A remark on Zilber's pseudoexponentiation*

David Marker
University of Illinois at Chicago
marker@math.uic.edu

1 Introduction

When studying the model theory of

$$\mathbb{C}_{\exp} = (\mathbb{C}, +, \cdot, \exp, 0, 1)$$

the first observation is that the integers can be defined as

$$\{x : \forall y \ \exp(y) = 1 \rightarrow \exp(xy) = 1\}.$$

Since $\mathbb{C}_{\exp}$ is subject to all of Gödel's phenomena, this is often also the last observation. After Wilkie proved that $\mathbb{R}_{\exp}$ is model complete, one could ask the same question for $\mathbb{C}_{\exp}$, but the answer is negative.

Proposition 1.1 $\mathbb{C}_{\exp}$ *is not model complete*

Proof If $\mathbb{C}_{\exp}$ is model complete, then every definable set is a projection of a closed set. Since $\mathbb{C}$ is locally compact, every definable set is F_σ. The same is true for the complement, so every definable set is also G_δ. But, since $\mathbb{Z}$ is definable, $\mathbb{Q}$ is definable and a standard corollary of the Baire Category Theorem tells us that $\mathbb{Q}$ is not G_δ.

Still, there are several interesting open questions about $\mathbb{C}_{\exp}$.

- Is $\mathbb{R}$ definable in $\mathbb{C}_{\exp}$?

*Partially supported by NSF grant DMS-0200393. This work was completed while I was a member of the Isaac Newton Institute for the Mathematical Sciences and I am grateful for their support.

• (quasiminimality) Is every definable set countable or co-countable? (Note that this is true in the structure $(\mathbb{C}, \mathbb{Z}, +, \cdot)$ where we add a predicate for $\mathbb{Z}$).

• (Mycielski) Is there an automorphism of $\mathbb{C}_{\exp}$ other than the identity and complex conjugation?[1]

A positive answer to the first question would tell us that $\mathbb{C}_{\exp}$ is essentially second order arithmetic, while a positive answer to the second would say that integers are really the only obstruction to a reasonable theory of definable sets.

A fascinating, novel approach to $\mathbb{C}_{\exp}$ is provided by Zilber's [6] pseudoexponentiation. Let $\mathcal{L}$ be the language $\{+, \cdot, E, 0, 1\}$. Zilber shows that there is an $\mathcal{L}_{\omega_1,\omega}(Q)$-sentence Φ, where Q is the quantifier "exists uncountably many", about algebraically closed exponential fields such that Φ has a unique model of power κ for each uncountable cardinal κ.

We briefly describe Φ. If $(K, +, \cdot, E) \models \Phi$, then:

• K is an algebraically closed field of characteristic 0;

• E is a homomorphism from $(K, +)$ onto $(K^\times, \cdot)$ and there is $\nu \in K$ transcendental over $\mathbb{Q}$ such that the kernel of E is $\mathbb{Z}\nu$;

• (Schanuel's Conjecture) if $z_1, \ldots, z_n \in K$ are linearly independent over $\mathbb{Q}$, then the transcendence degree of $\mathbb{Q}(z_1, \ldots, z_n, E(z_1), \ldots, E(z_n))$ over $\mathbb{Q}$ is at least n.

The next axioms are an attempt to make the model as existentially closed as possible. Given $V \subseteq K^{2n}$ we might want to find $z_1, \ldots, z_n$ with $(z_1, \ldots, z_n, E(z_1), \ldots, E(z_n)) \in V$. The problem is that Schanuel's Conjecture restrains us from putting points on small varieties.

Let $G_n(K) = K^n \times (K^\times)^n$. If $A = (m_{i,j})$ is a $k \times n$ matrix of integers, we let $[A] : G_n(K) \to G_k(K)$ be the function $[A](\overline{x}, \overline{y}) = (u_1, \ldots, u_k, v_1, \ldots, v_k)$ where

$$u_i = \sum_{j=1}^{n} m_{i,j} x_j \text{ and } v_i = \prod_{j=1}^{n} y_j^{m_{i,j}}.$$

Definition 1.2 $V \subseteq G_n(K)$ is *normal* if $\dim [A]V \geq k$ for any $k \times n$ matrix A of rank k where $1 \leq k \leq n$.

In particular $\dim V \geq n$.

[1] Mycielski has also asked a less central but delightfully intriguing question. What is the definable closure of $\emptyset$ in $\mathbb{C}_{\exp}$? Note, for example, π and $\sqrt{2}$ are $\emptyset$-definable.

Definition 1.3 $V \subseteq G_n(K)$ is *free* if we can not find $m_1, \ldots, m_n \in \mathbb{Z}$ and $b \in K$ such that V is contained in either the variety

$$\{(\overline{x}, \overline{y}) : m_1 x_1 + \ldots + m_n x_n = b\}$$

or

$$\{(\overline{x}, \overline{y}) : y_1^{m_1} \cdots y_n^{m_n} = b\}.$$

We can now state the last two axioms.

• (Strong Exponential Closure) For all finite A if $V \subseteq G_n(K)$ is irreducible, free and normal there is $(\overline{x}, E(\overline{x})) \in V$ a generic point of V over A.

• (Countable Closures) For all finite A, if $V \subseteq G_n(K)$ is irreducible, free and normal with $\dim V = n$ and defined over the definable closure of A, then $\{(\overline{z}, E(\overline{z})) \in V : \text{generic over } A\}$ is countable.

The countable closure axiom has a natural restatement in terms of Hrushovski-style dimension functions.

Definition 1.4 Let $X \subseteq K$ be finite. We define a predimension

$$\delta(X) = \text{td } (X \cup E(\text{span}(X)) - \text{ld}(X)$$

where $\text{span}(X)$ is the $\mathbb{Q}$-span and $\text{ld}(X)$ is the linear dimension of $\text{span}(X)$. We also define a dimension

$$\partial(X) = \sup\{\delta(Y) : X \subseteq Y \text{ is finite } \}$$

and a closure operator

$$\text{cl}(X) = \{a : \partial(X) = \partial(Xa)\}.$$

In the presence of the other axioms the countable closure axiom is equivalent to the assertion that closures of finite sets are countable.

There is an $\mathcal{L}_{\omega_1,\omega}(Q)$ sentence Φ formalising these axioms.

Theorem 1.5 (Zilber) *For all uncountable cardinals κ there is a unique model of Φ of cardinality κ. If $(K, +, \cdot, E) \models \Phi$, then every definable subset of K is countable or co-countable. If $A \subseteq K$ is finite and $a, b \notin \text{cl}(A)$ there is an automorphism of K taking a to b.*

This raises the tantalising question is $\mathbb{C}_{\exp}$ the unique model of Φ of cardinality $2^{\aleph_0}$? Zilber gives an argument that the countable closure axiom is true using Ax's work on Schanuel's Conjecture for differential fields. In this paper we investigate the simplest case of the Strong Exponential Closure axiom.

Suppose $p(X, Y) \in \mathbb{C}[X, Y]$ is nonconstant and $C \subseteq \mathbb{C} \times \mathbb{C}^\times$ is the curve $p(X, Y) = 0$. It is easy to see that C is normal and, in this case, C is free as long as both X and Y occur in p. We would like to find an infinite set of algebraically independent zeros of $f(z) = p(z, e^z)$. We will prove this in a special case under strong assumptions.

Theorem 1.6 *Assume Schanuel's Conjecture. Suppose $p \in \mathbb{Q}[X, Y]$ is irreducible and depends on X and Y. Then there are infinitely many algebraically independent zeros of $f(z) = p(z, e^z)$.*

I am grateful to Angus Macintyre and Alex Wilkie for several helpful discussions of this work.

2 Infinitely Many Zeros

Let $f : \mathbb{C} \to \mathbb{C}$ be an entire function.

Definition 2.1 We say that f has *order* at most ρ if for every $\epsilon > 0$, there is a constant C such that for all sufficiently large R, if $||z|| \leq R$, then

$$||f(z)|| \leq C^{R^{\rho+\epsilon}}.$$

If $p(X, Y) \in \mathbb{C}[X, Y] \setminus \mathbb{C}[X]$, then $f(z) = p(z, e^z)$ has order 1. We need one basic result from complex analysis (see [4] XIII 3.5).

Theorem 2.2 (Hadamard Factorization) *Suppose f is an entire function of order 1, let $z_1, z_2, \ldots$ be the nonzero zeros of f (listed with multiplicities). Then there are a and b such that*

$$f(z) = e^{az+b} z^m \prod_{n=1}^{\infty} \left(\left(1 - \frac{z}{z_n} \right) e^{z/z_n} \right),$$

where m is the order f at zero,

In particular, if f has order one and only finitely many zeros, then there are $a, b \in \mathbb{C}$ and $q(X) \in \mathbb{C}[X]$ such that

$$f(z) = e^{az+b}q(z).$$

Let $\mathbb{C}[X_1, \ldots, X_n]^E$ be the E-ring of exponential terms over $\mathbb{C}$. Viewing each term as a function on $\mathbb{C}^n$ gives a natural homomorphism from $\mathbb{C}[X_1, \ldots, X_n]^E$ to the ring of entire functions on $\mathbb{C}^n$. The following result was proved independently by van den Dries [2] and Henson and Rubel [3]. We will use only the $n = 1$ case which was an earlier unpublished result of Wilkie.

Theorem 2.3 *The natural homomorphism from $\mathbb{C}[X_1, \ldots, X_n]^E$ to the ring of holomorphic functions on $\mathbb{C}^n$ is injective.*

The following Corollary is reasonably well known.

Corollary 2.4 *If $p \in \mathbb{C}[X, Y]$ is irreducible and depends on X and Y then $f(z) = p(z, e^z)$ has infinitely many zeros.*

Proof Suppose $p(X, Y) \in \mathbb{C}[X, Y]$ irreducible depending on both X and Y. Let $f(z) = p(z, e^z)$. If f has only finitely many zeros, then by Hadamard Factorization

$$f(z) = e^{az}q(z)$$

for some $a \in \mathbb{C}$ and $q(X) \in \mathbb{C}[X]$.

By Theorem 2.3

$$p(z, e^z) - e^{az}q(z) = 0$$

is a term identity. This is only possible if $a \in \mathbb{N}$ and $p(X, Y) = Y^a q(X)$. This violates our assumptions on p.

Similar arguments can be used to show that terms of the form $p(z, e^z, \ldots, e^{z^n})$ usually have infinitely many zeros.

3 Algebraic Independence

We would like to go one step further and claim that $f(z) = 0$ has infinitely many algebraically independent zeros. We will only prove this only in case $p \in \mathbb{Q}^{\text{alg}}[X, Y]$.

Assumption For the remainder of the paper we assume that $p \in \mathbb{Q}^{\text{alg}}[X, Y]$ is irreducible and both X and Y occur in p.

Let $f(z) = p(z, e^z)$. We let $\deg_X p$ and $\deg_Y p$ denote the degree of p when viewed as a polynomial in $\mathbb{C}[Y][X]$ and $\mathbb{C}[X][Y]$, respectively.

Note that if $p(z, e^z) = 0$ and $z \neq 0$, then z is transcendental over $\mathbb{Q}$, as otherwise z, e^z are both algebraic over $\mathbb{Q}$ contradicting the Lindemann-Weierstrass Theorem.

For the remainder of the paper we will also assume Schanuel's Conjecture.

Schanuel's Conjecture If $z_1, \ldots, z_n \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then td $\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})/\mathbb{Q} \geq n$.

Two Independent Solutions

We begin by considering distinct nonzero z, w with $f(z) = f(w) = 0$. We would like to claim that z and w are algebraically independent. Unfortunately, this is not always true. For example, let

$$p(X, Y) = 1 + X^2 Y + Y^2.$$

If $p(z, e^z) = 0$, then $p(-z, e^{-z}) = 0$ as well. We will prove that this is the only possible algebraic dependence.

Theorem 3.1 *Assume Schanuel's Conjecture. Suppose $z, w \neq 0$, $f(z) = f(w) = 0$ and $z \neq \pm w$. Then z and w are algebraically independent.*

Proof Since $z, w \neq 0$, they are transcendental over $\mathbb{Q}$. Thus (z, e^z) and (w, e^w) are generic points of the curve $C \subset \mathbb{C} \times \mathbb{C}^\times$ given by $p(X, Y) = 0$.

For purposes of contradiction, assume z and w are algebraically dependent. Then

$$\text{td } (\mathbb{Q}(z, w, e^z, e^w)/\mathbb{Q}) = 1$$

and, by Schanuel's Conjecture, there are relatively prime integers m, n such that $mz = nw$. We may assume $n > 0$.

Let $v = z/n$. Then $e^z = (e^v)^n$ and $e^w = (e^v)^m$. Let $C_i \subseteq \mathbb{C} \times \mathbb{C}^\times$ be the (possibly reducible) curve $p(iX, Y^i) = 0$. Note that if $i = -j < 0$, then C_i is the zero set of the polynomial $Y^{j \deg_Y p} p(iX, Y^i)$. Since v is interalgebraic with z, (v, e^v) is a generic point of the curves C_n and C_m. This is only possible if C_n and C_m have a common irreducible component.

The map $\phi_i : C_i \to C$ given by $\phi_i(x, y) = (ix, y^i)$ is finite-to-one. Thus each irreducible component of C_i projects generically onto C.

If (x, y) is a generic point of an irreducible component V of C_n, and ω is an n^{th}-root of unity, then $(x, \omega y)$ is also the generic point of an irreducible component W. It follows that $(u, \omega v) \in W$ for all $(u, v) \in V$. Moreover if V_1 and V_2 are irreducible components of C_n and $x \in \mathbb{C}$ is generic, then there is $y \in \mathbb{C}$ and ω an n^{th}-root of unity such that $(x, y) \in V$ and $(x, \omega y) \in W$. Thus the n^{th}-roots of unity act transitively on the irreducible components of C_n.

Factor

$$p(nX, Y^n) = \prod_{i=1}^{l} q_i(X, Y)^{s_i}$$

where $q_1, \ldots, q_n$ are irreducible and relatively prime. Since the n^{th}-roots of unity act on the irreducible components of C_n, each $q_i(X, Y)$ is of the form $q_1(X, \omega Y)$ for some n^{th}-root of unity ω. Thus $s_1 = \ldots = s_l$. Let s be the common value of $s_1, \ldots, s_n$. Examining the degrees of the polynomials we see that

$$\begin{aligned} \deg_X p &= ls \deg_X q_1 \\ n \deg_Y p &= ls \deg_Y q_1 \end{aligned}$$

Suppose C_n and C_m have a common irreducible component given by $q(X, Y) = 0$ where q is irreducible. If $m > 0$, factor

$$p(mX, Y^m) = \prod_{i=1}^{k} r_i(X, Y)^t$$

where each r_i is irreducible. We may assume that $r_1 = q_1 = q$. The same analysis shows that

$$ls \deg_X q = \deg_X p = kt \deg_X q.$$

Since $\deg_X p \neq 0$, $ls = kt \neq 0$. Thus

$$n \deg_Y p = ls \deg_Y q = kt \deg_Y q = m \deg_Y(p).$$

But $\deg_Y p \neq 0$. Thus $n = m$, a contradiction.

The analysis is similar if $m < 0$. Rather than looking at $p(mX, Y^m)$ we consider

$$g(X, Y) = Y^{-m \deg_Y p} p(mX, Y^m).$$

Since p is irreducible,

$$\deg_X g = \deg_X p \text{ and } \deg_Y g = -m \deg_Y p.$$

The same argument now works to conclude that $n = -m$. Thus $n = 1$ and $m = -1$, a contradiction.

The Primitive Case

A key step in our proof is to reduce to a case where we do not worry about reducibility of the curve C_m given by $p(mX, Y^m) = 0$.

Definition 3.2 We say that $p(X, Y)$ is *primitive* if it is irreducible, depends on both variables and C_m is irreducible for each nonzero $m \in \mathbb{Z}$.

Theorem 3.3 *Assume Schanuel's Conjecture. If p is primitive and $z_1, \ldots, z_n$ are nonzero zeros of $f(z) = p(z, e^z)$ with $z_i \neq \pm z_j$ for $i < j$, then $z_1, \ldots, z_n$ are algebraically independent.*

Proof Suppose not. Let n be minimal such that there are algebraically dependent $z_1, \ldots, z_{n+1}$ nonzero zeros of f with $z_i \neq \pm z_j$ for $i < j$. Then

$$\text{td } (\mathbb{Q}(z_1, \ldots, z_{n+1}, e^{z_1}, \ldots, e^{z_{n+1}})/\mathbb{Q}) < n + 1$$

and, by Schanuel's Conjecture, there are integers $m_1, \ldots, m_n, m$ with no common factor such that

$$\sum_{i=1}^{n} m_i z_i = m z_{n+1}.$$

By Theorem 3.1, $n \geq 2$. By the minimality of n we may assume that all of the $m_i, m \neq 0$, and $z_1, \ldots, z_n$ are algebraically independent. Let $v_i = z_i/m$. Let C be the curve $p(X, Y) = 0$ and $\widehat{C} \subseteq \mathbb{C} \times \mathbb{C}^\times$ be the curve $p(mX, Y^m) = 0$. Since p is primitive, $\widehat{C}$ is irreducible. By the minimality of n, $(v_1, e^{v_1}), \ldots, (v_n, e^{v_n})$ are independent generic points on $\widehat{C}$. It follows that the function

$$(x_1, y_1, \ldots, x_n, y_n) \mapsto \left(\sum m_i x_i, \prod y_i^{m_i}\right)$$

maps $\widehat{C}^n$ to C.

Suppose $w_1, \ldots, w_n$ are any zeros of f. Then $(w_i/m, e^{w_i/m})$ is in $\widehat{C}$. Thus $\sum \frac{m_i}{m} z_i$ is also a zero of f. In particular,

$$w = \frac{(m_1 + m_2)}{m} z_1 + \frac{m_3}{m} z_3 + \ldots + \frac{m_n}{m} z_n$$

is also a zero of f. If $n > 2$, we may without loss of generality, assume that $m_1 m_2 > 0$, so this reduces the problem one level. Thus, by the minimality of n, this is only possible if $n = 2$. In this case we have that $mz_3 = (m_1 + m_2)z_1$, where $z_1 \neq 0$. By our analysis in Theorem 3.1, this is only possible if $m_1 + m_2 = 0, \pm m$.

If $m_1 + m_2 = 0$, then 0 is a zero of f and if z is a zero of f so is $\frac{m_i}{m} z$. This is only possible if $m_1 = -m_2 = \pm m$. Without loss of generality, we have $z_1 - z_2 = z_3$. But then $z_1 = z_3 + z_2$, so changing the roles of the variables we get a contradiction as above.

Suppose $m_1 + m_2 = -m$, let $r = \frac{m_1}{m}$, then

$$z_3 = rz_1 - (1 + r)z_2$$

and

$$w = rz_3 - (1 + r)z_2$$

is also a zero of f. But

$$w = r^2 z_1 - (1 + r)^2 z_2$$

and, by our early analysis we must have

$$-1 - 2r = r^2 - (1 + r)^2 = 0, \pm 1.$$

If $-1 - 2r = -1$, then we have a contradiction since $r \neq 0$. If $-1 - 2r = 1$, then $r = -1$ and $z_3 = -z_1$, a contradiction. If $-1 - 2r = 0$, then we have

$$w = r^2 z_1 - (1 + r)^2 z_2$$

and $r^2 - (1 + r)^2 = 0$, we are back in the case $m_1 + m_2 = 0$ and obtain a contradiction as above.

We are left with the case where $m_1 z_1 + m_2 z_2 = mz_3$ and $m_1 + m_2 = m$. Permuting z_1, z_2, z_3 and multiplying by -1 if necessary, we may assume that

$|m| \geq |m_1|, |m_2|$ and $m, m_1 > 0$. Indeed, since each $m_i \neq 0$, we will have $|m| > |m_1|, |m_2| > 0$,

Let

$$\begin{aligned} z_{k+1} &= \frac{m_1}{m} z_k + \frac{m_2}{m} z_2 \\ &= \left(\frac{m_1}{m}\right)^k z_1 + \left[1 - \left(\frac{m_1}{m}\right)^k\right] z_2. \end{aligned}$$

Let $M = \max ||z_1||, ||z_2||$ Then

$$||z_{k+1}|| \leq \left|\left|\left(\frac{m_1}{m}\right)^k\right|\right| M + \left|\left|1 - \left(\frac{m_1}{m}\right)^k\right|\right| M \leq 2M.$$

Thus the zeros of f are not discrete, a contradiction.

The General Case

We now prove Theorem 1.6.

We argue by induction on $\deg_X p$. If p is primitive, this follows from Theorem 3.3.

Suppose p is not primitive. Let C be the curve $p(X, Y) = 0$. Suppose $p(nX, Y^n)$ is reducible and let $\widehat{C}$ be an irreducible component. Suppose q is irreducible and $q(X, Y) = 0$ defines $\widehat{C}$. Arguing as above $\deg_X q < \deg_X p$.

In particular, if $\deg_X p = 1$, then p is primitive. If $\deg_X p > 1$ and p is not primitive, let n and $\widehat{C}$ be as above, then, by induction, there are $z_1, z_2, \ldots$ algebraically independent with $(z_i, e^{z_i}) \in \widehat{C}$. But then $nz_1, nz_2, \ldots$ are algebraically independent zeros of f.

There are a number of ways one could hope to strengthen the result, even for curves.

• Can we eliminate the assumption that p is defined over a number field?

• In the imprimitive case can we strengthen the conclusion to that of the primitive case? Theorem 3.1 has a much easier proof in the primitive case. We include the full argument in hopes that it might be a first step towards a stronger result.

• Consider the case when $p(X, Y) = Y - X$. In this case we would like to find infinitely many algebraically independent fixed points of e^z. Can we find them without using Schanuel's Conjecture?

References

[1] J. Ax, On Schanuel's conjectures. Ann. of Math. (2) 93, 1971 252–268.

[2] L. van den Dries, Exponential rings, exponential polynomials and exponential functions. Pacific J. Math. 113 (1984), no. 1, 51–66.

[3] C. W. Henson and L. A. Rubel, Some applications of Nevanlinna theory to mathematical logic: identities of exponential functions. Trans. Amer. Math. Soc. 282 (1984), no. 1, 1–32.

[4] S. Lang, *Complex Analysis* 4th edition, Springer, 1999.

[5] A. 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,(4), 1996,1051-1094.

[6] B. Zilber, Pseudo-exponentiation on algebraically closed fields of characteristic zero, Annals of Pure and Applied Logic, Vol 132 (2004) 1, 67-95