The Journal of Symbolic Logic
Volume 80, Number 4, December 2015

A PSEUDOEXPONENTIAL-LIKE STRUCTURE ON THE ALGEBRAIC NUMBERS

VINCENZO MANTOVA

Abstract. Pseudoexponential fields are exponential fields similar to complex exponentiation which satisfy the Schanuel Property, i.e., the abstract statement of Schanuel's Conjecture, and an adapted form of existential closure.

Here we show that if we remove the Schanuel Property and just care about existential closure, it is possible to create several existentially closed exponential functions on the algebraic numbers that still have similarities with complex exponentiation. The main difficulties are related to the arithmetic of algebraic numbers, and they can be overcome with known results about specialisations of multiplicatively independent functions on algebraic varieties.

§1. Introduction. Pseudoexponentiation is a structure introduced by Zilber in [7] in order to find out how $\mathbb{C}_{\exp}$ should look like if it were well-behaved, at least for the criteria of a model theorist. The unavoidable problem of $\mathbb{C}_{\exp}$ is that it defines the ring of integers, hence Peano's arithmetic, defying the model-theoretic tools widely used in the last decades.

However, Zilber proved that if $\mathbb{C}_{\exp}$ satisfies certain algebraic conjectures, Peano's arithmetic is in some sense the only true problem. He showed that there is a sentence Ψ, in the infinitary language $\mathcal{L}_{\omega_1,\omega}(Q)$, which is *uncountably categorical*, and that describes an exponential field which is reasonably similar to $\mathbb{C}_{\exp}$. Its models have been called pseudoexponential fields, perfect exponential fields, or Zilber fields. The two main statements contained in Ψ, which are currently only conjectures for $\mathbb{C}_{\exp}$, are the Schanuel Property and the Strong Exponential-algebraic Closure.

The Schanuel Property is just a rephrasing of Schanuel's Conjecture for an abstract exponential function E, and it asserts that for any $z_1, \dots, z_n$ in the base field we have

$$\text{tr. deg.}(z_1, \dots, z_n, E(z_1), \dots, E(z_n)) \geq \text{lin. d.}_{\mathbb{Q}}(z_1, \dots, z_n).$$

It is well known that the Schanuel Property is not enough to characterise well an exponential function, as formally shown by Hyttinen in [1]: there are $2^{2^{\aleph_0}}$ pairwise nonisomorphic surjective exponential functions on $\mathbb{C}$ satisfying the Schanuel Property and whose kernel is a cyclic group.

Here we show a related result, in a quite different vein, about the Exponential-algebraic Closure. We show that if we drop all the assumptions about transcendence

Received June 9, 2014.
Key words and phrases. exponential fields, exponential-algebraic closure, multiplicative dependencies.

© 2015, Association for Symbolic Logic
0022-4812/15/8004-0013
DOI:10.1017/jsl.2014.41

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

in Zilber's axiom Ψ, then we can construct several model where the Schanuel Property is falsified in the most drastic way: everything is algebraic!

THEOREM 1.1. *There is a function* $E : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ *such that*

(1) $E(x+y) = E(x) \cdot E(y)$ *for all* $x, y \in \overline{\mathbb{Q}}$;
(2) $\ker(E) = \omega\mathbb{Z}$ *for some* $\omega \in \overline{\mathbb{Q}}^*$;
(3) E *is surjective*;
(4) *for any absolutely free variety* V *over* $\overline{\mathbb{Q}}$ *there is a* $\overline{z} \subset \overline{\mathbb{Q}}$ *such that* $(\overline{z}, E(\overline{z})) \in V$, *and the points of this form are Zariski-dense in* V.

If we consider the class of structures K_E, where K is a field and E is an exponential function with cyclic kernel, then $\overline{\mathbb{Q}}_E$ is existentially closed: whenever $\overline{\mathbb{Q}}_E \subset K_{E'}$, and some finite system of polynomial exponential equations and inequations with parameters in $\overline{\mathbb{Q}}$ has a solution in $K_{E'}$, then it already has a solution in $\overline{\mathbb{Q}}_E$.

The proof of Theorem 1.1 is given using an explicit inductive construction very similar to the one of [4] and it is described, along with the list of Zilber's axioms, in Section 2. The fact that the construction itself is well-defined, and it works as desired, is proved in Section 3, thanks to some arithmetic properties of number fields about specialisations that were analysed in [6].

The author would like to thank his supervisor Prof. Alessandro Berarducci, who proposed to study pseudoexponential fields, Jonathan Kirby for having proposed the problem solved in this paper, Profs. David Masser and Umberto Zannier for the suggestions about the number-theoretic part of this paper that greatly simplified the discussion, and an anonymous referee for the useful corrections. This work was part of the author's PhD work at the italian Scuola Normale Superiore of Pisa, and it has been partially supported by the PRIN-MIUR 2009 "O-minimalità, teoria degli insiemi, metodi e modelli nonstandard e applicazioni", the EC's Seventh Framework Programme [FP7/2007–2013] under grant agreement no. 238381, and the FIRB 2010 "Nuovi sviluppi nella Teoria dei Modelli dell'esponenziazione".

§2. The construction.

2.1. Zilber's original axiomatisation. For the sake of clarity, we briefly recall the axiomatisation of actual pseudoexponential fields. A field K_E is a pseudoexponential field if it satisfies the following list of axioms. The terms in quotation marks are not defined here; we shall only explain the meaning of the properties that actually matter for our purposes. We refer the reader to [5, 7] for a more complete treatment of the subject.

2.1.1. Trivial properties of $\mathbb{C}_{\exp}$.

(ACF_0) K is an algebraic closed field of characteristic 0.
(E) E is a homomorphism $E : (K, +) \to (K^*, \cdot)$.
(LOG) E is surjective (every nonzero element has a logarithm).
(STD) the kernel is a cyclic group, i.e., $\ker E = \omega\mathbb{Z}$ for some $\omega \in K^*$.

2.1.2. Axioms conjecturally true on $\mathbb{C}_{\exp}$.

(SP) *Schanuel Property*: for every $z_1, \ldots, z_n \in K$

$$\text{tr. deg.}(z_1, \ldots, z_n, E(z_1), \ldots, E(z_n)) \geq \text{lin. d.}_{\mathbb{Q}}(z_1, \ldots, z_n).$$

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

(SEC) *Strong Exponential-algebraic Closure*: for every irreducible "absolutely free rotund" algebraic variety $V \subset K^n \times (K^*)^n$, and every finite subset $\overline{c} \subset K$ such that V is defined over $\overline{c}$, there is a $\overline{z} \in K^n$ such that $(\overline{z}, E(\overline{z}))$ is a generic point of V over $\overline{c}$.

2.1.3. A non-trivial property of $\mathbb{C}_{\exp}$ [7, Lemma 5.12].

(CCP) *Countable Closure Property*: for every irreducible "absolutely free rotund" algebraic variety $V \subset \mathbb{G}^n$ over K of "depth 0", and every finite subset $\overline{c} \subset K$ such that V is defined over $\overline{c}$, the set of the points of V of the form $(\overline{z}, E(\overline{z}))$ that are generic over $\overline{c}$ is at most countable.

For the purposes of this paper, we actually only care about the meaning of "absolutely free". The additional properties "rotund" and "depth 0" are deeply related to the presence of the Schanuel Property, and moreover they have rather complicated definitions, so we will omit them here.

DEFINITION 2.1. An irreducible algebraic variety $V \subset K^n \times (K^*)^n$ is *additively free* over $L \subset K$ if its projection onto K^n is not contained in a proper $\mathbb{Q}$-linear subspace defined over L. In other words, the coordinate functions of the factor K^n restricted to V are $\mathbb{Q}$-linearly independent from L.

We can state a similar property for the multiplicative side $(K^*)^n$.

DEFINITION 2.2. An irreducible algebraic variety $V \subset K^n \times (K^*)^n$ is *multiplicatively free* over $M \subset K^*$ if its projection onto $(K^*)^n$ is not contained in a proper algebraic subgroup of $(K^*)^n$ defined over M. In other words, the coordinate functions of the factor $(K^*)^n$ restricted to V are multiplicatively independent from M.

Absolute freeness is when we have both properties with $L = K$ and $M = K^*$.

DEFINITION 2.3. A variety $V \subset K^n \times (K^*)^n$ is *absolutely additively free* if it is additively free over K.

V is *absolutely multiplicatively free* if it is multiplicatively free over K^*.

V is *absolutely free* if it is both absolutely additively free and absolutely multiplicatively free.

2.2. Axioms for $\overline{\mathbb{Q}}_E$. Our goal is to build an exponential field $\overline{\mathbb{Q}}_E$ as similar as possible to pseudoexponentiation, but clearly without the axiom (SP). We definitely want, and actually we can, keep the trivial properties of $\mathbb{C}_{\exp}$ as they are. Moreover, the axiom (CCP) doesn't even need to be mentioned, as $\overline{\mathbb{Q}}$ itself is countable. The only axiom that requires some changes is (SEC), as it requires the points $(\overline{z}, E(\overline{z}))$ to be "generic", and in particular of transcendence degree more than zero, which is not possible in $\overline{\mathbb{Q}}$.

The axiom (SEC) is a special form of existential closure adapted to the presence of (SP) and to Hrushovski's amalgamation: if a system of equations and inequations in K_E has a solution in some "strong kernel preserving extension", than it has already a solution in K_E, plus a genericity assumption. For our purpose, we shall require that if a system of equations has a solution in some kernel preserving extension of $\overline{\mathbb{Q}}_E$, then it has a solution in $\overline{\mathbb{Q}}_E$. We drop genericity, and we simplify the discussion

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

by also dropping the word "strong", which is due to the presence of (SP) and it is therefore irrelevant for our purposes.

It can be easily verified that this condition is equivalent to the following:

(EC) For any absolutely free variety $V \subset \overline{\mathbb{Q}}^n \times (\overline{\mathbb{Q}}^*)^n$ there is a $\overline{z} \in \overline{\mathbb{Q}}^n$ such that $(\overline{z}, E(\overline{z})) \in V$, and the points of this form are Zariski-dense in V.

The two differences with (SEC) are that we do not require V to be rotund, which is essentially linked to the use of strong extensions and the presence of (SP), and that we explicitly force the points $(\overline{z}, E(\overline{z}))$ to be Zariski-dense, while in (SEC) this is automatic by genericity. (As we will note later, a quite standard argument can be used to show that the density condition is actually redundant.)

2.3. The construction. The construction is quite similar to other construction techniques [3, 4]. We define the function E by induction using a back-and-forth procedure.

Let us fix $\omega \in \overline{\mathbb{Q}}^*$ and let us define our base function as $E_{-1}(\frac{p}{q}\omega) = \zeta_q^p$, for $p, q \in \mathbb{Z}$, where $\{\zeta_q\}_{q\in\mathbb{Z}}$ is a "coherent" system of roots of unity, where by coherent we mean that $\zeta_{pq}^p = \zeta_q$ for all $p, q \in \mathbb{N}$. This yields $\ker(E_{-1}) = \omega\mathbb{Z}$.

Now let $\{\alpha_n\}$ be an enumeration of $\overline{\mathbb{Q}}^*$ and V_n an enumeration of all the irreducible absolutely free algebraic varieties V_n. At each step $n < \omega$ we proceed as follows:

(1) If α_n is not in the domain of E_{n-1}, we choose some $\beta \in \overline{\mathbb{Q}}^* \setminus \mathrm{img}(E_{n-1})$ and we define
$$E_{n-1}^1\left(\alpha + \frac{p}{q}\alpha_n\right) := E_{n-1}(\alpha) \cdot \beta^{p/q},$$
for all $\alpha \in \mathrm{dom}(E_{n-1})$ and $p, q \in \mathbb{Z}$, where $\beta^{1/q}$ is a coherent system of roots of β. If α_n is in the domain, we just define $E_{n-1}^1 := E_{n-1}$.

(2) If α_n is not in the image, we choose some $\beta \in \overline{\mathbb{Q}} \setminus \mathrm{dom}(E_{n-1}^1)$ and we define
$$E_{n-1}^2\left(\alpha + \frac{p}{q}\beta\right) := E_{n-1}^2(\alpha) \cdot \alpha_n^{p/q},$$
for all $\alpha \in \mathrm{dom}(E_{n-1}^1)$ and $p, q \in \mathbb{Z}$. If α_n is already in the image, we just define $E_{n-1}^2 := E_{n-1}^1$.

(3) If $V_n \subset \overline{\mathbb{Q}}^k \times (\overline{\mathbb{Q}}^*)^k$, we take a point $(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k) \in V_n$ such that
   (a) $\alpha_1, \dots, \alpha_k$ is $\mathbb{Q}$-linearly independent from $\mathrm{dom}(E_{n-1}^2)$;
   (b) $\beta_1, \dots, \beta_k$ is multiplicatively independent from $\mathrm{img}(E_{n-1}^2)$;
   and we define $E_n\left(\alpha + \frac{p_1}{q_1}\alpha_1 + \cdots + \frac{p_k}{q_k}\alpha_k\right) := E_{n-1}^2(\alpha) \cdot \beta_1^{p_1/q_1} \cdot \cdots \cdot \beta_k^{p_k/q_k}$ for all $\alpha \in \mathrm{dom}(E_{n-1}^2)$ and $p_i, q_i \in \mathbb{Z}$.

The limit function $E := \bigcup_{n<\omega} E_n$ is the function we looked for in Theorem 1.1. We can verify that the above construction is sound; the only critical step is (3), since it is not completely trivial that such a choice of α_i and β_i is possible. However, their existence can be deduced from Proposition 3.5, which is described in the next section.

Proof of Theorem 1.1. It is immediate to see that the steps (1) and (2) can always be performed, as $\mathrm{dom}(E_n)$, $\mathrm{img}(E_n)$, $\mathrm{dom}(E_n^1)$ and $\mathrm{img}(E_n^1)$ are always finite-rank groups, and therefore we can always find a suitable β.

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

Since $\mathrm{dom}(E_n^2)$ and $\mathrm{img}(E_n^2)$ are finite-rank subgroups as well, Proposition 3.5 implies that V_n contains a point with the required properties for step (3).

It is again immediate to see that E_n is a well defined function, and in particular E is well defined too, since $\mathrm{dom}(E_n)$ is always a $\mathbb{Q}$-vector space, and the new elements on which we define the function are always $\mathbb{Q}$-linearly independent from the previous domain. Moreover, E is defined everywhere.

Similarly, $\ker(E) = \ker(E_n) = \ker(E_{-1}) = \omega\mathbb{Z}$, since every time we define the new function, the new elements in the image are multiplicatively independent from the previous image. Moreover, E is surjective.

Finally, it is clear that each absolutely free variety contains a point of the form $(\overline{z}, E(\overline{z}))$. It is a standard argument to show that if every absolutely free variety V contains such a point, then such points are Zariski-dense.

Indeed, let V be a given irreducible absolutely free algebraic variety in $\overline{\mathbb{Q}}^k \times (\overline{\mathbb{Q}}^*)^k$ and let $W \subset V$ be a Zariski-closed proper subset of V. Without loss of generality, we may assume that there is a polynomial $p(\overline{x}) \in K[x_1, \ldots, x_{2k}]$ such that $W = V \cap \{p(\overline{x}) = 0\}$. It is now sufficient to consider the variety $H \subset \overline{\mathbb{Q}}^{k+1} \times (\overline{\mathbb{Q}}^*)^{k+1}$ defined by the same equations defining V on the first $2k$ coordinates of $\overline{\mathbb{Q}}^{k+1}$ and of $(\overline{\mathbb{Q}}^*)^{k+1}$, and by the equation $p(\overline{x})x_{2k+1} = 1$, where x_{2k+1} is the last coordinate of $\overline{\mathbb{Q}}^{k+1}$. This variety must contain a point of the form $(\overline{z}', E(\overline{z}'))$; its projection on $\overline{\mathbb{Q}}^k \times (\overline{\mathbb{Q}}^*)^k$ is a point of V outside of W. On varying W, this shows that such points are Zariski-dense in V. ⊣

Free exponential closure. We want to remark the fact that our construction actually satisfies the following "free" version of exponential-algebraic closure:

(FEC) *Free Exponential-algebraic Closure*: for every irreducible absolutely free algebraic variety $V \subset \overline{\mathbb{Q}}^n \times (\overline{\mathbb{Q}}^*)^n$, and every finite subset $\overline{c} \subset \overline{\mathbb{Q}}$, there is a $\overline{z} \in K^n$ such that $(\overline{z}, E(\overline{z})) \in V$ and $\overline{z}$ is $\mathbb{Q}$-linearly independent from $\overline{c}$.

This behaviour mimics the genericity assumption in (SEC), and it is in fact deeply related to it: it is shown in [2] that (SP) and (FEC) taken together imply (SEC).

§3. Points with independent coordinates. In order to finish the proof, we need to verify that absolutely free algebraic varieties always contain the points needed for step (3).

It is known that if we take a variety V and some functions on it that are multiplicatively independent (the functions are allowed to be constant), then for "most" points $P \in V(\overline{\mathbb{Q}})$ the values of the functions at P are still multiplicatively independent [6].

Similarly, it is also not difficult to show that for "most" points the specialisations of $\mathbb{Q}$-linearly independent functions are still $\mathbb{Q}$-linearly independent (again, the functions are allowed to be constant). In order to put together the two statements, we first intersect our variety with hyperplanes, using Bertini's theorem, to reduce to the case when V is a curve, and then we prove the case of curves. We first take care of the additive part.

PROPOSITION 3.1. *Let $\mathcal{C}$ be an absolutely irreducible curve defined over a field K, and let $k = \overline{\mathbb{Q}} \cap K$. Let $z_1, \ldots, z_n$ be some $\mathbb{Q}$-linearly independent functions in $K(\mathcal{C})$ (possibly constant).*

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

There is a number $d > 0$ such that for any nonconstant $x \in K(\mathcal{C})$, for any $\alpha \in \overline{\mathbb{Q}}$ with $[k(\alpha) : k] > d$, and for any nonsingular point $P \in x^{-1}(\alpha)$, the specialisations of $z_1, \dots, z_n$ at P are $\mathbb{Q}$-linearly independent.

PROOF. Let e be the maximum of $[K(\mathcal{C}) : K(z_i)]$ as z_i ranges among the nonconstant functions in the set $\{z_i\}_{i=1}^n$.

By assumption, if $m_1, \dots, m_n$ are some integer numbers, not all zero, the function $m_1 z_1 + \cdots + m_n z_n$ is not null. In particular, if it is constant, it never vanishes, while if it is nonconstant, its degree is at most ne, and therefore it vanishes on at most ne points of $\mathcal{C}$.

Now let $d := ne$ and let α and P be given as in the hypothesis: α is an algebraic number such that $[k(\alpha) : k] > d$ and P is a nonsingular point in $x^{-1}(\alpha)$. Let L be a normal extension of K that defines P. Clearly, $L \cap \overline{\mathbb{Q}} \supset k(\alpha)$ is a normal extension of k by the assumption $k = K \cap \overline{\mathbb{Q}}$. Since $\mathcal{C}$ is absolutely irreducible, we can extend the Galois action of $\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(L(\mathcal{C})/K(\mathcal{C}))$. Suppose by contradiction that there are integers $m_1, \dots, m_n$, not all zero, such that

$$m_1 z_1(P) + \cdots + m_n z_n(P) = 0,$$

then by conjugation we obtain several other $\sigma(P)$'s satisfying the same equality. Since $x(\sigma(P)) = \sigma(\alpha)$ and $[k(\alpha) : k] > ne$, we find that $m_1 z_1 + \cdots + m_n z_n$ vanishes at more than ne distinct conjugates of P, contradicting our previous observation, as desired. ⊣

COROLLARY 3.2. *Let $\mathcal{C}$ be an absolutely irreducible curve defined over a field k. Let $z_1, \dots, z_n$ be some $\mathbb{Q}$-linearly independent functions in $k(\mathcal{C})$.*

There is a number $d' > 0$ such that for any $P \in \mathcal{C}(\overline{k})$ with $[k(P) : k] > d'$, the specialisations of $z_1, \dots, z_n$ at P are $\mathbb{Q}$-linearly independent.

PROOF. Let us take a nonconstant function $x \in k(\mathcal{C})$ and let e be its degree.

Let d be the number obtained by Proposition 3.1 applied to x and $z_1, \dots, z_n$, and let d' be a number large enough so that $d' \geq d \cdot e$ and such that any point P with $[k(P) : k] > d'$ is nonsingular.

Now, if P is a point with $[k(P) : k] > d'$, then $x(P)$ is defined, finite and $[k(x(P)) : k] > d$. By the previous proposition, the specialisations of $z_1, \dots, z_n$ at P are $\mathbb{Q}$-linearly independent. ⊣

An analogous but different statement holds in the multiplicative case for varieties of dimension greater than 1.

PROPOSITION 3.3. *Let V be an absolutely irreducible variety defined over a field k with $\dim(V) > 1$. Let $w_1, \dots, w_n$ be some functions in $k(V)$ that are multiplicatively independent over $\overline{k}^*$.*

There is a nonconstant function $x \in k(V)$ such that the restrictions of $w_1, \dots, w_n$ at $V \cap x^{-1}(\alpha)$ are multiplicatively independent over $\overline{k}^*$ for almost all $\alpha \in \overline{k}$.

PROOF. Up to birational equivalence, we may assume that V is smooth and projective.

Since $w_1, \dots, w_n$ are multiplicatively independent modulo constants, it means that the Weil divisors of $w_1, \dots, w_n$ are $\mathbb{Q}$-linearly independent. Up to taking a multiplicative combination of the w_i's, we may assume that there are $W_1, \dots, W_n$ distinct prime divisors such that w_i has a pole in W_i, but has no zeroes and poles

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

among the remaining W_j's; in other words, the matrix $(o_{W_i}(w_j))_{i,j}$ is diagonal, where $o_{W_i}(w_j)$ is the order of w_j at W_i.

Up to enlarging k, we may assume that these prime divisors have degree 1 and are all defined over k. It is clear that among all the hyperplanes H that intersect V properly, the ones such that $H \cap W_i = H \cap W_j$, with $i \neq j$, form a proper Zariski-closed subset. By Bertini's theorem, it is also true that the ones such that $H \cap V$ is not smooth and absolutely irreducible, and similarly the ones such that $H \cap W_i$ is not smooth and absolutely irreducible, form proper Zariski-closed sets.

Therefore, we can find an hyperplane H represented by the equation $x = 0$ such that $x^{-1}(\alpha) \cap W_i$ and $x^{-1}(\alpha) \cap V$ are all smooth and distinct absolutely irreducible varieties for almost all $\alpha \in \overline{k}$. But then the restrictions of $w_1, \ldots, w_n$ to $x^{-1}(\alpha) \cap V$ are such that $(o_{H \cap W_i}(w_j))_{i,j}$ is still a diagonal matrix, which implies that their divisors are still $\mathbb{Q}$-linearly independent, hence the restrictions are multiplicatively independent over $\overline{k}^*$. ⊣

We shall use the above statements to reduce to the case of curves. For curves, we adopt a different strategy.

PROPOSITION 3.4. *Let $\mathcal{C} \subset \overline{\mathbb{Q}}^n \times (\overline{\mathbb{Q}}^*)^n$ be an irreducible curve over $\overline{\mathbb{Q}}$ and $L < \overline{\mathbb{Q}}$, $M < \overline{\mathbb{Q}}^*$ be two finite-rank subgroups. If $\mathcal{C}$ is absolutely multiplicatively free, and additively free over L, then there is a point $(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) \in \mathcal{C}$ such that $\alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent from L, and such that $\beta_1, \ldots, \beta_n$ are multiplicatively independent from M.*

PROOF. Without loss of generality, we may assume that $\mathcal{C}$ is absolutely irreducible. Let $z_1, \ldots, z_n$ and $w_1, \ldots, w_n$ be the coordinate functions of $\overline{\mathbb{Q}}^n \times (\overline{\mathbb{Q}}^*)^n$ restricted to $\mathcal{C}$ and $a_1, \ldots, a_m$ be a finite set of divisible generators of M. Let k be a number field defining $\mathcal{C}$ and containing $a_1, \ldots, a_m$.

Using the notation of [6], we define

- $\mathcal{C}(d, h)$ the set of all points of $\mathcal{C}$ of degree at most d and height at most h;
- $\mathcal{E}(d, h)$ the set of all points of $\mathcal{C}$ of degree at most d and height at most h such that the specialisations of $w_1, \ldots, w_n$ are multiplicatively dependent on M;
- $\omega(S)$, for a finite set S, the minimum degree of an hypersurface containing all the points of S.

Applying the main result of [6, Section 5] to $\mathbb{G}_m(k(\mathcal{C}))$ and to the group generated by $w_1, \ldots, w_n, a_1, \ldots, a_n$, we find a function $c_1(d)$ and a number k such that $\omega(\mathcal{E}(d, h)) \leq c_1(d)h^k$, while we also find a c_2 such that $\omega(\mathcal{C}(d, h)) \geq \exp(c_2(d)h)$ when d is at least the degree of $\mathcal{C}$.[1]

Now using Corollary 3.2 on $\mathcal{C}$ and L we obtain a number d_1 such that when $[k(P) : k] > d_1$ the specialisations of $z_1, \ldots, z_n$ at P are $\mathbb{Q}$-linearly independent from L. We may choose d_1 larger than the degree of $\mathcal{C}$. Now let d_2, h_1, h_2 be numbers such that

$$\omega(\mathcal{C}(d_2, h_2)) \geq \exp(c_2(d_2)h_2) > \omega(\mathcal{C}(d_1, h_1)) + c_1(d_2)h_2^k \geq$$
$$\geq \omega(\mathcal{C}(d_1, h_1)) + \omega(\mathcal{E}(d_2, h_2)).$$

[1] The statement of [6] is actually that $\omega(\mathcal{C}(d, h)) \geq \exp(ch)$ when $d = \deg(\mathcal{C})$. However, the proof only requires that there is a dominant map $\pi : \mathcal{C} \to \mathbb{P}^m$ of degree d with $m = \dim \mathcal{C}$. Such maps exist, for example, for any multiple of $\deg(\mathcal{C})$, as we can compose π with dominant self maps of $\mathbb{P}^m$ which exist for any positive degree.

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

Then there must be a point P of degree strictly greater than d_1 such that the specialisations of $w_1, \dots, w_n$ at P are multiplicatively independent from $a_1, \dots, a_n$, hence from M. Since its degree is greater than d_1, the specialisations of $z_1, \dots, z_n$ are also $\mathbb{Q}$-linearly independent from L, as desired. ⊣

Putting the statements together, we can prove the general version we need for step (3).

PROPOSITION 3.5. *Let $V \subset \overline{\mathbb{Q}}^n \times (\overline{\mathbb{Q}}^*)^n$ be an irreducible absolutely free variety over $\overline{\mathbb{Q}}$, and let $L < \overline{\mathbb{Q}}$, $M < \overline{\mathbb{Q}}^*$ be two finite-rank subgroups. There is a point $(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n) \in V$ such that $\alpha_1, \dots, \alpha_n$ are $\mathbb{Q}$-linearly independent from L and $\beta_1, \dots, \beta_n$ are multiplicatively independent from M.*

PROOF. We prove the theorem by induction on $m = \dim(V)$. Our inductive hypothesis is that if V is absolutely irreducible, absolutely multiplicatively free, and additively free over L, then it contains a point as in the conclusion. The base case $m = 1$ is covered by Proposition 3.4. Let k be a number field defining V.

Let us suppose that $m > 1$, and that we have proven the theorem for all the varieties of dimension $m - 1$. Let $z_1, \dots, z_n$ and $w_1, \dots, w_n$ be the coordinate functions of $\overline{\mathbb{Q}}^n \times (\overline{\mathbb{Q}}^*)^n$ restricted to V. Moreover, let $\{b_1, \dots, b_m\}$ be a $\mathbb{Q}$-basis of the vector space generated by L. By Proposition 3.3, there is a nonconstant function x such that for almost all $\alpha \in \overline{k}$ we have

(1) $V_\alpha := V \cap x^{-1}(\alpha)$ is absolutely irreducible;
(2) $\dim(V_\alpha) = m - 1$;
(3) the functions $\{w_1, \dots, w_n\}$ restricted to V_α are multiplicatively independent over $\overline{\mathbb{Q}}^*$.

Now take any transcendence base of $k(V)$ of the form $X \cup \{x\}$. Then V can be seen also as an absolutely irreducible curve over $k(X)$, and x is a nonconstant function on it.

By applying Proposition 3.1 to V seen as a curve over $K := k(X)$, as soon as $[k(\alpha) : k]$ is sufficiently large, the functions $\{z_1, \dots, z_n, b_1, \dots, b_m\}$ are $\mathbb{Q}$-linearly independent when restricted to V_α. Therefore V_α satisfies the same properties of V, and by inductive hypothesis, it contains a point P such that the specialisations of $z_1, \dots, z_1$ at P are $\mathbb{Q}$-linearly independent from L and the specialisations of $w_1, \dots, w_n$ at P are multiplicatively independent from M, as desired. ⊣

REMARK 3.6. The above proof relies on the results exposed in [6]. These results depend on the Northcott Property of number fields. Using other techniques of Diophantine geometry it is possible to obtain a similar result for other finitely generated fields without the same quantitative statements, but still strong enough to obtain again Proposition 3.4. This implies that this construction works also on all algebraically closed fields of characteristic 0, and in particular of any fixed transcendence degree.

REFERENCES

[1] TAPANI HYTTINEN, *Random logarithm and homogeneity*, ***Logic and Its Applications*** (Andreas Blass and Yi Zhang, editors), Contemporary Mathematics, pp. 137–166, American Mathematical Society, Providence, RI, 2005.

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press

[2] Jonathan Kirby, *A Note on the Axioms for Zilber's Pseudo-Exponential Fields*. ***Notre Dame Journal of Formal Logic***, vol. 54, no. 3–4, pp. 509–520, 2013.

[3] Jonathan Kirby, *Finitely presented exponential fields*. ***Algebra & Number Theory***, vol. 7, no. 4, pp. 943–980, 2013.

[4] Vincenzo Mantova, *Involutions on Zilber fields*, September 2011. `http://arxiv.org/abs/1109.6155` `arXiv:1109.6155`.

[5] David Marker, *A remark on Zilber's pseudoexponentiation*. ***Journal of Symbolic Logic***, vol. 71, no. 3, pp. 791–798, 2006.

[6] David W. Masser, *Specialisations of finitely generated subgroups of abelian varieties.* ***Transactions of the American Mathematical Society***, vol. 311, no. 1, pp. 413–424, 1989.

[7] Boris Zilber, *Pseudo-exponentiation on algebraically closed fields of characteristic zero*. ***Annals of Pure and Applied Logic***, vol. 132, no. 1, pp. 67–95, 2005.

DIVISION OF MATHEMATICS, SCHOOL OF SCIENCE AND TECHNOLOGY
UNIVERSITY OF CAMERINO
VIA MADONNA DELLE CARCERI 9, 62032, CAMERINO (MC)
ITALY
E-mail: vincenzo.mantova@unicam.it

https://doi.org/10.1017/jsl.2014.41 Published online by Cambridge University Press