Bull. London Math. Soc. 33 (2001) 641–646
DOI: 10.1112/S0024609301008487

ON DIFFERENCE FIELDS WITH QUANTIFIER ELIMINATION

RAHIM MOOSA

Abstract

This paper proves that a difference field (E, σ) admits quantifier elimination if and only if E is an algebraically closed field, and σ is an integer power of the Frobenius automorphism.

1. *Introduction: superstable difference fields*

Let $\mathscr{L}$ be the language of fields augmented by a new unary function symbol σ. A *difference field* is a field equipped with a distinguished automorphism (which we shall also denote by σ), viewed as an $\mathscr{L}$-structure. In this paper we are concerned with difference fields that satisfy various properties of a model-theoretic nature; superstability and quantifier elimination, in particular.

A trivial way of constructing superstable difference fields is as follows. Let E be any superstable field, and let σ be a definable (in the pure field language) automorphism of E. Then (E, σ), as it has no additional structure, is still superstable. As superstable fields are algebraically closed, the only automorphisms that can arise in this way are the identity in characteristic 0, and integer powers of the Frobenius in positive characteristic. For any integer n, let Fr^n be the nth power of the Frobenius automorphism, given by $x \mapsto x^{p^n}$, where p is the characteristic of the field (if $p = 0$, then define $Fr^n = \text{id}$ for all n). So, if (E, σ) is a superstable difference field obtained as above, then for some integer n, $\sigma = Fr^n$. We call such difference fields *trivial*, as in this case the automorphism adds no new structure to the field. Note that trivial difference fields of characteristic 0 are just fields equipped with the identity automorphism.

E. Hrushovski has shown (this is a consequence of [**2**, Proposition 3]) that if (E, σ) is a superstable difference field, then either σ is the identity automorphism, or the fixed field of σ is finite. In particular, this says that all superstable difference fields in characteristic 0 are trivial. Conjecturally, *all* superstable difference fields are trivial. While we are not able to resolve this conjecture in general, the main result of this paper considers the following special case.

Theorem 1.1. *All difference fields admitting quantifier elimination* (*in the language* $\mathscr{L}$) *are trivial.*

Note that difference fields with quantifier elimination are superstable. This was shown by S. Nonvidé [**3**], using the difference algebraic methods developed by R. M. Cohn in [**1**], and by A. Pillay, using model-theoretic methods, in a course taught at the University of Illinois at Urbana-Champaign.

Received 3 February 2000; final revision 20 November 2000.

1991 *Mathematics Subject Classification* 03C60, 12H10.

The following proposition is the most that we are able to say about the general superstable situation, and will be used in the proof of Theorem 1.1.

PROPOSITION 1.2. *Let (E, σ) be a κ-saturated superstable difference field, where κ is some uncountable cardinal. Then either (E, σ) is trivial, or, over any difference subfield of cardinality less than κ, there exists a transformally transcendental element.*

We now establish notation for the rest of the paper. If (E, σ) is a difference field, $K \subset E$ a difference subfield, A a subset of E, and $a \in E$, then the following conventions will be used: $\overline{K}$ denotes the (field-theoretic) algebraic closure of K; $(a)_\sigma$ is the infinite tuple $(\dots, \sigma^{-2}(a), \sigma^{-1}(a), a, \sigma(a), \sigma^2(a), \dots)$; $K(a)_\sigma$ is the difference field generated by K and a; and $\operatorname{acl}_\sigma(A)$ is the field-theoretic algebraic closure of the difference field generated by A. The transcendence degree of $(a)_\sigma$ over K is called the *transformal transcendence degree of a over K*, and is denoted by $\deg_\sigma(a/K)$. Recall that if $\deg_\sigma(a/K)$ is finite, then a is said to be *transformally algebraic over K*; if $\deg_\sigma(a/K)$ is infinite, then a is said to be *transcendental over K*. Note that if $\deg_\sigma(a/K)$ is finite, then it is the unique nonnegative integer m such that for any (or, equivalently, for some) integer i, $\{\sigma^i(a), \dots, \sigma^{i+m-1}(a)\}$ is algebraically independent but $\{\sigma^i(a), \dots, \sigma^{i+m}(a)\}$ is not.

2. *Uniformly algebraic difference fields*

In this section we prove Proposition 1.2, and point out a more or less immediate consequence (Corollary 2.4 below). It is also worth mentioning that the only way in which superstability will be used in this section is to conclude that a superstable difference field is algebraically closed, and that its fixed field is either finite or the whole field.

We begin by establishing some convenient terminology. Let (E, σ) be a κ-saturated difference field, for some uncountable cardinal κ. We say that (E, σ) is *uniformly algebraic* if there exists a σ-polynomial over E that vanishes on all of E. That is, there exist $n > 0$ and $P \in E[X_0, \dots, X_n]$, such that for all $a \in E$, $P(a, \sigma(a), \dots, \sigma^n(a)) = 0$. By saturation, this is equivalent to the existence of a countable difference subfield, $K \subset E$, over which every element of E is transformally algebraic. In fact, if (E, σ) is not uniformly algebraic, then over any difference subfield of cardinality less than κ, there are transformally transcendental elements. In this latter case, we say that (E, σ) is *transformally transcendental.*

In these terms, Proposition 1.2 claims that all saturated superstable uniformly algebraic difference fields are trivial. This will be a consequence of the following characterisation of uniformly algebraic difference fields in general. Note the absence of any stability-theoretic assumptions.

PROPOSITION 2.1. *If $(\mathbf{E}, \sigma)$ is a κ-saturated uniformly algebraic difference field (where κ is uncountable), then for some $n > 0$ and some integer m, $\sigma^n = Fr^m$.*

We show right away how Proposition 1.2 follows from Proposition 2.1.

Fix a saturated uniformly algebraic difference field (E, σ), that is in addition superstable. By Proposition 2.1, for some $n > 0$ and some integer m, $\sigma^n = Fr^m$ on E. We wish to show that σ is itself an integer power of the Frobenius automorphism. By **[2]**, it is sufficient to show that on some infinite subfield of E, σ is an integer power of the Frobenius automorphism. To see this last assertion, note that if $\sigma = Fr^k$ on some infinite subfield, then the fixed field of $Fr^{-k}\sigma$ is infinite, and hence is all of E (as $(E, Fr^{-k}\sigma)$ is still superstable).

By superstability (using [**2**] again), we may assume that E is an algebraically closed field of positive characteristic, say p. Let $\mathbf{F}_p$ denote the prime field of E. We first note that as $\sigma^n = Fr^m$, n must divide m. This can be deduced by considering the restrictions of σ and Fr to $\overline{\mathbf{F}_p} \subset E$ and using some elementary facts about the absolute Galois group of $\mathbf{F}_p$. So let $m = nk$. But as $\mathrm{Gal}(\overline{\mathbf{F}_p}/\mathbf{F}_p)$ is torsion-free, we can take nth roots; and thus on $\overline{\mathbf{F}_p}$, $\sigma = Fr^k$. By the above arguments, this implies that $\sigma = Fr^k$ on all of E. □

We now turn our attention to Proposition 2.1.

Proof of Proposition 2.1. Our only assumption on $(\mathbf{E}, \sigma)$ is that it is κ-saturated for some uncountable cardinal κ, and that it is uniformly algebraic. Let $\overline{\mathbf{E}}$ denote the algebraic closure of $\mathbf{E}$.

There exist a positive integer n and a polynomial in $n+1$ variables over $\mathbf{E}$ that vanishes on $(a, \sigma(a), \ldots, \sigma^n(a))$, for all $a \in \mathbf{E}$. Let n be the least such positive integer. Our goal is to show that on $\mathbf{E}$, σ^n must be some integer power of Frobenius.

The first step is to replace $\mathbf{E}$ by an *algebraic* (that is, field-definable) object in $\overline{\mathbf{E}}^{n+1}$ (this will be V below). Let $H = \{(x, \sigma(x), \ldots, \sigma^n(x)) : x \in \mathbf{E}\} \subset \overline{\mathbf{E}}^{n+1}$. Let V be the Zariski closure of H in $\overline{\mathbf{E}}^{n+1}$. Let k be a (countable) algebraically closed subfield of $\overline{\mathbf{E}}$ over which V is defined. By the minimality of n (and saturation), H contains an element of transcendence degree n over k. This implies that the dimension of V as a (possibly reducible) algebraic variety over k is at least n. On the other hand, $V \neq \overline{\mathbf{E}}^{n+1}$, as H is contained in the zero set of a nontrivial polynomial in $n+1$ variables over k. That is, the dimension of V is n.

Next, we extend the ring structure on $\mathbf{E}$ (which is immediately inherited by H) to V. As H is a subgroup of the algebraic group $\overline{\mathbf{E}}^{n+1}$ under coordinatewise addition, V (being the Zariski closure of H in $\overline{\mathbf{E}}^{n+1}$) is an algebraic subgroup of $(\overline{\mathbf{E}}^{n+1}, +)$. We want to show that V is in fact a subring; that is, it is closed under coordinatewise multiplication. Let $w \in H$ and let $M_w = \{v \in V \mid vw \in V\}$. Then M_w is a closed Zariski subset of V containing H (as H is closed under multiplication), and hence $M_w = V$. That is, for all $w \in H$ and $v \in V$, $vw \in V$. Now let $v \in V$. Then $\{w \in V \mid vw \in V\}$ is a closed Zariski subset of V which, as we have just seen, contains H—and hence is all of V. That is, for all $v, w \in V$, $vw \in V$. We have shown that V is an algebraic *subring* of $\overline{\mathbf{E}}^{n+1}$ under coordinatewise addition and multiplication.

The next step is to establish that V is the graph of a surjective function from $\overline{\mathbf{E}}^n$ to $\overline{\mathbf{E}}$. Let π_1 be the projection map from $\overline{\mathbf{E}}^{n+1}$ to the first n factors, and let π_2 be the projection map from $\overline{\mathbf{E}}^{n+1}$ to the last factor.

LEMMA 2.2. *The projections π_1 and π_2 restricted to V are surjective.*

Proof. For $a \in \mathbf{E}$ transcendental over k, $\sigma^n(a)$ is transcendental over k, and is contained in $\pi_2(V)$. Hence $\pi_2(V)$ is an infinite field-definable subgroup of $\overline{\mathbf{E}}^+$. By the strong minimality of algebraically closed fields, it must be all of $\overline{\mathbf{E}}$.

Similarly, $\pi_1(V)$ is a field-definable subgroup of $(\overline{\mathbf{E}}^+)^n$, and hence it is sufficient to show that it contains an element of transcendence degree n. By the minimality of n, $\pi_1(H)$ contains such an element, and hence so does $\pi_1(V)$. □

LEMMA 2.3. *For all* $x \in \overline{\mathbf{E}}^n$, $V_x = \{y \in \overline{\mathbf{E}} \mid (x, y) \in V\}$ *is a singleton.*

Proof. First of all, as $\pi_1(V) = \overline{\mathbf{E}}^n$ (by Lemma 2.2), each fibre is nonempty. As the projection to the first n factors is an algebraic group homomorphism, each fibre is an additive translate of the kernel, that is, of the fibre above $0 \in \overline{\mathbf{E}}^n$. So it is sufficient to show that $V_0 = \{0\}$. We do this by showing that V_0 is an ideal in $\overline{\mathbf{E}}$. Clearly, it is a subgroup. Let $h \in \overline{\mathbf{E}}$ and $v \in V_0$. As π_1 restricted to V is surjective, there is an $x \in \overline{\mathbf{E}}^n$ such that $(x, h) \in V$. Now, $(x, h)(0, v) = (0, hv) \in V$, and so $hv \in V_0$. Hence V_0 is an ideal of $\overline{\mathbf{E}}$. On the other hand, V_0 cannot be all of $\overline{\mathbf{E}}$, or else this would be true of each fibre, and V would be all of $\overline{\mathbf{E}}^{n+1}$. But $\dim V = n$. Thus $V_0 = \{0\}$, as desired. □

By Lemmas 2.2 and 2.3, V is the graph of a (field-)definable surjective function, $\phi : \overline{\mathbf{E}}^n \to \overline{\mathbf{E}}$. Since V is a subring of $\overline{\mathbf{E}}^{n+1}$, ϕ is a ring homomorphism. Note that by construction, if $x \in \mathbf{E}$, then

$$\phi(x, \sigma(x), \ldots, \sigma^{n-1}(x)) = \sigma^n(x).$$

As $\ker \phi$ must be a maximal ideal of $\overline{\mathbf{E}}^n$, it is a product of $n-1$ of the factors with $\{0\}$ in one of the coordinates, say the ith coordinate. Hence ϕ induces a (field-)definable automorphism of $\overline{\mathbf{E}}$: more precisely, an isomorphism from the ith factor of the domain of ϕ onto $\overline{\mathbf{E}}$. But the only field-definable automorphisms of an algebraically closed field are the integer powers of the Frobenius automorphism. So for some integer m, ϕ induces Fr^m on $\overline{\mathbf{E}}$. In particular, for all $x \in \mathbf{E}$, $Fr^m(\sigma^i(x)) = \sigma^n(x)$. This yields an algebraic relationship between $\sigma^i(x)$ and $\sigma^n(x)$, contradicting the minimality of n unless $i = 0$. Reading the above relationship with $i = 0$, we find that for all $x \in \mathbf{E}$, $Fr^m(x) = \sigma^n(x)$; that is, $Fr^m = \sigma^n$ on $\mathbf{E}$. This completes the proof of Proposition 2.1, and hence of Proposition 1.2. □

The following corollary will not be used in this paper, but may be of some independent interest.

COROLLARY 2.4. *Let* $(\mathbf{E}, \sigma)$ *be an* ω_1*-saturated superstable difference field. Suppose that for any countable* $A \subset \mathbf{E}$, $\mathrm{acl}_\sigma(A)$ *is model-theoretically algebraically closed. Then* $(\mathbf{E}, \sigma)$ *is trivial.*

Proof. By Proposition 1.2, it is sufficient to prove that there are no transformally transcendental elements in $\mathbf{E}$ over the prime field, $\mathbf{F}$. Suppose that $a \in \mathbf{E}$ is transformally transcendental over $\mathbf{F}$, and seek a contradiction. We know by [**2**], as above, that the fixed field of σ is finite; and so the map $\delta(x) = \sigma(x)x^{-1}$ is a definable endomorphism of $\mathbf{E}^\times$ with finite kernel. It follows that a is (model-theoretically) algebraic over $b = \delta(a)$. By assumption, this implies that a is field-theoretically algebraic over $\mathbf{F}(b)_\sigma$. That is, for some n, $\mathbf{F}(a, \sigma^{-n}(b), \ldots, b, \ldots, \sigma^n(b))$ has transcendence degree $\leqslant 2n + 1$ over $\mathbf{F}$. Now, by choice of b,

$$\mathbf{F}(a, \sigma^{-n}(b), \ldots, b, \ldots, \sigma^n(b)) = \mathbf{F}(\sigma^{-n}(a), \ldots, a, \ldots, \sigma^{n+1}(a)).$$

But as a is transformally transcendental over $\mathbf{F}$, the right-hand side has transcendence degree $2n + 2$ over $\mathbf{F}$. This contradiction proves the corollary. □

3. *Transformally transcendental difference fields*

In this section we prove that ω_1-saturated transformally transcendental difference fields *do not* admit quantifier elimination in the language $\mathscr{L}$. Since difference fields admitting quantifier elimination are superstable, this together with Proposition 1.2 (proved in the previous section) will yield Theorem 1.1; that is, all difference fields admitting quantifier elimination are trivial.

Fix $(\mathbf{E}, \sigma)$, an ω_1-saturated difference field that is transformally transcendental over a countable difference subfield $k \subset \mathbf{E}$. To begin with, we may assume that $\mathbf{E}$ is algebraically closed (or else $(\mathbf{E}, \sigma)$ does not admit quantifier elimination and we are done) and k is the algebraic closure of the prime field. We aim to show that quantifier-free types in $(\mathbf{E}, \sigma)$ do not determine complete types. We shall do this by constructing two distinct complete types over k with the same quantifier-free fragment.

Let q be a prime number different from char($\mathbf{E}$). If one is willing to assume that char($\mathbf{E}$)$\neq 2$, then we can let $q = 2$ and some of the notation is simplified. Let ζ be a qth root of unity not equal to the identity, and choose $a, b \in \mathbf{E}$ such that $b^q = a$ with a (and hence b) transformally transcendental over k. Note that ζ generates the group of qth roots of unity, and that all these roots are in k. Moreover, σ permutes the qth roots of unity and (as it fixes the identity) there is a positive integer n strictly less than q such that σ^n fixes ζ. The action of σ on the qth roots of unity is determined by its action on ζ, and thus σ^n fixes all the qth roots of unity. In the case where $q = 2$, we see that ζ is -1 and n is 1.

Now let

$$p_1(x) = \mathrm{tp}\Big(\frac{b}{\sigma^n(b)}/k(a)_\sigma\Big) \quad \text{and} \quad p_2(x) = \mathrm{tp}\Big(\frac{b}{\sigma^n(\zeta^n b)}/k(a)_\sigma\Big).$$

Let $\phi(x, a)$ be the formula

$$\exists y \Big(y^q = a \wedge \frac{y}{\sigma^n(y)} = x\Big).$$

Clearly, $\mathbf{E} \models \phi(b/\sigma^n(b), a)$ with $y = b$. On the other hand, if $y^q = a$, then for some $0 \leqslant i \leqslant q$, $y = \zeta^i b$. As σ^n fixes all qth roots of unity, we get

$$\frac{y}{\sigma^n(y)} = \frac{\zeta^i b}{\zeta^i \sigma^n(b)} = \frac{b}{\sigma^n(b)}.$$

But as $0 < n < q$, we know that $\zeta^n \neq 1$, and so $y/\sigma^n(y) \neq b/\sigma^n(\zeta^n b)$. That is, $b/\sigma^n(\zeta^n b)$ does not satisfy the formula $\phi(x, a)$. Hence $p_1 \neq p_2$, as $p_1 \vdash \phi(x, a)$ and $p_2 \vdash \neg\phi(x, a)$.

Our next task, then, is to show that p_1 and p_2 have the same quantifier-free fragment. Let $L \subset \mathbf{E}$ be the difference subfield $k(b/\sigma^n(b), a)_\sigma = k(b/\sigma^n(\zeta^n b), a)_\sigma$. We shall construct an automorphism of (L, σ) fixing $k(a)_\sigma$ pointwise and taking $b/\sigma^n(b)$ to $b/\sigma^n(\zeta^n b)$. This will imply that p_1 and p_2 have the same quantifier-free fragment.

The desired automorphism will be defined in a series of steps. To begin with, by transformal transcendentality of b over k, $(\sigma^i(b))_i$ and $(\sigma^i(\zeta b))_i$ are both transcendence bases for $k(b)_\sigma$ over k. Hence, working in the pure field structure, the map τ taking $\sigma^i(b)$ to $\sigma^i(\zeta b)$ for all integers i determines a k-(field-)automorphism of $k(b)_\sigma$. Now τ fixes $k(a)_\sigma$ pointwise; indeed, for each i, both $\sigma^i(b)$ and $\sigma^i(\zeta b)$ are qth roots of $\sigma^i(a)$. Since τ commutes with σ and fixes $b/\sigma^n(b)$ (as σ^n fixes ζ), we find that τ fixes

$L \subset k(b)_\sigma$ pointwise. Hence $\tau\sigma$ is a (field-)automorphism of $k(b)_\sigma$ that agrees with σ on L. That is, (L, σ) is a substructure of each of $(k(b)_\sigma, \sigma)$ and $(k(b)_\sigma, \tau\sigma)$.

Now consider the sequence $((\tau\sigma)^i(b))_i$. As τ commutes with σ and permutes the qth roots of $\sigma^i(a)$ (namely, $\{\sigma^i(b), \sigma^i(\zeta b), \ldots, \sigma^i(\zeta^{q-1}b)\}$) for each i, we see that $((\tau\sigma)^i(b))_i$ is again a transcendence basis for $k(b)_\sigma$ over k. But we are in a better position this time, since our new sequence is obtained by the iterated application of an automorphism to b (namely, $\tau\sigma$)—and hence the map β taking $\sigma^i(b)$ to $(\tau\sigma)^i(b)$ for each i determines a k-isomorphism (of difference fields, this time) from $(k(b)_\sigma, \sigma)$ to $(k(b)_\sigma, \tau\sigma)$. We want to know what β does to L. Once again β will fix $k(a)_\sigma$ pointwise (as both $\sigma^i(b)$ and $(\tau\sigma)^i(b)$ are qth roots of $\sigma^i(a)$ for each i). Moreover,

$$\beta\Big(\frac{b}{\sigma^n(b)}\Big) = \frac{b}{(\tau\sigma)^n(b)} = \frac{b}{\zeta^n\sigma^n(B)} = \frac{b}{\sigma^n(\zeta^n b)}.$$

Hence β takes $(b/\sigma^n(b))_\sigma$ to $(b/\sigma^n(\zeta^n b))_{\tau\sigma}$. As $\tau\sigma$ and σ agree on L, and

$$L = k(a)_\sigma\Big(\frac{b}{\sigma^n(b)}\Big)_\sigma = k(a)_\sigma\Big(\frac{b}{\sigma^n(\zeta^n b)}\Big)_\sigma,$$

we see that β restricts to an automorphism of (L, σ), fixing $k(a)_\sigma$ pointwise and taking $b/\sigma^n(b)$ to $b/\sigma^n(\zeta^n b)$, as desired.

What we have shown is that

$$\operatorname{qftp}\left(a, \frac{b}{\sigma^n(b)}/k\right) = \operatorname{qftp}\left(a, \frac{b}{\sigma^n(\zeta^n b)}/k\right)$$

but

$$\operatorname{tp}\left(a, \frac{b}{\sigma^n(b)}/k\right) \neq \operatorname{tp}\left(a, \frac{b}{\sigma^n(\zeta^n b)}/k\right).$$

Hence $(\mathbf{E}, \sigma)$ *does not* eliminate quantifiers. □

We have completed the proof of Theorem 1.1. Indeed, let (E, σ) be a difference field admitting quantifier elimination in the language $\mathscr{L}$. Let (E', σ) be an elementary extension of (E, σ) that is ω_1-saturated. Then (E', σ) also admits quantifier elimination, and so by what we have just seen, (E', σ) must be transformally algebraic. Since (E', σ) is superstable, Proposition 1.2 implies that (E', σ) must be trivial. Hence (E, σ) is trivial, as desired. □

ACKNOWLEDGEMENTS. I would like to thank Zoé Chatzidakis and Anand Pillay for their helpful suggestions. I would also like to thank the CNRS-UIUC cooperation programme for supporting me at the Université Paris 7, where part of the work presented here was done.

References

1. R. M. COHN, *Difference algebra*, Tracts in Mathematics 17 (Interscience, New York, 1965).

2. E. HRUSHOVSKI, 'On superstable fields with automorphisms', *The model theory of groups* (Ed. A. Nesin and A. Pillay, University of Notre Dame Press, 1989).

3. S. NONVIDÉ, 'Corps aux différences finies', *C. R. Acad. Sci. Paris* (1992) 423–425.

Department of Mathematics
University of Illinois
at Urbana-Champaign
1409 West Green Street
Urbana, Illinois 61801, USA

moosa@math.uiuc.edu