_0 \setminus \{4\}$, and if $\mathrm{char}(k) = 0$, we let $Q = Q_0 \setminus \{2\}$. If Q is empty, then $G(k) \simeq \hat{\mathbb{Z}}$, and we are done. So, we assume that Q is nonempty.

By Proposition 16.3.5 of [9], for each n, $k(t)$ has a Galois extension L_n which is regular over k and with $\mathcal{G}al(L_n/k(t)) = \mathbb{Z}/n\mathbb{Z}$. Let L be the field composite of all L_n, $n \in Q$. Then $\mathcal{G}al(L/k(t)) \simeq \prod_{n\in Q} \mathbb{Z}/n\mathbb{Z}$. Observe that $L \cap k^{\mathrm{alg}} = k$, because all the L_n are regular extensions of k and Galois over $k(t)$ of relatively prime order.

Take a topological generator σ_0 of $\mathcal{G}al(L/k(t))$, and a topological generator σ_1 of $G(k)$. Let $\sigma \in G(k(t))$ extend $(\sigma_0, \sigma_1) \in \mathcal{G}al(Lk^{\mathrm{alg}}/k(t)) \simeq \mathcal{G}al(L/k(t)) \times G(k)$; then the subfield A of $k(t)^{\mathrm{alg}}$ fixed by σ is a regular extension of k, with Galois group isomorphic to $\hat{\mathbb{Z}}$, since its Galois group is procyclic, projects onto $G(k)$, onto all $\mathbb{Z}/p\mathbb{Z}$ with p a prime, and onto $\mathbb{Z}/4\mathbb{Z}$ if $\mathrm{char}(k) = 0$.

By general properties of pseudofinite fields and by $\aleph_\varepsilon$-saturation of F, there is a k-embedding φ of A inside F, in such a way that $\varphi(A)^{\mathrm{alg}} \cap F = \varphi(A)$. This is classical, and follows for instance from Lemma 20.2.2 in [9]. □

Lemma 3.2. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$, and let K be a difference field with* $\mathrm{Fix}(\sigma)(K)$ *pseudofinite and κ-saturated. Then there is a model $\mathcal{U}$ of* ACFA *containing K which is κ-saturated and with* $\mathrm{Fix}(\sigma)(\mathcal{U}) = \mathrm{Fix}(\sigma)(K)$.

Proof. (Compare with Afshordel's result [1].) Let $\mathcal{U}_1$ be a κ-saturated model of ACFA containing K, and let $\mathcal{U} \subseteq \mathcal{U}_1$ be maximal such that

$$F := \mathrm{Fix}(\sigma)(\mathcal{U}) = \mathrm{Fix}(\sigma)(K).$$

We show that $\mathcal{U}$ satisfies our conclusion. First observe that $\mathcal{U}$ is algebraically closed. Let $A = \mathrm{acl}(A) \subset \mathcal{U}$ be small and let $p \in S_1(A)$. Then p is realised in $\mathcal{U}_1$, and we take some $a \in \mathcal{U}_1$ realising p, with $\mathrm{SU}(a/\mathcal{U})$ minimal. Let $B \supset A$ be small such that $a \mathop{\smile\!\!\!\!\!\!\;|}_B \mathcal{U}$, and replace p by $\mathrm{tp}(a/B)$.

If $\mathrm{tp}(a/\mathcal{U}) \perp^a \mathrm{Fix}(\sigma)$, then $\mathcal{U}(a)_\sigma^{\mathrm{alg}}$ has the same fixed field as $\mathcal{U}$: indeed, $\mathcal{U}(a)_\sigma^{\mathrm{alg}}$ and $\mathrm{Fix}(\sigma)(\mathcal{U}_1)$ are linearly disjoint over their intersection, which is contained in $\mathcal{U}$ and therefore in K. So by maximality of $\mathcal{U}$, $a \in \mathcal{U}$.

Assume now that $\mathrm{tp}(a/\mathcal{U}) \not\perp^a \mathrm{Fix}(\sigma)$. Then there is some small $C \subset \mathcal{U}$ containing B, and a realisation a' of $\mathrm{tp}(a/B)$ such that $C(a')_\sigma \cap \mathrm{Fix}(\sigma)(\mathcal{U}_1)$ contains some element b not in $\mathcal{U}$. We may and do assume that $\mathrm{Fix}(\sigma)(C)$ has absolute Galois group isomorphic to $\hat{\mathbb{Z}}$ (by Lemma 3.1). But as F is κ-saturated, $\mathrm{tp}_F(b/C \cap F)$ is realised in F, by some b_1. Then b_1 realises $\mathrm{tp}(b/C)$ (see the first paragraph of 2.10). Thus, by κ-saturation of $\mathcal{U}_1$, there is some $a_1 \in \mathcal{U}_1$ such that $\mathrm{tp}(a_1, b_1/C) = \mathrm{tp}(a', b/C)$.

But then a_1 realises p, and $\mathrm{SU}(a_1/\mathcal{U}) \leq \mathrm{SU}(a'/B) - \mathrm{SU}(b/C) < \mathrm{SU}(a/B)$, which gives us the desired contradiction.

So in both cases, p is realised in $\mathcal{U}$. □

Corollary 3.3. *Let κ be as above, and K an algebraically closed difference field with* $\mathrm{Fix}(\sigma)(K)$ *κ-saturated. If $\mathcal{U}$ is a κ-prime model of* ACFA *over K then* $\mathrm{Fix}(\sigma)(\mathcal{U}) = \mathrm{Fix}(\sigma)(K)$.

Lemma 3.4. *Let $\mathcal{U}$ be an $\aleph_\varepsilon$-saturated model of* ACFA *of characteristic* 0, *and let K be an algebraically closed difference subfield of $\mathcal{U}$ which contains $F := \mathrm{Fix}(\sigma)(\mathcal{U})$. Let $a \in \mathcal{U}$ be such that $p = \mathrm{tp}(a/K)$ is qf-internal to $\mathrm{Fix}(\sigma)$, $p \perp^a \mathrm{Fix}(\sigma)$, and assume that $\sigma(a) \in K(a)$. Then there are a (very) small $A \subseteq K$ and a tuple $b \in \mathcal{U}$ of realisations of p such that*

1. *$FA(b)$ contains all realisations (in $\mathcal{U}$) of $\mathrm{qftp}(a/A)[\ell]$, for any $\ell \geq 1$;*
2. *if $b' \in \mathcal{U}$ realises $\mathrm{qftp}(b/A)[m]$ for some $m \geq 1$, then $FA(b')$ contains all realisations (in $\mathcal{U}$) of $\mathrm{qftp}(a/A)[\ell]$ for $\ell \geq 1$;*
3. *$\mathrm{tp}(a/A) \vdash \mathrm{tp}(a/K)$, and $\mathrm{tp}(b/A) \vdash \mathrm{tp}(b/K)$.*

Proof. Let $k \subset K$ be small such that $a \mathop{\smile\!\!\!\!\!\!\mid}_k K$ and $\mathcal{G}al(\mathrm{Fix}(\sigma)(k)^{\mathrm{alg}}/\mathrm{Fix}(\sigma)(k))$ is isomorphic to $\hat{\mathbb{Z}}$. Then $\sigma(a) \in k(a)$ and kF contains $\mathrm{Fix}(\sigma^\ell)(\mathcal{U})$ for all $\ell \geq 1$. By assumption, there is some small B (in $\mathcal{U}$, by $\aleph_\varepsilon$-saturation of $\mathcal{U}$) independent from a over k such that $a \in BF$. Hence, there is a tuple c in $B(a)_\sigma \cap F = B(a) \cap F$ such that $B(a) = B(c)$ (by Remarks 2.13). Let $D = \mathrm{Cb}(a, c/B)$. Then $D(c) = D(a)$, and $D \subset k(c_1, a_1, \ldots, c_n, a_n)$ for some independent realisations (c_i, a_i) of $\mathrm{qftp}(c, a/B)$ (in some elementary extension of $\mathcal{U}$). By $\aleph_\varepsilon$-saturation of $\mathcal{U}$, we may assume that $(c_1, a_1, \ldots, c_n, a_n)$ is in $\mathcal{U}$, and is independent from (c, a) over D. We let $b = (a_1, \ldots, a_n)$, $A = \overline{\mathrm{Cb}}(k, c_1, a_1, \ldots, c_n, a_n/K)$; then $D \subset kF(b)$, and A is small. As A contains $c_1, \ldots, c_n$ $(\in F \subset K)$ and k, we also have $D \subset A(b)$, whence $a \in FA(b)$. Note that $a \mathop{\smile\!\!\!\!\!\!\mid}_k A$ since $A \subset K$.

If $a' \in \mathcal{U}$ realises $\mathrm{qftp}(a/A(b))$, then the difference fields $D(a)$ and $D(a')$ are isomorphic. Hence there is some $c' \in D(a') \cap F$ such that $D(c') = D(a')$, i.e., $a' \in FA(b)$.

Let a' be an arbitrary realisation of $\mathrm{qftp}(a/A)$, and let b' be a realisation of $\mathrm{qftp}(b/A)$, which is independent from (b, a') over A. By the previous paragraph (as b' consists of n realisations of $\mathrm{qftp}(a/A(b))$) we know that $b' \in FA(b)$. The difference fields $A(b)$ and $A(b')$ are A-isomorphic, and this isomorphism extends to an isomorphism of difference fields $A(b, a) \to A(b', a')$. Hence, $a' \in FA(b') \subseteq FA(b)$, as desired. If a' realises $\mathrm{qftp}(a/A)[\ell]$ and is independent from D over k, then the σ^ℓ-difference fields $D(a')$ and $D(a)$ are isomorphic over D. Let $f(x)$ be the tuple of rational functions over D such that $f(a) = c$; then $\sigma^\ell(f(a')) = f(a')$ and

$D(a') = D(f(a'))$. Hence a' belongs to $FA(b)$. An argument similar to the one given in the first case shows it for arbitrary realisation of $\mathrm{qftp}(a/A)[\ell]$ and shows (1).

Note that we have in fact shown that $FA(b') = FA(b)$, and so the conclusion of (1) also holds for b'. An easy argument allows to remove the assumption that b' is independent from b over A: let b'' realise $\mathrm{qftp}(b/A)$, independent from (b, b') over A; then by the proof of the first part: $FA(b'') = FA(b)$ and $FA(b') = FA(b'')$.

Working in $\mathcal{U}[\ell]$, and noting that if $m \mid \ell$ then the realisations of $\mathrm{qftp}(a/A)[m]$ also realise $\mathrm{qftp}(a/A)[\ell]$, part (1) gives (2).

For the proof of (3), we first show that every realisation b' of $\mathrm{qftp}(b/A)[\ell]$ (in $\mathcal{U}$) is independent from K over A. Indeed, by (2), we know that $FA(b) = FA(b')$, and therefore $FK(b) = FK(b') = K(b) = K(b')$ (as $A, F \subseteq K$). This implies that $\mathrm{tr.deg}(b/K) = \mathrm{tr.deg}(b'/K)$, and therefore that $b' \mathop{\smile\!\!\!\!\!\!\mid}_A K$. As $\mathcal{U}$ is $\aleph_\varepsilon$-saturated and A is small, this shows that if $d \in K$, then

$$\mathrm{qftp}(b/A)[\ell] \perp^a \mathrm{qftp}(d/A)[\ell].$$

By Proposition 4.9 of [5], if $\mathrm{tp}(b/A) \not\vdash \mathrm{tp}(b/K)$, then there would be some tuple $d \in K$ and integer $\ell \geq 1$ such that $\mathrm{qftp}(d/A)[\ell] \not\perp^a \mathrm{tp}(b/A)[\ell]$. But as we just saw, this is impossible, and this gives us (3). (This is where the characteristic 0 assumption is crucial.) □

Remark 3.5. In the above notation, note that if $\mathcal{U} \prec \mathcal{U}'$ and $F' = \mathrm{Fix}(\sigma)(\mathcal{U}')$, then $F'A(b)$ contains all realisations of $\mathrm{qftp}(a/A)[\ell]$ in $\mathcal{U}'$, for any $\ell \geq 1$.

Lemma 3.6. *Let $K, A, b, \mathcal{U}$ be as in Lemma 3.4, and let L be a difference subfield of $\mathcal{U}$ containing K. Then there is a small A' containing A such that* $\mathrm{tp}(b/A') \vdash \mathrm{tp}(b/L)$. *In particular*, $\mathrm{tp}(a/A') \vdash \mathrm{tp}(a/L)$.

Proof. Let $A' \subset L$ be small, containing A and such that $b \mathop{\smile\!\!\!\!\!\!\mid}_{A'} L$. Then the proof of (3) works. □

Corollary 3.7. *Let K and $\mathcal{U}$ be as in Lemma 3.4, and p be a type which is almost internal to* $\mathrm{Fix}(\sigma)$. *Then any K-indiscernible sequence (a_i) of realisations of p in $\mathcal{U}$ is finite.*

Proof. Let $(a_i)_{i<\omega}$ be a sequence of realisations of p in $\mathcal{U}$ which is K-indiscernible. Then either $a_0 \in K$, or $\mathrm{tp}(a_0/K)$ is almost orthogonal to $\mathrm{Fix}(\sigma)$ (since K contains $F := \mathrm{Fix}(\sigma)(\mathcal{U})$). By Lemma 2.14 there is $a_0' \in K(a_0)_\sigma$ such that $\sigma(a_0') \in K(a_0')$, $a_0 \in K(a_0')^{\mathrm{alg}}$ and $\mathrm{tp}(a_0'/K)$ is qf-internal to $\mathrm{Fix}(\sigma)$. It suffices to show the result for $p = \mathrm{tp}(a_0'/K)$. Let b be the finite tuple of realisations of $\mathrm{tp}(a_0'/K)$ given by Lemma 3.4. If $n > d = \mathrm{tr.deg}(K(b)/K)$ and $\mathrm{tp}(a_i', a_i/K) = \mathrm{tp}(a_0', a_0/K)$, then we know that $a_n' \in K(a_0', \ldots, a_{d-1}')^{\mathrm{alg}}$ (because $K \supset F$). Hence the sequence is finite. □

Definition 3.8. We call a type p over a set A *acceptable* (in $K \supset A$) if A is the algebraic closure of a finite tuple, and either $\mathrm{SU}(p) = 1$ and p is one-based, or p is qf-internal to $\mathrm{Fix}(\sigma)$, almost orthogonal to $\mathrm{Fix}(\sigma)$, and if b realises p then $\sigma(b) \in A(b)$, $\mathrm{tp}(b/A) \vdash \mathrm{tp}(b/K)$, and the set of realisations of $\mathrm{qftp}(b/A)[\ell]$ for $\ell \geq 1$, in some model $\mathcal{U}$ of ACFA containing K, is contained in $A(b)\,\mathrm{Fix}(\sigma)(\mathcal{U})$.

Notation 3.9. Let p be a one-based type of SU-rank 1 over the very small set A. If $A \subset B \subset C$, we denote by $p|B$ the unique nonforking extension of p to B, and by $\dim_B p(C)$ the cardinality of a maximal B-independent subset of realisations of $p|B$ in C.

Lemma 3.10. *Let p be an acceptable one-based type over the very small A, and let K be an algebraically closed difference field containing A. We work in a sufficiently saturated model $\mathcal{U}$ of* ACFA. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$.*

(1) *If K contains κ many A-independent realisations of p, then the nonforking extension of p to K is not κ-isolated, and conversely.*

(2) *Assume that* $\dim_A p(K) < \kappa$. *One of the following holds*:

  (a) *There is some $n < \omega$ and realisations $a_0, \dots, a_{n-1}$ of $p|K$ such that* $\dim_A p(\mathrm{acl}(Ka_0, \dots, a_{n-1})) \geq \kappa > \dim_A p(K)$. *Furthermore, if n is minimal with this property, then* $\mathrm{tp}(a_0, \dots, a_{n-1}/K)$ *is κ-isolated (but* $p|\,\mathrm{acl}(Ka_0, \dots, a_{n-1})$ *is not).*

  (b) *If B is a set of K-independent realisations of $p|K$ of size $\lambda < \kappa$, then* $\dim_A\ p(\mathrm{acl}(KB)) < \kappa$.

Proof. (1) If $C = \mathrm{acl}(C) \subset K$ is small, then C contains $< \kappa$ A-independent realisations of p, so that the nonforking extension of p to C is realised in K, and $p|K$ is not κ-isolated. The converse is clear: the nonforking extension of p to K is implied by its restriction to $\mathrm{acl}(A, p(K))$.

(2) Case (a) is clear by (1) and because dim is additive. So, assume that there is no such n, and let B be as in (b), and $(a_i)_{i<\lambda} \subset B$ a maximal sequence of independent over K realisations of p, and assume that $\lambda < \dim_A p(\mathrm{acl}(KB)) = \mu \geq \kappa$. So $\mathrm{acl}(Ka_i \mid i < \lambda)$ contains a set C consisting of μ many A-independent realisations of p. Then for each $c \in C$, there is some finite $I_c \subset \lambda$ such that $c \in \mathrm{acl}(Ka_i \mid i \in I_c)$. As $\lambda < \mu$, some set I_c appears μ times. Thus $\dim_A p(\mathrm{acl}(Ka_i \mid i \in I_c)) = \mu \geq \kappa$, which contradicts our assumption. □

Remark 3.11. Let p be the generic 1-type over K, and κ an infinite cardinal. Then p is κ-isolated if and only if $\Delta(K) < \kappa$. This follows easily from the description and properties of the generic types (see 2.7).

Definition 3.12. Let $K = \mathrm{acl}(K) \subset L = \mathrm{acl}(L) \subset \mathcal{U}$. We say that L is *normal over* K (in $\mathcal{U}$) if whenever a is a tuple in L, then L contains all realisations of $\mathrm{tp}(a/K)$ in $\mathcal{U}$.

Lemma 3.13. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$, let $K \subseteq L$ be algebraically closed difference subfields of $\mathcal{U}$, where $\mathcal{U}$ is κ-saturated, and suppose* $\mathrm{Fix}(\sigma)(\mathcal{U}) \subset K$. *Assume that $\mathcal{U}$ is κ-atomic over K.*

(1) *Let a be a finite tuple in $\mathcal{U}$. Then $\mathcal{U}$ is κ-atomic over* $\mathrm{acl}(Ka)$.

(2) *Let $B \subset \mathcal{U}$ be transformally independent over K, and assume that either $|B| < \kappa$, or that B is a transformal transcendence basis of $\mathcal{U}$ over K. Then $\mathcal{U}$ is κ-atomic over* $\mathrm{acl}(KB)$.

(3) *If L is normal over K then $\mathcal{U}$ is κ-atomic over L.*

Proof. (1) Clearly $\mathcal{U}$ is κ-atomic over Ka, but we want something stronger. Let $b \in \mathcal{U}$ be a finite tuple, and let C be a small subset of K such that $\mathrm{tp}(a, b/C) \vdash \mathrm{tp}(a, b/K)$. Note that if b' realises $\mathrm{tp}(b/Ca)$ then $b' \mathop{\smile\!\!\!\!\!\!\mid}_{Ca} K$, since $(a, b') \mathop{\smile\!\!\!\!\!\!\mid}_C K$ by κ-isolation of $\mathrm{tp}(a, b/K)$. Let us first show the result when $\mathrm{SU}(b/Ca) < \omega$. If $\mathrm{SU}(b/Ca) = 0$, then $b \in \mathrm{acl}(Ca)$ and the result is obvious. The proof is by induction on $\mathrm{SU}(b/Ca)$; using the semiminimal analysis of $\mathrm{tp}(b/\mathrm{acl}(Ca))$ and induction, we may assume that $\mathrm{tp}(b/\mathrm{acl}(Ca))$ is either 1-based of SU-rank 1, or almost internal to $\mathrm{Fix}(\sigma)$. If $\mathrm{tp}(b/\mathrm{acl}(Ca))$ is one-based, then it is also stable, hence has a unique nonforking extension to any superset of $\mathrm{acl}(Ca)$, in particular to $\mathrm{acl}(Ka)$, and by the remark in the previous paragraph, we get the result: $\mathrm{tp}(b/\mathrm{acl}(Ca)) \vdash \mathrm{tp}(b/\mathrm{acl}(Ka))$.

Assume now that $\mathrm{tp}(b/\mathrm{acl}(Ca))$ is almost internal to $\mathrm{Fix}(\sigma)$, and let $b' \in \mathrm{acl}(Cab)$ be such that $b \in \mathrm{acl}(Cab')$, $\sigma(b') \in \mathrm{acl}(Ca)(b')$, and $\mathrm{tp}(b'/\mathrm{acl}(Ca))$ is qf-internal to $\mathrm{Fix}(\sigma)$ (see Lemma 2.14). By Lemma 3.4, there is a finite tuple $e \in \mathrm{acl}(Ka)$ such that $\mathrm{tp}(b'/\mathrm{acl}(e)) \vdash \mathrm{tp}(b'/\mathrm{acl}(Ka))$. Then $\mathrm{tp}(b'/\mathrm{acl}(Cae)) \vdash \mathrm{tp}(b'/\mathrm{acl}(Ka))$, and because $b \in \mathrm{acl}(Cab')$, we get the desired conclusion.

For the general case, because b is a finite tuple, there is a finite tuple $d \in \mathrm{acl}(Cab)$ such that $\mathrm{SU}(d/Ca) < \omega$, and $\mathrm{tp}(b/\mathrm{acl}(Cad))$ is orthogonal to all types of finite SU-rank. (Indeed, this follows from supersimplicity: if $\mathrm{tp}(b/\mathrm{acl}(Ca))$ is nonorthogonal to some type q of finite SU-rank, then there is $b_1 \in \mathrm{acl}(Cab)$ with $0 < \mathrm{SU}(b_1/\mathrm{acl}(Ca)) < \omega$; repeat the procedure with $\mathrm{tp}(b/\mathrm{acl}(Cab_1))$ until it stops.) By the first case, we know that there is a small $C' \subset \mathrm{acl}(Ka)$ containing C such that $\mathrm{tp}(d/\mathrm{acl}(C'a)) \vdash \mathrm{tp}(d/\mathrm{acl}(Ka))$, and that $\mathrm{acl}(Kad)$ is κ-atomic over $\mathrm{acl}(Ka)$. By Remarks 2.17(1), it suffices to show that $\mathrm{tp}(b/\mathrm{acl}(Kad))$ is κ-isolated. By [6, Theorem 5.3] (see also [6, Appendix B]), $\mathrm{tp}(b/\mathrm{acl}(Cad))$ is stationary. But by the first paragraph of the proof, we know that every realisation of $\mathrm{tp}(b/\mathrm{acl}(Cad))$ is independent from K over $\mathrm{acl}(Cad)$, and this gives the result.

(2) If $B = \varnothing$ there is nothing to prove, so suppose it is not. Then $\Delta(K) < \kappa$ by Remark 3.11. Let a be a finite tuple in $\mathcal{U}$, and let $b \subset B$ be a finite tuple such that $a \mathop{\smile\!\!\!\!\!\!\mid}_{Kb} B$. Let $c \subset a$ be a transformal transcendence basis of $K(a, b)_\sigma$ over $K(b)_\sigma$ (and therefore also over $K(B)_\sigma$). If $c \neq \varnothing$, then $|B| < \kappa$,

$\Delta(K(B)) < \kappa$, and therefore $\mathrm{tp}(c/\operatorname{acl}(KB))$ is κ-isolated. Moreover, as a is transformally algebraic over $K(b,c)_\sigma$, and $B\setminus\{b\}$ is purely transformally transcendental over $K(b,c)_\sigma$, $\mathrm{tp}(a/\operatorname{acl}(Kbc))$ and $\mathrm{tp}(B/\operatorname{acl}(Kbc))$ are orthogonal, and by stationarity of $\mathrm{tp}(B/\operatorname{acl}(Kbc))$, we get that $\mathrm{tp}(B/\operatorname{acl}(Kbc)) \vdash \mathrm{tp}(B/\operatorname{acl}(Kba))$. By symmetry,

$$\mathrm{tp}(a/\operatorname{acl}(Kbc)) \vdash \mathrm{tp}(a/\operatorname{acl}(KBc)).$$

But $\mathrm{tp}(a,b,c/K)$ is κ-isolated, hence so is $\mathrm{tp}(a/\operatorname{acl}(Kbc))$ by (1), and this gives the result.

(3) Let a be a finite tuple in $\mathcal{U}$, and consider $\mathrm{tp}(a/L)$. Let $d \subset a$ be maximal transformally independent over L. If $d \neq \varnothing$, then d is transformally independent over K, which implies that $\Delta(L/K) = 0$ (by normality of L/K), and that $\Delta(K) = \Delta(L) < \kappa$ (by κ-isolation of $\mathrm{tp}(d/K)$). Therefore $\mathrm{tp}(d/L)$ is κ-isolated.

If $\Delta(L/K) \neq 0$, note that by normality of L over K in $\mathcal{U}$, every element of the tuple a which is not in L is transformally algebraic over K. So, replacing a by $a\setminus L$, we may assume they are all transformally algebraic over K, i.e., that $\mathrm{SU}(a/K) < \omega$. We then let $d = \varnothing$.

In both cases, by (2), $\mathcal{U}$ is κ-atomic over $\operatorname{acl}(Kd)$, and the normality of L over K implies the normality of $\operatorname{acl}(Ld)$ over $\operatorname{acl}(Kd)$. Working over $\operatorname{acl}(Kd)$, we may therefore assume that a and $D := \overline{\mathrm{Cb}}(a/L)$ are transformally algebraic over K.

We use induction on $\mathrm{SU}(a/L)$, and using the semiminimal analysis, we find $b \in \operatorname{acl}(Da)$ such that $\mathrm{tp}(a/\operatorname{acl}(Db))$ is either one-based of SU-rank 1, or almost internal to $\mathrm{Fix}(\sigma)$.

If $\mathrm{tp}(a/\operatorname{acl}(Db))$ is almost internal to $\mathrm{Fix}(\sigma)$, then so is $\mathrm{tp}(a/\operatorname{acl}(Lb))$. By Lemma 2.14, there is $a' \in \operatorname{acl}(Lba)$ such that $a \in \operatorname{acl}(Lba')$ and $\mathrm{tp}(a'/\operatorname{acl}(Lb))$ is qf-internal to $\mathrm{Fix}(\sigma)$. By Lemma 3.4, there is a very small $D' \supseteq D$ such that $\mathrm{tp}(a'/\operatorname{acl}(D'b)) \vdash \mathrm{tp}(a'/\operatorname{acl}(Lb))$, and we may choose it so that $a \in \operatorname{acl}(D'ba')$. This shows that $\mathrm{tp}(a/\operatorname{acl}(Lb))$ is κ-isolated, and therefore so is $\mathrm{tp}(a/L)$.

So assume that $p := \mathrm{tp}(a/\operatorname{acl}(Db))$ is one-based of SU-rank 1, and let c be a tuple containing b such that $\operatorname{acl}(Db) = \operatorname{acl}(c) =: C$. We need to show that $\dim_C p(\operatorname{acl}(Lc)) < \kappa$. As $\mathcal{U}$ is κ-atomic over K, we know that $\mathrm{tp}(a,c/K)$ is κ-isolated, and therefore $\dim_C p(\operatorname{acl}(Kc)) < \kappa$. So, if $\dim_C p(\operatorname{acl}(Lc)) \geq \kappa$, then there is some $a' \in \operatorname{acl}(Lc)\setminus \operatorname{acl}(Kc)$ realising p. Recall that by our earlier step, c, a' are transformally algebraic over K, and therefore so is $e = \mathrm{Cb}(Kca'/L)$. Consider now $\operatorname{acl}(Kca') \cap \operatorname{acl}(Ke) =: E \subset L$; by Proposition 3.1 of [2], $\mathrm{tp}(e/E)$ is almost internal to $\mathrm{Fix}(\sigma)$, and therefore orthogonal to all one-based types. As $\mathrm{tp}(a'/Kc)$ is one-based, and $a' \in \operatorname{acl}(Kce) \setminus \operatorname{acl}(Kc)$, it follows that $e \in E$, since almost internality to $\mathrm{Fix}(\sigma)$ and nonorthogonality to a one-based type imply algebraicity. That is, $e \in \operatorname{acl}(Kca') \cap L$, and as $a' \notin \operatorname{acl}(Kc)$, the tuples a' and e are equialgebraic over $\operatorname{acl}(Kc)$. Hence $\operatorname{acl}(Kca)$ contains a realisation of $\mathrm{tp}(e/\operatorname{acl}(Kc))$, because

$\text{tp}(a/\operatorname{acl}(Kc)) = \text{tp}(a'/\operatorname{acl}(Kc))$. But this contradicts the normality of $\operatorname{acl}(Lc)$ over $\operatorname{acl}(Kc)$. So, $\dim_C(p(\operatorname{acl}(Lc)) < \kappa$, and $\text{tp}(a/Lb)$ is κ-isolated. □

Theorem 3.14. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$, and let K be an algebraically closed difference field of characteristic* 0 *such that $F := \text{Fix}(\sigma)(K)$ is pseudofinite and κ-saturated.*

(1) *Then there is a κ-prime model $\mathcal{U}$ over K.*

(2) *Furthermore, $\mathcal{U}$ is κ-atomic over K, and every sequence of K-indiscernibles has length $\leq \kappa$ (i.e., if $\kappa = \aleph_\varepsilon$, $\leq \aleph_0$; by convention, if κ is meant as a cardinal, then $\aleph_\varepsilon$ will mean $\aleph_0$).*

Proof. By Lemma 3.2, there is a κ-saturated model $\mathcal{U}_1$ of ACFA containing K and with fixed field $F = \text{Fix}(\sigma)(K)$. We will construct a submodel $\mathcal{U}$ of $\mathcal{U}_1$ which is κ-prime over K and satisfies (2). This $\mathcal{U}$ will be κ-constructed.

Step 0. Taking care of the transformal transcendence degree.

If the transformal transcendence degree of K is $< \kappa$, then as any κ-saturated model of ACFA has transformal transcendence degree at least κ, we enlarge K as follows: let $B \subset \mathcal{U}_1$ be a set which is transformally independent over K and of cardinality κ; by [5, Corollaries 2.11], this condition completely determines the K-isomorphism type of $K(B)_\sigma^{\text{alg}}$, and therefore any κ-prime model contains a K-isomorphic copy of $K(B)_\sigma^{\text{alg}}$. We let $K_0 = K(B)_\sigma^{\text{alg}}$. We need to show (2). Each finite subset of B realises a κ-isolated type over K, since the transformal transcendence degree of K is $< \kappa$. Moreover, every tuple in K_0 realises an isolated type over $K(B)_\sigma$; hence K_0 is κ-atomic over K. It is also κ-constructed over K.

Let $(a_i)_{i<\lambda} \subset K_0$ be a K-indiscernible sequence and λ a cardinal. If the a_i are transformally independent over K, then we know that $|\lambda| \leq \kappa$. If not, then by indiscernibility, the transformal transcendence degree of $K(a_i \mid i < \lambda)_\sigma$ over K is finite, and we choose a finite subset c of B such that $K(a_i \mid i < \lambda)_\sigma$ is transformally algebraic over $K(c)_\sigma$. As the elements of B are transformally independent over K, this implies that all the a_i are in fact algebraic over $K(c)_\sigma$. Consider now $D := \overline{\text{Cb}}(c/Ka_i \mid i < \lambda)$. For every i, we know that $a_i \in K(c)_\sigma^{\text{alg}}$, and therefore by definition of D, $a_i \in D(c)_\sigma^{\text{alg}}$. But c is finite, D is contained in the algebraic closure of a finite set (by 2.6), and therefore $D(c)_\sigma^{\text{alg}}$ is countable. Hence so is λ. This shows condition (2) for the extension K_0/K.

We build a sequence K_n, $n < \omega$, of algebraically closed difference subfields of $\mathcal{U}_1$ such that

(i) if p is an acceptable type over a very small $A \subset K_n$, then K_{n+1} contains κ-many A-independent realisations of p;

(ii) K_{n+1} is κ-constructed over K_n.

We let $K_0 = K$ if the transformal transcendence degree of K is $\geq \kappa$, and $K(B)_\sigma^{\mathrm{alg}}$ as in step 0 otherwise. We assume K_n constructed and wish to build K_{n+1}. Let p_β, $\beta < \lambda$, be an enumeration of the acceptable types in K_n, with corresponding very small bases A_β.

Step 1. Defining $K_{n+1} = \bigcup_{\beta<\lambda} K'_\beta$.

We build the sequence K'_β by induction on β, and let $K'_0 = K_n$. If β is a limit ordinal, then we let $K'_\beta = \bigcup_{\gamma<\beta} K'_\gamma$, and $K_{n+1} = K'_\lambda$. We build them so that $K'_{\beta+1}$ satisfies the following:

(i′) $K'_{\beta+1}$ contains κ-many A_β-independent realisations of p_β;

(ii′) $K'_{\beta+1}$ is κ-constructed over K'_β.

Assume K'_β constructed. If p_β has κ-many A_β-independent realisations in K'_β, then we let $K'_{\beta+1} = K'_\beta$. Otherwise, we need to distinguish two cases:

Case 1: p_β is one-based.

Let a_i, $i < \kappa$, be a sequence of K'_β-independent realisations of p_β (a priori, in some elementary extension of $\mathcal{U}_1$). By Lemma 3.10, either there is $n < \omega$ such that $\mathrm{acl}(K'_\beta, a_i \mid i < n)$ contains κ-many A_β-independent realisations of p_β; in that case, taking a minimal such n, $\mathrm{tp}(a_0, \dots, a_{n-1}/K'_\beta)$ is κ-isolated and therefore realised in $\mathcal{U}_1$, so that we may assume $a_0, \dots, a_{n-1} \in \mathcal{U}_1$ and we set $K'_{\beta+1} = \mathrm{acl}(K'_\beta, a_i \mid i < n)$. Then (i′) and (ii′) follow.

If there is no such n, then for every $\lambda < \kappa$, $\mathrm{acl}(K'_\beta a_i \mid i < \lambda)$ does not contain κ-many A_β-independent realisations of p; by the same reasoning we may assume the a_i are in $\mathcal{U}_1$ and we define $K'_{\beta+1} = \mathrm{acl}(K a_i \mid i < \kappa)$. Then (i′) and (ii′) again are satisfied.

Case 2: Not case 1.

Let $a_\beta \in \mathcal{U}_1$ realise p_β, $K'_{\beta+1} = K'_\beta(a_\beta)^{\mathrm{alg}}$. By assumption on p_β, we have $\mathrm{tp}(a_\beta/A_\beta) \vdash \mathrm{tp}(a_\beta/K_n)$. By Lemma 3.6, there is a very small subset B of K'_β which contains A_β and is such that $\mathrm{tp}(a_\beta/B) \vdash \mathrm{tp}(a/K'_\beta)$. So, $\mathrm{tp}(a_\beta/K'_\beta)$ is κ-isolated. We let $K'_{\beta+1} = K'_\beta(a_\beta)_\sigma^{\mathrm{alg}}$. We know that $FK'_\beta(a_\beta)_\sigma$ contains all realisations of $\mathrm{tp}(a_\beta/B)$ in $\mathcal{U}_1$. But since $\mathcal{U}_1$ is κ-saturated, it therefore contains κ independent realisations of $\mathrm{tp}(a_\beta/A_\beta)$, which shows (i′).

We now define $\mathcal{U} = \bigcup_{n\in\omega} K_n$.

Step 2. Show that $\mathcal{U}$ is κ-saturated.

Let $C \subset \mathcal{U}$ be small, and p a 1-type over C, realised by a in $\mathcal{U}_1$. If $\mathrm{SU}(p) = \omega$, then a is transformally transcendental over C; as C is small, K_0 contains a realisation of p. So we may assume that $\mathrm{SU}(p) < \omega$, and the proof is by induction on $\mathrm{SU}(p)$: we assume that for any small D, any 1-type q over D of smaller SU-rank than p is realised in $\mathcal{U}$.

If $\mathrm{SU}(p) = 0$ there is nothing to prove, as p is realised in C. If there is some $b \in C(a)_\sigma^{\mathrm{alg}}$ such that $0 < \mathrm{SU}(b/C) < \mathrm{SU}(a/C)$, then we get the result by induction: $\mathrm{tp}(b/C)$ is realised by some $b' \in \mathcal{U}$, and there is $a' \in \mathcal{U}$ such that $\mathrm{tp}(a', b'/C) = \mathrm{tp}(a, b/C)$ since $\mathrm{acl}(Cb')$ is small and $\mathrm{SU}(a/Cb) < \mathrm{SU}(p)$.

Hence we may assume that there is no such b, whence p is either one-based of SU-rank 1 or almost internal to $\mathrm{Fix}(\sigma)$ (by the semiminimal analysis of 2.15). We need to distinguish three cases.

Case 1: p is one-based of SU-rank 1.

Let $A \subset C$ be very small such that p does not fork over A. Let $n < \omega$ be such that $A \subset K_n$; then p, being acceptable, occurs as a p_β, and is therefore realised in K_{n+1}.

Case 2: p is realised in $\mathrm{Fix}(\sigma)$.

If $a \in \mathrm{Fix}(\sigma)$, we saw in 2.10 that $\mathrm{tp}_F(a/C \cap F) \vdash \mathrm{tp}(a/C)$. The saturation hypothesis on F then gives the result: p is realised in F.

Case 3: Assume now that $p \perp^a \mathrm{Fix}(\sigma)$, p almost internal to $\mathrm{Fix}(\sigma)$.

By Lemma 2.14, there is $a_1 \in C(a)_\sigma$ such that $\mathrm{tp}(a_1/C)$ is qf-internal to $\mathrm{Fix}(\sigma)$, $\sigma(a_1) \in C(a_1)$, and $a \in C(a_1)^{\mathrm{alg}}$. We may replace p by $\mathrm{tp}(a_1/C)$, i.e., assume that p is qf-internal to $\mathrm{Fix}(\sigma)$. Let $C_0 \subset C$ be very small such that p does not fork over C_0. By Lemma 3.4 there is a tuple b of realisations of p and a very small D containing C_0, contained in $\mathrm{acl}(CF)$, such that $FD(b)$ contains all realisations of $\mathrm{qftp}(a/D)$, and $\mathrm{tp}(b/D) \vdash \mathrm{tp}(b/\mathrm{acl}(CF))$. Thus, $\mathrm{tp}(b/D)$ is acceptable, and if n is such that $D \subset K_n$, then p in realised in K_{n+1}.

Step 3. $\mathcal{U}$ is κ-prime over K.

This is clear, by Remarks 2.17(2)–(3).

Step 4. $\mathcal{U}$ is κ-atomic over K.

When κ is regular or $\aleph_\varepsilon$, then this follows from $\mathcal{U}$ being κ-constructed over K. The proof in the singular case is a little more delicate, and is done by induction. We already saw that K_0 is κ-atomic over K. Let a be a finite tuple in $\mathcal{U}$, and (in the notation of Step 1) choose n minimal such that $a \in K_{n+1}$, and β minimal such that $a \in K'_{\beta+1}$. If $n = -1$, there is nothing to prove (by Step 0), so assume $n \geq 0$. By definition of $K'_{\beta+1}$, there are a tuple b in K'_β and a tuple c of realisations of p_β such that $a \in \mathrm{acl}(Kbc)$. We may assume that $\mathrm{acl}(Kb)$ contains A_β, and that $c \mathop{\smile\!\!\!\!\!\!\,|}_{Kb} K'_\beta$. By the induction hypothesis, $\mathrm{tp}(b/K)$ is κ-isolated, and it therefore suffices to show that $\mathrm{tp}(c/\mathrm{acl}(Kb))$ is κ-isolated (by Remarks 2.17(1)). If p_β is qf-internal to $\mathrm{Fix}(\sigma)$ then we know by Lemma 3.4 that there is some very small $D \subset \mathrm{acl}(Kb)$ such that $\mathrm{tp}(c/D) \vdash \mathrm{tp}(c/\mathrm{acl}(Kb))$, and we are done.

If p_β is one-based, then we may assume that the elements of the tuple c are independent over K'_β, maybe at the cost of increasing $b \in K'_\beta$. Then, by the construction of $K'_{\beta+1}$ in Step 1, we know that $\mathrm{tp}(c/K'_\beta)$ is κ-isolated, so that if c' is a proper subtuple of c (consisting of realisations of p_β), then $\dim_{A_\beta} p_\beta(\mathrm{acl}(K'_\beta c')) < \kappa$. In particular, $\dim_{A_\beta} p(\mathrm{acl}(Kbc')) < \kappa$, and $\mathrm{tp}(c/\mathrm{acl}(Kb))$ is κ-isolated (by Lemma 3.10).

Remark (notation as in Step 1 and above). The same proof shows that $\mathcal{U}$ is κ-atomic over each K_n, and over each K'_β. Moreover, the fact that $\mathcal{U}$ is κ-atomic over K'_β implies that $p_\beta(\mathcal{U}) \subset K'_{\beta+1}$.

Step 5. If $(b_i)_{i<\lambda} \subset \mathcal{U}$ is K-indiscernible, with λ a cardinal, then $\lambda \leq \kappa$.

By supersimplicity, for some $n < \omega$ the elements b_i, $n < i < \lambda$, are independent over $K(b_0, \dots, b_n)_\sigma$. If $\mathrm{SU}(b_{n+1}/Kb_0, \dots, b_n) \geq \omega$, then the tuple b_{n+1} contains an element which is transformally transcendental over K, and as the transformal transcendence degree of $\mathcal{U}$ over K is $\leq \kappa$, we get $\lambda \leq \kappa$. So we may assume $\mathrm{SU}(b_{n+1}/\mathrm{acl}(Kb_0, \dots, b_n)) < \omega$.

Let $L = \mathrm{acl}(Kb_0, \dots, b_n)$. Then the sequence $(b_i)_{n<i<\lambda}$ is indiscernible over L. Note that the sequence $\mathrm{acl}(Lb_i)$, $n < i < \lambda$, is also indiscernible over L under a suitable enumeration of each $\mathrm{acl}(Lb_i)$. Hence, if $c_{n+1} \in \mathrm{acl}(Lb_{n+1})$, there are $c_i \in \mathrm{acl}(Lb_i)$, $n+1 < i < \lambda$, such that the sequence $(c_i)_{n<i<\lambda}$ is indiscernible over L. Using the semiminimal analysis (2.15) we may therefore assume that either $\mathrm{tp}(c_i/L)$ is one-based of SU-rank 1, or that $\mathrm{tp}(c_i/L)$ is almost internal to $\mathrm{Fix}(\sigma)$. If $\mathrm{tp}(c_i/L)$ is almost internal to $\mathrm{Fix}(\sigma)$, then the result follows by Corollary 3.7. The one-based case is a little more complicated.

Towards a contradiction, assume that $\lambda > \kappa$ and $\mathrm{tp}(c_{n+1}/L)$ is one-based of SU-rank 1, let $C \subset L$ be a very small set such that $\mathrm{tp}(c_{n+1}/L)$ does not fork over C, and set $p = \mathrm{tp}(c_{n+1}/C)$. Then the tuples c_i, $n < i < \lambda$, form a Morley sequence over C and over L. Let N be κ-prime over $M := \mathrm{acl}(L, c_i \mid n < i < \kappa)$. We may assume that $N \prec \mathcal{U}$.

Claim. $\mathcal{U}$ is κ-prime over L.

It suffices to show that $\mathcal{U}$ is κ-constructed over L. To do that it is enough to show that each LK_m is κ-constructed over LK_{m-1}.

If $m = 0$ and $K_0 \neq K$, let B_0 be a finite subset of B (the transformal transcendence basis of $\mathcal{U}$ over K) such that $b := (b_0, \dots, b_n)$ is independent from K_0 over $\mathrm{acl}(KB_0)$. In particular, b is transformally algebraic over $\mathrm{acl}(KB_0)$, and therefore $\mathrm{tp}(B/\mathrm{acl}(KB_0)) \vdash \mathrm{tp}(B/\mathrm{acl}(LB_0))$ (reason as in the proof of Lemma 3.13(1)), and as $\mathrm{tp}(B_0/L)$ is κ-isolated, it follows that K_0 is κ-constructed over L.

Assume now $m > 0$, and that we have shown that LK'_β is κ-constructed over L. If p_β is not one-based, then by Lemma 3.6, $\mathrm{tp}(a_\beta/\mathrm{acl}(LK'_\beta))$ is κ-isolated, and we are done. Assume now that p_β is one-based; by construction there is a set $(a_\alpha)_{\alpha<\mu}$ of K'_β-independent realisations of $p_\beta|K'_\beta$ such that $K'_{\beta+1} = \mathrm{acl}(K'_\beta, a_\alpha \mid \alpha < \mu)$, and either $\mu \in \omega$ or $\mu = \kappa$.

If $\mu \in \omega$, as $\mathcal{U}$ is κ-atomic over K'_β, we get that $\mathrm{tp}(a_0, \dots, a_{\mu-1}, b/K'_\beta)$ is κ-isolated and therefore $LK'_{\beta+1}$ is κ-constructed over LK'_β. If $\mu = \kappa$, then $\dim_{K'_\beta} p_\beta(\mathrm{acl}(K'_\beta, b, a_\gamma \mid \gamma < \alpha)) < \kappa$ for each $\alpha < \kappa$, so that $LK'_{\beta+1}$ is κ-constructed over LK'_β (here we use that $p_\beta(\mathcal{U}) \subset K'_{\beta+1}$ and that b is finite).

Hence, $\mathcal{U}$ being κ-prime over L, there is an L-embedding f of $\mathcal{U}$ into N. So we have $L \subset f(\mathcal{U}) \prec N \prec \mathcal{U}$. As $\lambda > \kappa$ and the c_i are independent over L, there is some $n < j < \lambda$ such that $f(c_j) \notin M$. But $\dim_M(p) \geq \kappa$, and by Lemma 3.10, $p|M$ is not isolated. But N is κ-atomic over M, and $f(c_j)$ realises p and is not in M, which gives us the desired contradiction. This finishes the proof of (2) and of the theorem. □

Proposition 3.15. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$, and let $\mathcal{U}$ and $\mathcal{U}'$ be κ-saturated models of* ACFA *of characteristic* 0*. Assume that $\mathcal{U}$ (resp., $\mathcal{U}'$) contains an algebraically closed difference field K (resp., K'), over which it is κ-atomic and over which every sequence of indiscernibles has length $\leq \kappa$. Assume moreover that $F := \mathrm{Fix}(\sigma)(K) = \mathrm{Fix}(\sigma)(\mathcal{U})$, $\mathrm{Fix}(\sigma)(K') = \mathrm{Fix}(\sigma)(\mathcal{U}')$, and that we have an isomorphism $f : K \to K'$. Let p be an acceptable type over some very small $A \subset K$, and $p' = f(p)$. If $L = \mathrm{acl}(Kp(\mathcal{U}))$ and $L' = \mathrm{acl}(Kp'(\mathcal{U}'))$, then f extends to an isomorphism between L and L'.*

Proof. Note that p' is also acceptable, with very small basis $A' = f(A)$. If p is not one-based, then this is clear by Lemma 3.4: $L = \mathrm{acl}(Kb)$, $L' = \mathrm{acl}(K'b')$ for some tuples b realising p and b' realising p'. We extend $f|A$ to an isomorphism $g_0 : \mathrm{acl}(Ab) \to \mathrm{acl}(A'b')$ which sends b to b'; as $\mathrm{tp}(b/A) \vdash \mathrm{tp}(b/K)$ and $\mathrm{tp}(b'/A') \vdash \mathrm{tp}(b'/K')$, $g_0 \cup f$ extends to an isomorphism $\mathrm{acl}(Kb) \to \mathrm{acl}(K'b')$.

Assume now that p is one-based. Any κ-saturated model of ACFA containing A contains (at least) κ realisations of p which are independent over A; hence so do $\mathcal{U}$ and $\mathcal{U}'$. Let $(a_i)_{i<\lambda} \subset \mathcal{U}$ be a set of realisations of p which is maximal independent over K, with λ a cardinal, and let $(a'_i)_{i<\mu} \subset \mathcal{U}'$ be defined analogously over K'. By Lemma 3.10 and our hypothesis on the length of K-indiscernible sequences, either λ is finite or $\lambda = \kappa$. If $\lambda = n < \omega$, then as $\mathrm{tp}(a'_0, \dots, a'_{n-1}/K') = f(\mathrm{tp}(a_0, \dots, a_{n-1}/K))$, it follows that $\mathrm{acl}(K'a'_0, \dots, a'_{n-1})$ contains κ-many independent realisations of $f(p)$, so that $\mu \leq n$. The symmetric argument gives $\mu = \lambda$. Define g on $K(a_i \mid i < \lambda)_\sigma$ by $g(a_i) = a'_i$, and extend to $L = \mathrm{acl}(Ka_i \mid i < \lambda)$. □

Theorem 3.16. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$, and let $\mathcal{U}$ and $\mathcal{U}'$ be κ-saturated models of* ACFA *of characteristic* 0 *containing an algebraically closed difference field K, with $F := \mathrm{Fix}(\sigma)(K) = \mathrm{Fix}(\sigma)(\mathcal{U}) = \mathrm{Fix}(\sigma)(\mathcal{U}')$. Assume that $\mathcal{U}$ and $\mathcal{U}'$ are κ-atomic over K, and that any sequence of K-indiscernibles in $\mathcal{U}$ or in $\mathcal{U}'$ has length $\leq \kappa$. Then $\mathcal{U} \simeq_K \mathcal{U}'$.*

Proof. We start with the generic type: if the transformal transcendence degree of K is $\geq \kappa$, then $\mathcal{U}$ and $\mathcal{U}'$ are transformally algebraic over K. If not, then let D be a transformal transcendence basis of $\mathcal{U}$ over K and D' a transformal transcendence basis of $\mathcal{U}'$ over K. They have the same cardinality κ, and there is a K-isomorphism $K(D)_\sigma^{\mathrm{alg}} \to K(D')_\sigma^{\mathrm{alg}}$. By Lemma 3.13, $\mathcal{U}$ and $\mathcal{U}'$ still satisfy the hypotheses over $K(D)_\sigma^{\mathrm{alg}}$ and $K(D')_\sigma^{\mathrm{alg}}$. Hence we may assume that both $\mathcal{U}$ and $\mathcal{U}'$ are transformally algebraic over K. We define by induction on n an increasing sequence K_n of algebraically closed subfields of $\mathcal{U}$ such that for each n, if p is an acceptable type over some (very small) $A \subset K_{n-1}$, then K_n contains all realisations of p in $\mathcal{U}$, and furthermore, $K_n = \mathrm{acl}(K_{n-1}P)$ for the set P of all realisations (in $\mathcal{U}$) of acceptable types over some subset of K_{n-1}. Then each K_n is normal over K_{n-1} (and in fact over K), and so by Lemma 3.13, $\mathcal{U}$ satisfies the hypotheses over K_n. Note also that $\mathcal{U} = \bigcup_{n<\omega} K_n$. We let $L_n \subset \mathcal{U}'$ be defined analogously. It then suffices to build a sequence g_n of K-isomorphisms $K_n \to L_n$.

Assume g_{n-1} already built. Let p_β, $\beta < \lambda$, be an enumeration of all acceptable types over a subset of K_{n-1}, with associated small basis A_β. Note that $f(p_\beta)$, $\beta < \lambda$, enumerates all acceptable types over subsets of L_{n-1}, since if q is an acceptable type over the very small $C \subset L_{n-1}$, so is $g_{n-1}^{-1}(q)$ (over $g_{n-1}^{-1}(C) \subset K_{n-1}$). We build by induction on $\beta < \lambda$ an increasing sequence K'_β of algebraically closed difference subfields of $\mathcal{U}$ such that K'_β contains all realisations in $\mathcal{U}$ of p_γ for all $\gamma < \beta$. Assume we have extended g_{n-1} to an isomorphism $f_\beta : K'_\beta \to L'_\beta$, where L'_β contains all realisations in $\mathcal{U}'$ of $g_{n-1}(p_\gamma)$ for all $\gamma < \beta$. As $\mathcal{U}$ is κ-atomic over K_{n-1}, it is also κ-atomic over K'_β (by Lemma 3.13), and similarly, $\mathcal{U}'$ is κ-atomic over $L'_\beta = f_\beta(K'_\beta)$. Extending f_β to an isomorphism $f_{\beta+1} : K'_{\beta+1} \to L'_{\beta+1}$ is given by Proposition 3.15.

As remarked before, if q is an acceptable type over some $A' \subset L'_{n-1}$, then $g_{n-1}^{-1}(q) = p_\beta$ for some $\beta < \lambda$, and so L'_n contains $q(\mathcal{U}')$, and K'_n contains $g_{n-1}^{-1}(q)(\mathcal{U})$. This finishes the induction step. Then $g = \bigcup_{n<\omega} g_n$ is a K-isomorphism between $\mathcal{U}$ and $\mathcal{U}'$. □

Theorem 3.17. *Let κ be an uncountable cardinal or $\aleph_\varepsilon$ and let K be an algebraically closed difference field of characteristic* 0, *with* $\mathrm{Fix}(\sigma)(K)$ *pseudofinite and κ-saturated. Then* ACFA *has a κ-prime model over K, and it is unique up to K-isomorphism.*

Proof. This follows immediately from Theorem 3.16 together with Theorem 3.14, as the properties are preserved by elementary substructures. □

Remark 3.18. Note that the result also holds under the weaker hypothesis that K is algebraically closed, $|\mathrm{Fix}(\sigma)(K)| < \kappa$, and $\kappa^{<\kappa} = \kappa \geq \aleph_1$, so that the theory of pseudofinite fields has a unique (up to K-isomorphism) saturated model of cardinality κ containing $\mathrm{Fix}(\sigma)(K)$. (This uses the stable embeddability of $\mathrm{Fix}(\sigma)$; see 2.10.)

References

[1] B. Afshordel, "Generic automorphisms with prescribed fixed fields", *J. Symb. Log.* **79**:4 (2014), 985–1000. MR Zbl

[2] Z. Chatzidakis, "A note on canonical bases and one-based types in supersimple theories", *Confluentes Math.* **4**:3 (2012), art. id. 1250004. MR Zbl

[3] Z. Chatzidakis, "A note on the non-existence of prime models of theories of pseudo-finite fields", preprint, 2020. arXiv 2004.05593

[4] Z. Chatzidakis, C. Hardouin, and M. F. Singer, "On the definitions of difference Galois groups", pp. 73–109 in *Model theory with applications to algebra and analysis*, vol. I, edited by Z. Chatzidakis et al., London Math. Soc. Lecture Note Ser. **349**, Cambridge Univ. Press, 2008. MR Zbl

[5] Z. Chatzidakis and E. Hrushovski, "Model theory of difference fields", *Trans. Amer. Math. Soc.* **351**:8 (1999), 2997–3071. MR Zbl

[6] Z. Chatzidakis and E. Hrushovski, "Model theory of endomorphisms of separably closed fields", *J. Algebra* **281**:2 (2004), 567–603. MR Zbl

[7] R. M. Cohn, *Difference algebra*, Interscience Publishers, New York, 1965. MR Zbl

[8] J.-L. Duret, "Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendence", pp. 136–162 in *Model theory of algebra and arithmetic* (Karpacz, Poland, 1979), edited by L. Pacholski et al., Lecture Notes in Math. **834**, Springer, 1980. MR Zbl

[9] M. D. Fried and M. Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Math. (3) **11**, Springer, 2008. MR Zbl

[10] E. Hrushovski, "Pseudo-finite fields and related structures", pp. 151–212 in *Model theory and applications*, edited by L. Bélair et al., Quad. Mat. **11**, Aracne, Rome, 2002. MR Zbl

[11] S. Lang, *Elliptic functions*, 2nd ed., Grad. Texts in Math. **112**, Springer, 1987. MR Zbl

[12] O. León Sánchez and M. Tressl, "Differentially large fields", preprint, 2020. To appear in *Algebra & Number Theory*. arXiv 2003.02886

[13] A. Pillay and S. Shelah, "Classification theory over a predicate, I", *Notre Dame J. Formal Logic* **26**:4 (1985), 361–376. MR Zbl

[14] S. Shelah and A. Usvyatsov, "Classification over a predicate — the general case: Part I — structure theory", preprint, 2019. arXiv 1910.10811

[15] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math. **106**, Springer, 2016. MR Zbl

Received 29 Aug 2022. Revised 31 Dec 2022.

ZOÉ CHATZIDAKIS:

zoe.chatzidakis@imj-prg.fr
Université Paris Cité and Sorbonne Université, CNRS, IMJ-PRG, F-75013 Paris, France

Model Theory

msp.org/mt

See inside back cover or msp.org/mt for submission instructions.

Model Theory (ISSN 2832-904X electronic, 2832-9058 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

MT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

https://msp.org/

Model Theory

no. 2 vol. 2 2023

Celebratory issue on the occasion of

Ehud Hrushovski's 60th Birthday