

*On the decidability of the real field with a
generic power function*

Jones, Gareth and Servi, Tamara

2010

MIMS EPrint: **2011.55**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: <http://eprints.maths.manchester.ac.uk/>

And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

On the decidability of the real field with a generic power function

Gareth Jones ^{*} Tamara Servi [†]

Abstract

We show that the theory of the real field with a generic real power function is decidable, relative to an oracle for the rational cut of the exponent of the power function. We show the existence of generic computable real numbers, hence providing an example of a decidable o-minimal proper expansion of the real field by an analytic function.

Key words: real power functions; decidability; o-minimality.

MSC2000: Primary 03C64; 03B25

1 Introduction

In the 1930's, Alfred Tarski proved that the theory of the real ordered field $\overline{\mathbb{R}} := \langle \mathbb{R}; +, -, \cdot, 0, 1, < \rangle$ is decidable. Subsequently, he asked whether his result could be extended to the theory of the real exponential field $\mathbb{R}_{\text{exp}} := \langle \overline{\mathbb{R}}, \text{exp} \rangle$. This question remains open and has links with some questions in transcendence theory. For example, given $m, n \in \mathbb{Z}$, a decision procedure for \mathbb{R}_{exp} would tell us if $me^e - n = 0$ holds in \mathbb{R}_{exp} , and it is, at present, not known whether e^e is irrational. Similarly, it is not known if e, e^e and e^{e^e} are algebraically independent and a decision procedure would have to determine, given a polynomial $p \in \mathbb{Z}[X, Y, Z]$, if $p(e, e^e, e^{e^e}) = 0$. Now, there is a famous conjecture due to Schanuel which, roughly, asserts that no such algebraic relations hold between values of the exponential function unless they are forced by the addition law (for the precise statement, and much more information, see [Waldschmidt00]). Building on Wilkie's model

^{*}School of Mathematics, University of Manchester, Oxford Road, Manchester M13 9PL, UK; Gareth.Jones-3@manchester.ac.uk.

[†](*Corresponding author*) Centro de Matemática e Aplicações Fundamentais, Av. Prof. Gama Pinto 2, 1649-003 Lisboa, Portugal; tamara.servi@googlemail.com.

completeness result for \mathbb{R}_{exp} [Wilkie96], Macintyre and Wilkie show that if Schanuel's conjecture is true then \mathbb{R}_{exp} is decidable [MW96]. Unfortunately, Schanuel's conjecture is thought to be out of reach. Indeed, even the simple cases mentioned above are major problems in transcendence theory.

Given this, it seems reasonable to look for any decidable expansion of the real field by some transcendental analytic function. In this paper, we give an example of such an expansion.

1.1 Theorem. *Let α be a real number, and assume that α is not 0-definable in \mathbb{R}_{exp} . Let x^α be the function from \mathbb{R} to \mathbb{R} which sends positive x to $\exp(\alpha \log x)$ and is 0 elsewhere. Then the theory of the structure $\mathbb{R}^\alpha := \langle \mathbb{R}, \alpha, x^\alpha \rangle$ is decidable, relative to an oracle for the cut of α in \mathbb{Q} .*

Theorem 1.1 gives some evidence for a positive answer to Tarski's original question, as it proves the decidability of a fragment of the theory of the expansion of \mathbb{R}_{exp} by a symbol for α .

The key to proving this is a recent Schanuel condition for certain power functions, which is due to Bays, Kirby and Wilkie (see [BKW08] and Section 3). Given their result, the proof proceeds as in [MW96], using a theorem of Miller's [Miller94] in place of the model completeness of \mathbb{R}_{exp} . In the final section, we prove the existence of a computable number α which is not 0-definable in \mathbb{R}_{exp} , and so obtain a theory which is decidable without any reference to an oracle. Unfortunately, this number is constructed by a diagonalisation procedure, so is rather far from being explicit.

As this paper was being written, we found out that, independently and by quite different methods, Dan Miller has also shown the existence of a decidable proper o-minimal expansion of the real field.

In the proof of Theorem 1.1 we show that, if α is *generic* (i.e. α is not 0-definable in \mathbb{R}_{exp}), then the theory T defined below is complete and hence provides an (explicit) axiomatization for $\text{Th}(\mathbb{R}^\alpha)$.

1.2 Definition. Let T be the subtheory of $\text{Th}(\mathbb{R}^\alpha)$ axiomatized by the following axiom schemes:

- [OF] Axioms of ordered field;
- [DCB] Axioms of definably complete Baire structure;
- [DE(x^α)] The differential equation $\forall x > 0 x(x^\alpha)' = \alpha x^\alpha$, $\forall x \leq 0 x^\alpha = 0$ and $(1)^\alpha = 1$;
- [L] Axioms ensuring that certain unary functions, definable using only the restriction of x^α to the interval $[1, 2]$, have rational exponents at $+\infty$;

- [CUT(α)] A set of sentences implying that the constant interpreted by α in \mathbb{R}^α , satisfies the Dedekind cut of α over \mathbb{Q} .

Notice that T is recursive, relative to [CUT(α)].

Concerning [DCB], definably complete Baire structures were introduced in [FS09] and are shown to admit a recursive axiomatization; together with schemes [OF] and [DE(x^α)], the scheme [DCB] ensures the o-minimality of the models (see [FS09, Cor. 8.2]).

The scheme [L] will be discussed in Section 2.

2 Effective model-completeness in the restricted case

In this section we consider a restricted power function

$$x_{\text{res}}^\alpha := \begin{cases} x^\alpha & \text{if } x \in [1, 2] \\ 0 & \text{otherwise} \end{cases}$$

for some real number α , and the associated expansion of the real field $\mathbb{R}_{\text{res}}^\alpha := \langle \overline{\mathbb{R}}, \alpha, x_{\text{res}}^\alpha \rangle$; let L be its underlying language. We show the effective model-completeness of $\text{Th}(\mathbb{R}_{\text{res}}^\alpha)$, i.e. we exhibit a recursively axiomatized subtheory T_{res} , which is model-complete.

2.1 Definition. Given an L -structure K , expanding a field, and n, r in \mathbb{N} , let $\bar{x} = (x_1, \dots, x_n)$ range over K^n and $\bar{y} = (y_1, \dots, y_r)$ range over the box $(1, 2)^r$, interpreted in K . We refer to the variables \bar{x} and \bar{y} as *unbounded* and *bounded* respectively. Let $M_{n,r}^{\text{res}}(K)$ be the ring of functions on $K^n \times (1, 2)^r$ which can be expressed as polynomials (with coefficients in K) in the variables $\bar{x}, \bar{y}, \bar{y}^{-1} = (y_1^{-1}, \dots, y_r^{-1}), \bar{y}^\alpha = (y_1^\alpha, \dots, y_r^\alpha)$. We call such functions *restricted power polynomials*.

We now state Axiom Scheme [L] precisely.

2.2 Definition. Let τ be a recursive function taking triples of natural numbers to finite sets of rational numbers. Let K be an L -structure. We say that K satisfies axiom scheme [L $_\tau$] if, given $a \in K$; $f_1, \dots, f_{n+r-1}, g \in M_{n,r}^{\text{res}}(K)$ of total degree at most m ; $\phi = (\phi_2, \dots, \phi_{n+r}) : (a, +\infty) \rightarrow K^{n+r-1}$ definable continuous functions such that

$$\text{for } i = n+1, \dots, n+r \quad \text{Im } \phi_i \subseteq (1, 2),$$

$$\text{for } i = 1, \dots, n+r-1 \quad \forall t > a \quad f_i(t, \phi_2(t), \dots, \phi_{n+r}(t)) = 0,$$

$$\text{for } t > a \quad \det \frac{\partial(f_1, \dots, f_{n+r-1})}{\partial(x_2, \dots, x_n, y_1, \dots, y_r)}(t, \phi(t)) \neq 0,$$

either $g(t, \phi(t))$ is identically zero or else there exists $q \in \tau(n, r, m)$ such that $\lim_{t \rightarrow \infty} t^q g(t, \phi(t))$ is finite and nonzero.

Axiom scheme $[\mathbf{L}_\tau]$ asserts that, if C is a regular restricted power polynomial curve and g is an restricted power polynomial function, then $g \upharpoonright C$ has rational exponent at $+\infty$. Moreover, the recursive function τ finds such an exponent (up to finitely many choices) independently of the parameters defining g and C .

Notice that every $\mathbb{R}_{\text{res}}^\alpha$ -definable unary function has a rational exponent by [Dries86]; what we need to prove is that, in the situation described in axiom scheme $[\mathbf{L}_\tau]$, we can actually find such exponents recursively.

2.3 Theorem. *There exists a recursive function τ as above such that the axiom scheme $[\mathbf{L}_\tau]$ is true in $\mathbb{R}_{\text{res}}^\alpha$.*

Before proving the above theorem, we shall explain how the axiom scheme $[\mathbf{L}]$ is used.

2.4 Definition. Let T_{res} be the L -theory axiomatized by the following schemes:

- [OF] Axioms of ordered field;
- [DCB_{res}] Axioms of definably complete Baire structure;
- [DE(x_{res}^α)] The differential equation $\forall x \in [1, 2] \ x(x^\alpha)' = \alpha x^\alpha$, $\forall x \notin [1, 2], \ x^\alpha = 0$ and $(1)^\alpha = 1$.
- [L] The axiom scheme $[\mathbf{L}_\tau]$, where τ is as in Theorem 2.3.

2.5 Theorem. *T_{res} is model-complete.*

Proof. The reader can check that the proof of [Wilkie96, First Main Theorem] goes through for the theory T_{res} . Axiom scheme $[\mathbf{L}]$ is exactly what is required to make the proof in Section 8 work. See also [MW96, pag.448]. \square

In order to prove Theorem 2.3, we first show that, by a change of coordinates, we can reduce to proving the following statement, where the roles of zero and $+\infty$ are interchanged, and we only consider the function $g = x_n$.

2.6 Theorem. *There is a recursive function τ' taking triples of natural numbers to finite sets of rational numbers with the following property: given $n, r, m \in \mathbb{N}$, τ' returns $\tau'(n, r, m)$ such that, given $\varepsilon \in \mathbb{R}^+$; $g_1, \dots, g_{n+r-1} \in M_{n,r}^{\text{res}}(\mathbb{R})$ of total degree at most m ; $\psi = (\psi_2, \dots, \psi_{n+r}) : (0, \varepsilon) \rightarrow \mathbb{R}^{n+r-1}$ definable continuous functions such that*

$$\text{for } i = n + 1, \dots, n + r \quad \text{Im } \psi_i \subseteq (1, 2),$$

$$\begin{aligned}
& \text{for } i = 2, \dots, n \quad \lim_{s \rightarrow 0^+} \psi_i(s) = 0 \text{ and} \\
& \text{for } i = n + 1, \dots, n + r \quad \lim_{s \rightarrow 0^+} \psi_i(s) = 1, \\
& \text{for } i = 1, \dots, n + r - 1 \text{ and } s \in (0, \varepsilon) \quad g_i(s, \psi_2(s), \dots, \psi_{n+r}(s)) = 0, \\
& \text{for } s \in (0, \varepsilon), \det \frac{\partial(g_1, \dots, g_{n+r-1})}{\partial(x_2, \dots, x_n, y_1, \dots, y_r)}(s, \psi(s)) \neq 0,
\end{aligned}$$

either ψ_n is identically zero, or else there exists $q \in \tau'(n, r, m)$ such that $\lim_{s \rightarrow 0^+} s^q \psi_n(s)$ is finite and nonzero.

Here are the details of the proof that Theorem 2.6 implies Theorem 2.3.

Proof. By o-minimality, all definable unary functions have a limit in $\mathbb{R} \cup \{\pm\infty\}$. We may assume that $\lim_{t \rightarrow +\infty} g(t, \phi(t))$ is either zero or $\pm\infty$, otherwise we could take $q = 0$.

Let

$$\begin{aligned}
S &:= \{j \in \mathbb{N} : 2 \leq j \leq n \text{ and } \lim_{t \rightarrow +\infty} \phi_j(t) = \pm\infty\}, \\
S' &:= \{j \in \mathbb{N} : 2 \leq j \leq n \text{ and } \lim_{t \rightarrow +\infty} \phi_j(t) = r_j \in \mathbb{R}\}, \\
K &:= \{n+i \in \mathbb{N} : 1 \leq i \leq r, \phi_{n+i} \text{ is eventually decreasing and } \lim_{t \rightarrow +\infty} \phi_{n+i}(t) = r_{n+i} \in [1, 2]\}, \\
K' &:= \{n+i \in \mathbb{N} : 1 \leq i \leq r, \phi_{n+i} \text{ is eventually increasing and } \lim_{t \rightarrow +\infty} \phi_{n+i}(t) = r_{n+i} \in [1, 2]\}.
\end{aligned}$$

Let z_L be a new variable, i.e. $z_L \notin (\bar{x}, \bar{y})$.

Let

$$\begin{aligned}
x_1^* &= x_1^{-1} \\
x_i^* &= \begin{cases} \frac{1}{x_i} & \text{if } i \in S \\ x_i + r_i & \text{if } i \in S' \end{cases} \\
z_L^* &= \begin{cases} \frac{1}{z_L} & \text{if } \lim_{t \rightarrow +\infty} g(t, \phi(t)) = \pm\infty \\ z_L & \text{if } \lim_{t \rightarrow +\infty} g(t, \phi(t)) = 0 \end{cases} \\
y_i^* &= \begin{cases} r_{n+i} y_i & \text{if } n+i \in K \\ \frac{r_{n+i}}{y_i} & \text{if } n+i \in K' \end{cases}
\end{aligned}$$

Let $\rho_1, \dots, \rho_{n+r}$ be polynomials such that $f_i(\bar{x}, \bar{y}) = \rho_i(\bar{x}, \bar{y}, \bar{y}^{-1}, \bar{y}^\alpha)$, for $i = 1, \dots, n + r - 1$, and $g(\bar{x}, \bar{y}) = \rho_{n+r}(\bar{x}, \bar{y}, \bar{y}^{-1}, \bar{y}^\alpha)$. Define

$$h_i(\bar{x}, \bar{y}) = \rho_i(\bar{x}^*, \bar{y}^*, (\bar{y}^*)^{-1}, (\bar{y}^*)^\alpha), \quad A(\bar{x}, \bar{y}) = x_1^m \prod_{j \in S, n+l \in K'} x_j^m y_l^{m\alpha},$$

$$g_i(\bar{x}, \bar{y}) = A(\bar{x}, \bar{y}) h_i(\bar{x}, \bar{y}) \quad (i = 1, \dots, n+r), \quad g_L(\bar{x}, z_L, \bar{y}) = z_L (A(\bar{x}, \bar{y}) z_L^* - g_{n+r}(\bar{x}, \bar{y})).$$

Note that $g_i \in M_{n,r}^{\text{res}}(\mathbb{R})$ and $g_L \in M_{n+1,r}^{\text{res}}(\mathbb{R})$.

Consider the system \mathcal{S} of $n+r$ equations in $n+r+1$ variables given by $g_L = g_1 = \dots = g_{n+r-1} = 0$.

We now define $\psi_i(s)$ such that $\psi_i^*(s) = \phi_i(s^{-1})$. We set $t = s^{-1}$.

Let

$$\psi_i(s) = \begin{cases} \frac{1}{\phi_i(t)} & \text{if } i \in S \\ \phi_i(t) - r_i & \text{if } i \in S' \end{cases}$$

$$\psi_L(s) = \begin{cases} \frac{1}{g(t, \phi(t))} & \text{if } \lim_{t \rightarrow +\infty} g(t, \phi(t)) = \pm\infty \\ g(t, \phi(t)) & \text{if } \lim_{t \rightarrow +\infty} g(t, \phi(t)) = 0 \end{cases}$$

$$\psi_j(s) = \begin{cases} \frac{\phi_j(t)}{r_j} & \text{if } j \in K \\ \frac{r_j}{\phi_j(t)} & \text{if } j \in K' \end{cases}$$

Let $\psi(s) = (\psi_2(s), \dots, \psi_n(s), \psi_{n+1}(s), \dots, \psi_{n+r}(s))$ and $\Psi(s) = (\psi_2(s), \dots, \psi_n(s), \psi_L(s), \psi_{n+1}(s), \dots, \psi_{n+r}(s))$.

Notice that $g_i(s, \psi(s)) = A(t, \phi(t))f_i(t, \phi(t))$.

Arguing as in [MW96, pag.452], we can show that $(s, \Psi(s))$ is a nonsingular solution of the system \mathcal{S} for every $s \in (0, \varepsilon)$, for some ε . Moreover, the other hypotheses of 2.6 are satisfied. Hence we can find $q \in \tau'(n+1, r, 2m)$ such that $\lim_{s \rightarrow 0^+} s^q \psi_L(s)$ is finite and nonzero. Now clearly $g(t, \phi(t))$ (as in Definition 2.2) has exponent $\pm q$. □

To prove Theorem 2.6, we need the following lemma.

2.7 Lemma. *Let $D_0 = \{z \in \mathbb{C} : |z| < 1\}$ and $D_1 = \{z \in \mathbb{C} : |z - 1| < 1\}$ and $\mathcal{D} := D_0^n \times D_1^r$. There exists a recursive function $\mu : \mathbb{N}^2 \rightarrow \mathbb{N}$ such that if $h_1(\bar{z}), \dots, h_{n+r}(\bar{z}) : \mathcal{D} \rightarrow \mathbb{C}$ can be expressed as polynomials in z_i ($i = 1, \dots, n+r$) and z_i^α ($i = n+1, \dots, n+r$) of total degree $\leq m$, then the system $h_1 = \dots = h_{n+r} = 0$ has at most $\mu(n+r, m)$ nonsingular solutions in \mathcal{D} .*

Proof. The proof proceeds as in [MW96, Lemma 3.2], using Khovanskii theory [Khovanskii91] and the fact that the real and imaginary parts of the functions h_j are Pfaffian maps with respect to a Pfaffian chain obtained by composition of the functions $1/x, \sqrt{x}, \arctan x, \exp x, \log x$ and $\sin x, \cos x$ restricted to a bounded interval. □

Proof of Theorem 2.6. Let μ be as in Lemma 2.7. We claim that there exist $c \in \mathbb{Z}, d \in \mathbb{N}^+$ such that $d \leq \mu(n+r-1, m)$ and $\lim_{s \rightarrow 0^+} s^{c/d} \psi_n(s)$ is finite and nonzero.

The proof of the claim can be taken word by word from [MW96, pp. 454–455]. We recall the main ideas. Since every ψ_i has a Puiseux expansion at zero, we can choose the smallest d such that for all i there is an analytic function θ_i and an $\varepsilon > 0$ such that for $s \in (0, \varepsilon)$, $\psi_i(s) = \theta_i(s^{1/d})$. The denominator of the exponent of ψ_n is smaller than d , so it's enough to bound d . To do this, let $g = (g_1, \dots, g_{n+r-1})$ and $\theta = (\theta_1, \dots, \theta_{n+r})$. Consider the change of variable $t = s^{1/d}$. Choosing ε to be sufficiently small, we may assume that $g(t^d, \theta(t)) = 0$ for all $t \in (0, \varepsilon)$. We refer to the notation of the statement of the previous lemma. Let $\hat{\theta}$ be the analytic continuation of θ on the domain $D = \{z \in \mathbb{C} : |z| < \varepsilon\}$ and suppose that ε was chosen small enough to guarantee that $\hat{\theta}_{n+i}(D) \subseteq D_1$ for $i = 1, \dots, r$; let \hat{g} be the analytic continuation of g on the domain \mathcal{D} . Then for all $u \in D$, $\hat{g}(u^d, \hat{\theta}(u)) = 0$. Fix $u_0 \in D$ and consider the following function.

$$h : \begin{array}{ccc} D_0^{n-1} \times D_1^r & \rightarrow & \mathbb{C}^{n+r-1} \\ \bar{z} & \mapsto & \hat{g}(u_0^d, \bar{z}) \end{array}$$

obtained from \hat{g} by fixing the first variable. By Lemma 2.7, the system $h = 0$ has at most $\mu(n+r-1, m)$ regular solutions in \mathcal{D} .

Let $\omega_1, \dots, \omega_d$ be distinct d^{th} -roots of unity and let $u_i = u_0 \omega_i$ for $i = 1, \dots, d$. We can choose u_0 such that $\hat{\theta}(u_1), \dots, \hat{\theta}(u_d)$ are distinct (see [MW96, pag. 455]). Note that $\hat{\theta}(u_i)$ are d distinct regular solutions of $h = 0$, since $h(\hat{\theta}(u_i)) = \hat{g}(u_0^d, \hat{\theta}(u_i)) = \hat{g}(u_i^d, \hat{\theta}(u_i)) = 0$ (an easy calculation shows the regularity). This concludes the proof of the claim.

Now we can conclude as in [MW96, pag. 456] and observe that, after possibly replacing x_n with $-x_n$ in g , ψ_n is a bijection from $(0, \varepsilon)$ to some interval $(0, \varepsilon')$. Define $\eta_n = \psi_n^{-1}$ and $\eta_i = \psi_i \circ \psi_n^{-1}$ for $i \neq n$; after swapping x_n and x_1 in g , we obtain that $(s, \eta(s))$ satisfies the hypotheses of the claim we just proved. Hence there exist $c' \in \mathbb{Z}, d' \in \mathbb{N}^+$ such that $d' \leq \mu(n+r-1, m)$ and $\lim_{s \rightarrow 0^+} s^{c'/d'} \eta_n(s)$ is finite and nonzero. It follows that it must be $cc' = dd'$, so that we can set $\tau'(n, r, m) = \{(u, v) \in \mathbb{Z} : |u|, |v| \leq \mu(n+r-1, m)\}$ \square

3 Reduction to and decidability of the existential fragment

In this section we first show that, in order to prove the decidability of $\text{Th}(\mathbb{R}^\alpha)$, it is enough to recursively axiomatize its existential fragment $\exists \text{Th}(\mathbb{R}^\alpha)$. Subsequently, we proceed to prove that, if α is generic, then T axiomatizes $\exists \text{Th}(\mathbb{R}^\alpha)$, thus concluding the proof of Theorem 1.1.

3.1 Proposition.

$$T \cup \exists \text{Th}(\mathbb{R}^\alpha) \vdash \text{Th}(\mathbb{R}^\alpha).$$

Proof. The complete theory $\text{Th}(\mathbb{R}_{\text{res}}^\alpha)$ of $\mathbb{R}_{\text{res}}^\alpha$ is model complete [Wilkie96] and o-minimal. It is also of rational type (see [Miller94] and [Wilkie96]). Since it is o-minimal, $\text{Th}(\mathbb{R}_{\text{res}}^\alpha)$ has definable Skolem functions, hence we can expand the original language to a language L' which contains a symbol for every Skolem function. Take the L' -expansion by definition $\mathbb{R}_{\text{res}}^\alpha(L')$ and its complete theory $T_{\text{res}}^\alpha(L')$, which admits universal axiomatization. Notice that $T_{\text{res}}^\alpha(L')$ is still of rational type. Let $T^\alpha(L')$ be the theory of the L' -expansion $\mathbb{R}^\alpha(L')$ of \mathbb{R}^α (where the symbols of L' are interpreted as the Skolem functions of the restricted power function, as above). [Miller94, 3.2] implies that $T^\alpha(L')$ is axiomatized by $T_{\text{res}}^\alpha(L')$ and a recursive scheme P of universal axioms à la Ressayre. It follows that $\text{Th}(\mathbb{R}_{\text{res}}^\alpha) \cup P \vdash \text{Th}(\mathbb{R}^\alpha)$.

By [FS09], T is an o-minimal subtheory of $\text{Th}(\mathbb{R}^\alpha)$, which proves the axioms in the scheme P (one only needs to use the uniqueness of solutions of the differential equation defining a power function). By model completeness of T_{res} , we have that $\text{Th}(\mathbb{R}_{\text{res}}^\alpha)$ is axiomatized by T_{res} and the existential fragment $\exists \text{Th}(\mathbb{R}_{\text{res}}^\alpha)$ of $\text{Th}(\mathbb{R}_{\text{res}}^\alpha)$. Putting everything together, we obtain that $T \cup \exists \text{Th}(\mathbb{R}_{\text{res}}^\alpha) \vdash \text{Th}(\mathbb{R}^\alpha)$, hence, in particular, the conclusion. \square

3.2 Definition. Let $K \models T$ and R be a subring of K ; Let $M_n(R)$ be the ring of polynomials in the variables $x_1, \dots, x_n, x_1^\alpha, \dots, x_n^\alpha$, with coefficients in R .

The following lemma, the proof of which is easy, reduces the existential formulas we must study to a simple form.

3.3 Lemma. *Every existential sentence is K -equivalent to a sentence of the form $\exists \bar{x} g(\bar{x}) = 0$, for some $n \in \mathbb{N}$ and $g \in M_n(\mathbb{Z}[\alpha])$.*

We will first discuss the existence of regular zeroes (Theorem 3.7) and subsequently the general case (Theorem 3.11).

3.4 Definition. For $\bar{x} = (x_1, \dots, x_n) \in K^n$ we denote by $\|\bar{x}\| := \max |x_i|$ the norm of \bar{x} . For a definable C^1 map $F : K^n \rightarrow K^n$, the maps F' and F'' (and their operator norms) are defined in the obvious way (see [Servi08, Remark 1.3.2]). Let $JF(\bar{x}) := \det F'(\bar{x})$ and let $V^{\text{reg}}(F) := \{\bar{x} \in K^n : F(\bar{x}) = 0 \wedge JF(\bar{x}) \neq 0\}$.

Let $B(\bar{x}_0, r) = \{\bar{x} \in K^n : \|\bar{x} - \bar{x}_0\| < r\}$ be the open ball centered in \bar{x}_0 and with radius r .

3.5 Lemma. *There is an effective procedure which, given $n, N \in \mathbb{N}$ and $F = (f_1, \dots, f_n) \in (M_n(\mathbb{Z}[\alpha]))^n$, produces $\theta = \theta(n, N, F) \in \mathbb{N}$ such that:*

$$T \models \forall \bar{x}_0 (\|\bar{x}_0\| < N, \|F(\bar{x}_0)\| < \theta^{-1}, |JF(\bar{x}_0)| > N^{-1} \Rightarrow \\ \exists \bar{x} \in B(\bar{x}_0, N^{-1}) \cap V^{\text{reg}}(F)).$$

Proof. By [Servi08, Theorem 1.4.1] we have that the following holds in every model K of T . Let $a_0, a_1, a_2 \geq 1$ and $m = (4n^3 a_0^3 a_1 a_2)^{-1}$, $r = (2n^3 a_0^2 a_1 a_2)^{-1}$. For all $\bar{x}_0 \in K^n$,

If $\|F(\bar{x}_0)\| < m$ and $\forall \bar{y} \in B(\bar{x}_0, r) |F'(\bar{y})^{-1}| < a_0$ and $|F'(\bar{y})| < a_1$ and $|F''(\bar{y})| < a_2$,

Then $\exists \bar{x} F(\bar{x}) = 0$ and $\bar{x} \in B(\bar{x}_0, r)$.

Notice that, if $h \in M_n(\mathbb{Z}[\alpha])$, then in K we can effectively bound the norm of $h(\bar{x})$ for $\bar{x} \in B(0, N+1)$. For example, if $\alpha > 0$ and $h(\bar{x}) = \sum_{|I|, |J| \leq k} b_{IJ} \bar{x}^I (\bar{x}^\alpha)^J$ (where I, J are multi-indices of length n), then we can use [CUT(α)] to find $M \in \mathbb{N}$ such that $\alpha < M$ and obtain

$$|h(\bar{x})| \leq \sum |b_{IJ}| \|\bar{x}\|^{|I|} \|x\|^{|J|M} \leq k^2 \max |b_{IJ}| (N+1)^{k(M+1)}.$$

The linear map $F'(\bar{x})$ can be represented as the $n \times n$ matrix A , whose entries are $\frac{\partial f_i}{\partial x_j}$. If A is invertible, then there is an $n \times n$ matrix $\text{ad}A$ such that $A^{-1} = \frac{\text{ad}A}{JF(\bar{x})}$. The entries c_{ij} of $\text{ad}A$ are $(-1)^{i+j} \det M_{ji}$, where M_{ij} is the $(n-1) \times (n-1)$ minor of A obtained from A by eliminating the i -th row and the j -th column. In particular, the entries of $\text{ad}A$ are polynomials in the entries of A .

Choose $\theta_0 \in \mathbb{N}$ such that the following holds:

$$\forall \bar{x} \in B(0, N+1) |F'(\bar{x})|, |F''(\bar{x})|, \max_{i,j} |c_{ij}(\bar{x})|, \max_i |\partial JF / \partial x_i(\bar{x})| < \theta_0.$$

Let $a_0 = 2nN\theta_0$ and $a_1 = a_2 = \theta_0$. Let $m = (4n^3 a_0^3 a_1 a_2)^{-1} = (32n^6 N^3 \theta_0^5)^{-1}$ and $r = (2n^3 a_0^2 a_1 a_2)^{-1} = (8n^5 N^2 \theta_0^2)^{-1}$. Finally put $\theta = m^{-1}$.

We claim that the hypotheses of the above statement are satisfied with this choice of a_0, a_1, a_2 . The only nontrivial thing to check is that for all $\bar{y} \in B(\bar{x}_0, r) |F'(\bar{y})^{-1}| < a_0$. We first observe that for all $\bar{y} \in B(\bar{x}_0, r)$, $JF(\bar{y}) \neq 0$. In fact from the mean value theorem it follows that $|JF(\bar{y})| \geq |JF(\bar{x}_0)| - \|\bar{y} - \bar{x}_0\| n \max_{\bar{x} \in B(0, N+1)} \max_i |\partial JF / \partial x_i(\bar{x})|$. Hence it is enough to check that $N^{-1} - rn\theta_0 > (2N)^{-1}$. Now,

$$|F'(\bar{y})^{-1}| \leq |JF(\bar{y})|^{-1} n \max_{i,j} |c_{ij}(\bar{y})| < 2Nn\theta_0 = a_0.$$

Hence [Servi08, Theorem 1.4.1] applies and gives us the required conclusion. \square

3.6 Lemma. *Let $h \in M_n(\mathbb{Z}[\alpha])$, $\bar{q} \in \mathbb{Q}^n$ and suppose that $\mathbb{R}^\alpha \models h(\bar{q}) < 0$. Then $T \vdash h(\bar{q}) < 0$.*

Proof. Using [CUT(α)] and the Taylor expansion of x^α (which, by axiom [DE(x^α)], coincides with the Taylor expansion of x^α in \mathbb{R}^α), we can find, for every $n \in \mathbb{N}$, semi-algebraic functions f_n, g_n such that

$$T \models f_n(\bar{q}) < h(\bar{q}) < g_n(\bar{q}) \wedge |f_n(\bar{q}) - g_n(\bar{q})| < 1/n.$$

Now, there exists an $n \in \mathbb{N}$ such that $\mathbb{R}^\alpha \models g_n(\bar{q}) < 0$. Since T contains the theory of real closed fields, the truth of the last statement can be transferred to every model of T . \square

3.7 Theorem. *Let $F = (f_1, \dots, f_n) \in (M_n(\mathbb{Z}[\alpha]))^n$. Suppose that $\mathbb{R}^\alpha \models \exists \bar{x} \in V^{\text{reg}}(F)$. Then $T \vdash \exists \bar{x} \in V^{\text{reg}}(F)$*

Proof. Let $\bar{x}_0 \in \mathbb{R}^n$ such that $\bar{x}_0 \in V^{\text{reg}}(F)$. Choose $N \in \mathbb{N}$ such that $\|\bar{x}_0\| < N$ and $|JF(\bar{x}_0)| > N^{-1}$. Compute $\theta = \theta(n, N, F)$ as in Lemma 3.5 and notice that $\|F(\bar{x}_0)\| = 0 < \theta^{-1}$. By continuity, we can find $\bar{q} \in \mathbb{Q}^n$ such that in \mathbb{R}^α the following holds:

$$\|\bar{q}\| < N \wedge |JF(\bar{q})| > N^{-1} \wedge \|F(\bar{q})\| < \theta^{-1}. \quad (*)$$

By Lemma 3.6, in every model of T the inequalities in (*) hold. We conclude the proof by Lemma 3.5. \square

The following result is an easy consequence of the Noether normalization lemma.

3.8 Proposition. *Let R be a domain. Let $m \in \mathbb{N}$, $Q \subseteq R[x_1, \dots, x_m]$ a prime ideal such that $Q \cap R = \{0\}$ and let $r = \text{trdeg}_R \text{Frac}(\frac{R[x_1, \dots, x_m]}{Q})$. Then there exists $q_0 \in R[x_1, \dots, x_m] \setminus Q$ such that the ideal $q_0 Q$ is generated by $m-r$ polynomials.*

3.9 Definition. A real number α is exponentially algebraic if the following holds: there exist $n \in \mathbb{N}$, $\alpha_2, \dots, \alpha_n \in \mathbb{R}$, $f_1, \dots, f_n \in \mathbb{Z}[x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n}]$ such that $(\alpha, \alpha_2, \dots, \alpha_n) \in V^{\text{reg}}(f_1, \dots, f_n)$. Otherwise, α is said to be *exponentially transcendental*. It is well known (see for example [JW]) that a real number is generic if and only if it is exponentially transcendental.

We now state the Schanuel condition, proved in [BKW08, Theorem 1.1], that is needed to conclude our proof.

3.10 Theorem. *Let α be exponentially transcendental and $\bar{a} = (a_1, \dots, a_n) \in (\mathbb{R}^+)^n$ and suppose the coordinates of \bar{a} are multiplicatively independent. Then,*

$$\text{trdeg}_{\mathbb{Q}(\alpha)} \mathbb{Q}(\alpha)(\bar{a}, \bar{a}^\alpha) \geq n.$$

We are ready to prove the last step of our main result.

3.11 Theorem. *Assume that α is generic. Let $g \in M_n(\mathbb{Z}[\alpha])$ be such that $\mathbb{R}^\alpha \models \exists \bar{x} g(\bar{x}) = 0$. Then $T \vdash \exists \bar{x} g(\bar{x}) = 0$.*

Proof. By [Wilkie96, Theorem 5.1] there exist $F \in (M_n(\mathbb{Z}[\alpha])[\bar{x}^{-1}])^n$ and $\bar{a} \in \mathbb{R}^n$ such that $g(\bar{a}) = 0$ and $\bar{a} \in V^{\text{reg}}(F)$. By multiplying the components of F by suitable powers of \bar{x} , we may assume that \bar{x}^{-1} does not appear in F . By Theorem 3.7, F has a regular zero in every model of T . The problem is that this need no longer be a zero of g .

We first show that we may assume that the coordinates of \bar{a} are multiplicatively independent. So, suppose not, then there exist $b_1, \dots, b_n \in \mathbb{Z}$ such that $\prod_{i=1}^n a_i^{b_i} = 1$. Hence, $a_n = (\prod_{i=1}^{n-1} a_i^{b_i})^{-1/b_n}$. Define

$$h(x_1, \dots, x_{n-1}) = \prod_{i=1}^{n-1} x_i^{b_i m} g(x_1^{b_n}, \dots, x_{n-1}^{b_n}, (\prod_{i=1}^{n-1} x_i^{b_i})^{-1}),$$

where m is the total degree of g viewed as a polynomial in $2n$ variables. Notice that $(a_1^{1/b_n}, \dots, a_{n-1}^{1/b_n}) \in \mathbb{R}^{n-1}$ is a zero of h , which can be completed to a zero in \mathbb{R}^n of $h \in M_n(\mathbb{Z}[\alpha])$, with the last coordinate independent from the others. Moreover, in every model of T every zero (c_1, \dots, c_{n-1}) of h gives rise to a zero $(c_1^{b_n}, \dots, c_{n-1}^{b_n}, (\prod_{i=1}^{n-1} c_i^{b_i})^{-1})$ of g . Hence we can repeat the process until we obtain that the coordinates of the zero are multiplicatively independent.

Secondly, we may assume that the coordinates of \bar{a} are all positive. In fact, suppose (by reordering the variables) that the first k coordinates of \bar{a} are negative. Then $(-a_1, \dots, -a_k, a_{k+1}, \dots, a_n)$ is a zero of $g^*(\bar{x}) := g(-x_1, \dots, -x_k, x_{k+1}, \dots, x_n)$. If we prove that in every model K of T the function g^* has a zero $\bar{\gamma} = (c_1, \dots, c_n) \in K^n$, then we also obtain that g has a zero $\bar{\gamma}' = (-c_1, \dots, -c_k, c_{k+1}, \dots, c_n) \in K^n$.

Let $\bar{x} = (x_1, \dots, x_n), \bar{y} = (y_1, \dots, y_n), \bar{z} = (z_1, \dots, z_n)$. For $h \in M_n(\mathbb{Z}[\alpha])$, define $\tilde{h}(\bar{y}, \bar{z}) \in \mathbb{Z}[\alpha][\bar{y}, \bar{z}]$ as the unique polynomial such that for all \bar{x} , $h(\bar{x}) = \tilde{h}(\bar{x}, \bar{x}^\alpha)$. Put $\tilde{x} = (\bar{x}, \bar{x}^\alpha)$.

Using the fact that \bar{a} is a regular zero, it is easy to see that $\text{trdeg}_{\mathbb{Q}(\alpha)} \mathbb{Q}(\alpha)(\bar{a}, \bar{a}^\alpha)$ is at most n . Since \bar{a} is multiplicatively independent, we may apply Theorem 3.10 to conclude that

$$\text{trdeg}_{\mathbb{Q}(\alpha)} \mathbb{Q}(\alpha)(\bar{a}, \bar{a}^\alpha) = n.$$

Let $P := \{q \in \mathbb{Z}[\alpha][\bar{y}, \bar{z}] : q(\tilde{a}) = 0\}$. Then P is a prime ideal and hence by Proposition 3.8, there exists $p_0 \in \mathbb{Z}[\alpha][\bar{y}, \bar{z}] \setminus P$ such that the ideal $p_0 P$ is generated by n polynomials p_1, \dots, p_n . Let $h_i(\bar{x}) := p_i(\bar{x}, \bar{x}^\alpha) \in M_n(\mathbb{Z}[\alpha])$ for $i = 0, \dots, n$ and $h_{n+1}(\bar{x}, x_{n+1}) := x_{n+1} h_0(\bar{x}) - 1 \in M_{n+1}(\mathbb{Z}[\alpha])$. Let $H =: (h_1, \dots, h_{n+1}) \in (M_{n+1}(\mathbb{Z}[\alpha]))^{n+1}$.

Using the fact that $\bar{a} \in V^{\text{reg}}(F)$, we easily see that $(\bar{a}, h_0(\bar{a})^{-1}) \in \mathbb{R}^{n+1}$ is a regular solution of the system $H = 0$; in particular $V^{\text{reg}}(H) \neq \emptyset$ in \mathbb{R}^{n+1} , hence, by Theorem 3.7, for every model K of T there exists $(\bar{\gamma}, \gamma_{n+1}) \in K^{n+1}$ which is a regular solution of $H = 0$ in K . In particular,

$$K \models \bigwedge_{i=1}^n h_i(\bar{\gamma}) = 0 \wedge h_0(\bar{\gamma}) \neq 0 \quad (1)$$

We claim that $K \models g(\bar{\gamma}) = 0$.

Notice that $\tilde{g} \in P$, hence

$$\mathbb{R}^\alpha \models \forall \bar{y}, \bar{z} \quad p_0(\bar{y}, \bar{z})\tilde{g}(\bar{y}, \bar{z}) = \sum b_j(\bar{y}, \bar{z})p_j(\bar{y}, \bar{z}) \quad (2)$$

Now, the above is a polynomial identity with coefficients in $\mathbb{Z}[\alpha]$. Let us rewrite (2) as

$$\mathbb{R}^\alpha \models \forall \bar{y}, \bar{z} \quad \sum c_i(\bar{y}, \bar{z})\alpha^i = 0, \quad c_i \in \mathbb{Z}[\bar{y}, \bar{z}] \quad (3)$$

Since α is exponentially transcendental (in particular, transcendental), for all i and for all \bar{y}, \bar{z} we have $c_i(\bar{y}, \bar{z}) = 0$. By Tarski's decidability result for $\text{Th}(\mathbb{R})$, the latter holds in every real closed field, hence in particular (3) holds in K . Hence,

$$K \models h_0(\bar{\gamma})g(\bar{\gamma}) = \sum \hat{b}_j(\bar{\gamma})h_j(\bar{\gamma}), \quad (4)$$

(where $\hat{b}_j(\bar{x}) = b_j(\bar{x}, x^\alpha)$). Putting equations (1) and (4) together, we obtain that $K \models g(\bar{\gamma}) = 0$. This concludes the proof of Theorem 3.11. \square

4 Existence of a computable generic number

In this section we show the existence of computable generic numbers. Let $I = [-1, 1]$. Fix, by [Servi08, Theorem 4.4.2], a recursive enumeration \mathcal{E} of the tuples (m, f_1, \dots, f_m) such that $m \in \mathbb{N}$, $f_i \in \mathbb{Z}[\bar{x}, e^{\bar{x}}]$ are exponential polynomials in m variables and there exists $\bar{x} \in I^m \cap V^{\text{reg}}(f_1, \dots, f_m)$.

We describe an algorithm which at stage $n \in \mathbb{N}$ outputs $a_n \in \{1, 2\}$ which is different from the n^{th} decimal place of the first coordinate of some regular zero of the n^{th} tuple (m, f_1, \dots, f_m) in the above enumeration (more precisely, $a_n = 1$, unless the mentioned decimal place is already equal to 1, in which case $a_n = 2$).

Once we have exhibited such an algorithm, we claim that the number $\alpha = \sum_{i \geq 1} a_i 10^{-i}$ is a computable generic number. In fact, suppose for a

contradiction that α is not generic, i.e. there exist $m \in \mathbb{N}$ and $\bar{y} \in \mathbb{R}^m$ such that $\bar{y} = (\alpha, y_2, \dots, y_m)$ and $f_i \in \mathbb{Z}[\bar{x}, e^{\bar{x}}]$ such that $\bar{y} \in V^{\text{reg}}(f_1, \dots, f_m)$. Suppose, for now, that $\bar{y} \in I^m$. Then there exists $m' \geq m$ and a system $g_1, \dots, g_{m'}$ of exponential polynomials in m' variables such that (\bar{y}, \bar{z}) is the only regular common zero of the g_i s (for some \bar{z}). This new system occurs at stage n (for some $n \in \mathbb{N}$) in the above mentioned enumeration. But then $a_n \neq a_n$, a contradiction.

It remains to show that we may suppose \bar{y} is in I^m . This can be achieved by replacing any occurrence of y_i with an appropriate integer multiple of that variable (this will also not change the fact that the Jacobian is nonzero).

We now exhibit the algorithm. For every $m, n \in \mathbb{N}$, fix an enumeration $\mathcal{E}^{m,n}$ of the mn -tuples $c^{m,n} = (c_{1,1}, \dots, c_{1,n}, c_{2,1}, \dots, c_{m,n}) \in \{0, \dots, 9\}^{mn}$.

1. We consider the n^{th} tuple (m, f_1, \dots, f_m) in the enumeration \mathcal{E} mentioned above. Let $\bar{f} = (f_1, \dots, f_m)$.
2. Let $c^{m,n} \in \mathcal{E}^{m,n}$ and $k \in \mathbb{N}$. For $i = 1, \dots, m$, let $q_i = \sum_{j=1}^n \frac{c_{i,j}}{10^j}$ and $\bar{q} = (q_1, \dots, q_m) \in I^m \cap \mathbb{Q}^m$.
3. Compute $\theta = \theta(m, 10^{k \cdot n}, \bar{f})$, where θ is as in [MW96, Theorem 4.1].
4. Verify if $\|\bar{f}(\bar{q})\| < \theta^{-1}$ and $|\text{Jac } \bar{f}(\bar{q})| > 10^{-k \cdot n}$.
5. If this is not the case, then consider the next tuple $(c^{m,n}, k)$ in $\mathcal{E}^{m,n} \times \mathbb{N}$. Otherwise, output $a_n = 1$ if $c_{1,n} \neq 1$ and $a_n = 2$ if $c_{1,n} = 1$.

We prove that the procedure always stops, giving an output a_n on input n with the required properties. Notice first that if the procedure stops for a given tuple (\bar{q}, k) , then by [MW96, Theorem 4.1] there exists $\bar{\gamma} \in \mathbb{R}^m$ such that $\bar{\gamma} \in V^{\text{reg}}(\bar{f})$ and $\|\bar{\gamma} - \bar{q}\| < 10^{-k \cdot n}$. In particular, we output a_n which is different from the n^{th} decimal place of γ_1 , as required.

Viceversa, since $\bar{f} = 0$ does have some regular solution $\bar{\gamma} \in I^m$, by continuity there exist (\bar{q}, k) such that the inequalities at step 4 are satisfied. Hence the procedure always stops.

Acknowledgements. We are grateful to Chris Miller for initial discussions and to Jonathan Kirby for advice on exponentially transcendental numbers. We would also like to thank the Fields Institute, where some of this work was done.

References

- [BKW08] M. Bays, J. Kirby, A. Wilkie, *A Schanuel property for exponentially transcendental powers*, submitted, October 2008.

- [Dries85] L. Van den Dries, *The field of reals with a predicate for the powers of two*, Manuscripta Math. 54 (1985), no. 1-2, 187–195.
- [Dries86] L. Van den Dries, *A generalization of the Tarski-Seidenberg theorem, and some nondefinability results*, Bull. Amer. Math. Soc., vol. 15 n. 2, 1986.
- [FS09] A. Fornasiero and T. Servi, *Definably Complete Baire structures*, submitted.
- [JW] G. Jones, A. Wilkie, *Locally Polynomially Bounded Structures*, Bull. London Math. Soc. 40 (2008), 239–248.
- [Khovanskii91] A. G. Khovanskii, *Fewnomials*, Translations of Mathematical Monographs, 88. American Mathematical Society, Providence, RI, 1991. viii+139 pp.
- [Lang66] S. Lang, *Algebra*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Don Mills, Ont. 1966 x+294 pp.
- [MW96] A. Macintyre, A. Wilkie, *On the decidability of the real exponential field*, in: Kreisliana, A. K. Peters, Wellesley, MA, 1996, pp. 441–467.
- [Miller94] C. Miller, *Expansions of the real field with power functions*, Annals of Pure and Applied Logic 68 (1994), 79–94.
- [Servi08] T. Servi, *On the First-Order Theory of Real Exponentiation*, Pisa, Edizioni della Normale, 2008, ISBN 978-88-7642-325-3.
- [Waldschmidt00] M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren der Mathematischen Wissenschaften 326, Berlin, Springer-Verlag, 2000, ISBN 3-540-66785-7.
- [Wilkie96] A. J. Wilkie, *Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function*, J. Amer. Math. Soc. 9 (1996) 1051–1094.