Page Proof

Journal of Algebra and Its Applications
Vol. 12, No. 7 (2013) 1350055 (22 pages)

DOI: 10.1142/S0219498813500552

World Scientific
www.worldscientific.com

ON THE MODEL THEORY OF THE LOGARITHMIC FUNCTION IN COMPACT LIE GROUPS

SONIA L'INNOCENTE
School of Science and Technology — Division of Mathematics
University of Camerino
Via Madonna Delle Carceri 9, 62032 Camerino (MC), Italy
sonia.linnocente@unicam.it

FRANÇOISE POINT
Département de Mathématique
Université de Mons, Le Pentagone
20, Place du Parc, B-7000 Mons, Belgium
point@math.univ-paris-diderot.fr

CARLO TOFFALORI
School of Science and Technology — Division of Mathematics
University of Camerino
Via Madonna Delle Carceri 9, 62032 Camerino (MC), Italy
carlo.toffalori@unicam.it

Received 14 December 2011
Accepted 7 March 2013
Published

AQ: Please provide the keywords and the mathematics subject classification codes.

Given a compact linear Lie group G, we form a natural expansion of the theory of the reals where G and the graph of a logarithm function on G live. We prove its effective model-completeness and decidability modulo a suitable variant of Schanuel's Conjecture.

MS classification: 03C60 (primary), 03C10, 03C64, 03B25, 22E
Keywords:
Compact Lie groups, effective model completeness, o-minimality, Lang property, Schanuel Conjecture.

1. Introduction

Let K be either the field $\mathbb{R}$ of reals or the field $\mathbb{C}$ of complexes and for every positive integer n, let $M(n, K)$ be the algebra of $n \times n$ matrices with entries in K. Recently, Macintyre [12, 13] has explored the model theory of Lie groups G and their associated Lie algebras A over K with the corresponding logarithm and exponential maps. He mostly restricted himself to the case where G is a closed subgroup of $\mathrm{GL}(n, K)$ for some positive integer n and A the corresponding algebra of matrices. He points out various interpretability (and non-interpretability) results

2. Compact Lie Groups

We first review basic facts in the theory of Lie groups as exposed in [17] and connect them to the theory of linear Lie groups [18]. We emphasize, in particular, the role of the exponential and logarithmic functions and we introduce in this way the framework of this paper.

Recall that a Lie group G is a topological Hausdorff group which has a compatible analytic atlas (see [17, Chap. 2]). The space $\mathcal{X}$ of left invariant vector fields on G is isomorphic as an $\mathbb{R}$-vector space to the tangent space $T_1(G)$ at the identity 1 of G. The Lie algebra $\mathcal{G}$ of G is defined as $T_1(G)$ with its $\mathbb{R}$-vector space structure and equipped with a Lie product coming from $\mathcal{X}$. (One identifies the vectors of $T_1(G)$ and the left invariant vector fields.) Each x in $\mathcal{G}$ is tangent at 1 to the image of a unique 1-parameter subgroup θ_x of G (a 1-parameter subgroup is an analytic homomorphism from $\mathbb{R}$ into G). This last description allows one to define a map, called the exponential map, from $\mathcal{G}$ to G by $e_G(x) := \theta_x(1)$. One shows that there is an open neighborhood U of 0 in $\mathcal{G}$ such that the exponential map $e_G\lceil_U$ is injective and so it has an inverse denoted by $\log_G$. The Campbell–Baker–Hausdorff formula relates, via this exponential map, the group structure on G and the algebraic structure on $\mathcal{G}$ (see [17, Chap. 3]).

With any $g \in G$, we associate an automorphism A_g of G: $h \to g \cdot h \cdot g^{-1}$, which induces a linear map on $\mathcal{G}$; this allows one to define an operator Ad from G to $\mathrm{GL}(\mathcal{G})$ which is called the adjoint representation of G. Given a Lie group G, we can equip its tangent space $T_1(G)(= \mathcal{G})$ with an inner product and transport it at $T_g(G)$ for any $g \in G$ and show it is a Riemannian metric. This metric is said to be left (respectively right) invariant if the left (respectively right) translation on G is an isometry (see [17, 4.2]) and invariant if it is both left and right invariant. This last property characterizes the compact Lie groups, namely a Lie group G has an invariant Riemannian metric if and only if $\mathrm{Ad}(G)$ is relatively compact in $\mathrm{GL}(\mathcal{G})$ (see [17, Theorem 4.2.3]).

As a corollary, one obtains that any compact Lie group possesses an invariant Riemannian metric (see [17, Corollary 4.2.5]) and if G is a connected compact Lie group, the exponential map is surjective (see [17, 4.3.5]).

Let G be a compact connected Lie group. Using the adjoint representation, and choosing an inner product on $\mathcal{G}$ such that Ad is an orthogonal representation, we get that $\mathrm{Ad}(G) \subseteq O(\mathcal{G})$, where $O(\mathcal{G})$ denotes the group of all linear transformations on $\mathcal{G}$ which are orthogonal with respect to the corresponding inner product.

$\mathrm{Ad}(G) \subseteq O(\mathcal{G})$ $\subseteq$

We have the following characterization of compact Lie groups among compact topological groups, due to Pontryagin. A compact topological group is a compact Lie group if and only if it is isomorphic as a topological group to a closed subgroup of some orthogonal group $O(n)$ if and only if it is isomorphic as a topological group to a closed subgroup of some unitary group $U(n)$ (see [17, Theorem 6.1.1]).

Recall that $U(1)$ is called the one-dimensional torus T (or the circle group); a torus is a group of the form T^n, for some $n \in \mathbb{N} - \{0\}$. These are the compact, connected, abelian Lie groups (see [17, p. 77]).

The compact Lie groups G are classified as follows (see [17, Theorem 6.4.5]). Let G_0 denote its identity connected component. (Since G is compact, this subgroup is necessarily of finite index). Every compact connected Lie group G_0 is analytically isomorphic with a unique group of the form $(T_0 \times \tilde{G}_1 \times \cdots \times \tilde{G}_m)/C$, where G_0 has a finite covering $\tilde{G}_0$ such that $\tilde{G}_0/C \simeq G_0$ with C a finite central subgroup, T_0 is the identity component of the center of G_0 (and so a torus) and each $\tilde{G}_i$, $1 \leq i \leq m$, is a compact, connected, simply connected simple Lie group and so isomorphic to either $\mathrm{SU}(n)$, $\mathrm{Sp}(n)$, $\mathrm{Spin}(n)$ (a covering of $\mathrm{SO}(n)$) and G_2, F_4, E_6, E_7, E_8 (see [17, pp. 137, 138]). The proof of this theorem uses the fact that the adjoint representation of G_0 is a direct sum of irreducible ones. So the Lie algebra $\mathcal{G}$ of G is a direct sum of its center and simple ideals of $\mathcal{G}$ and the center of $\mathcal{G}$ corresponds to the connected component of the center of G and the simple ideals to the normal connected simple subgroups of G. Then, one shows that the map from $T_0 \times \tilde{G}_1 \times \cdots \times \tilde{G}_m$ to G sending $(x_0, \ldots, x_m)$ to $x_0 \cdot \ldots \cdot x_m$ is equal on a neighborhood of the identity to $e_G \circ \log_{T_0 \times \tilde{G}_1 \times \cdots \times \tilde{G}_m}$, where $\log_{T_0 \times \tilde{G}_1 \times \cdots \times \tilde{G}_m}$ is simply the inverse on a suitable neighborhood of the exponential map $e_{T_0 \times \tilde{G}_1 \times \cdots \times \tilde{G}_m}$.

We will deal with some of these compact Lie groups, following the research direction opened by [13] and described in our introduction. We will consider these groups in a first-order setting, namely in an expansion of the field of real numbers with a predicate for the graph of a logarithm function Log we are going to define on them.

Recall that a *real Lie group* of degree n is any Lie group which is topologically isomorphic to a subgroup of $\mathrm{GL}(n, \mathbb{R})$. As reviewed above, any compact Lie group is a real linear Lie group.

Even if we plan to work in an expansion of $\mathbb{R}$, it is convenient for us to recall how the exponential and logarithmic functions, exp and log respectively, are usually defined on the Lie algebra $M(n, K)$ of $n \times n$ matrices over the field K, when K is either the field $\mathbb{R}$ or $\mathbb{C}$. Incidentally, let us point out that we are denoting by log (with a small l) this logarithmic function and by Log (with a capital L) the map we are going to introduce and study. We endow $M(n, K)$ with a norm $\|\cdot\|$ (for instance, the operator norm or the Frobenius norm (i.e. the sum of squares of the absolute values of the entries of the matrix) and define exponential and logarithm functions on matrices as follows:

(1) $\exp : M(n, K) \to \mathrm{GL}(n, K)$ by $\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}$,
(2) $\log : B_1(I) \to M(n, K)$ by $\log(x) = \sum_{k=1}^{\infty} \frac{(-1)^k \cdot (x - I)^k}{k}$,

where I denote the identity matrix and $B_1(I)$ the ball of radius 1 and center I.

These functions have the following properties. Let N_0 be the connected component of 0 in the open neighborhood $\exp^{-1}(B_1(1_A))$ of 0. Then, we have that (see [6, Proposition 5.3]):

(1) for all $x \in N_0$, $\log(\exp(x)) = x$,
(2) for all $x \in B_1(1_A)$, $\exp(\log(x)) = x$,

Proposition 2.1. *For every A and G as listed before, the theory of $(A, G, \mathbb{R}, \exp)$ is undecidable.*

Proof. The integers can be defined as the elements of the field $\mathbb{R}$ that fix the kernel of exp setwise. Their ring structure is just that inherited from the field $\mathbb{R}$. $\square$

Now, we come back to the expansions of $\overline{\mathbb{R}}$ we are interested in. Let A be one of the Lie algebras listed above. Observe that both A and its corresponding Lie group are definable in the ordered field of reals $\overline{\mathbb{R}} := (\mathbb{R}, +, -, \cdot, <, 0, 1)$. To see this, just recall that $\mathbb{C}$ can be viewed as a subset of $\mathbb{R}^2$ and its ring structure can be given by the graphs of the addition, defined componentwise, and the multiplication, defined by: $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$. Then an $n \times n$ matrix over $\mathbb{R}$ can be represented as an ordered [illegible] of reals and an $n \times n$ matrix over $\mathbb{C}$ can be represented as an ordered $2n^2$-tuple of real numbers. Similarly, an $n \times n$ matrix over the quaternions can be viewed as an ordered $4n^2$-tuple of reals. Matrix addition and multiplication can be again defined in a natural way. This ultimately allows to define $SU(n)$, $SO(n)$ and $Sp(n)$ in $\overline{\mathbb{R}}$, both as sets, indeed subsets of a suitable direct power of $\mathbb{R}$, and as groups and the same holds for the corresponding Lie algebras. This approach which can also be formalized in a first-order setting, has been described in [13, Sec. 2].

AQ: We have changed " n2-uple to "n2-tuple" Is this okay?

YES.

First, we note that the expansion $(\overline{\mathbb{R}}, \exp\restriction_A)$ by the graph of the exponential map exp restricted to one of the Lie algebras A listed above, is undecidable.

Proposition 2.2. *The theory of $(\overline{\mathbb{R}}, \exp\restriction_A)$ is undecidable.*

Proof. First, let us prove it in the unitary case. Observe that $su(n)$ includes the diagonal matrices of the form

$$D(\theta) = \operatorname{diag}(i\theta, -i\theta, 0, \ldots, 0)$$

with θ a real, as an $\emptyset$-definable subset. The kernel of exp restricted to these matrices gives a copy of the integers, where addition can be defined via matrix addition, and multiplication via matrix multiplication times the matrix $D(\frac{1}{2\pi})$ — here 2π can be defined as the least real $\theta > 0$ such that $\exp(D(\theta))$ is zero. In this way, the ring of integers is definable in our structure, which implies undecidability.

The symplectic case can be treated in a similar way, while for the orthogonal case one can refer to the block-diagonal matrices ~~but~~ having the first 2×2 block of the form

$$\begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}$$

with θ a real and the other blocks either $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ or, for an odd n, a further 0. $\square$

So, let us turn now our attention to the logarithm. We will need the following description of the linear Lie groups $SU(n)$, $SO(n)$ and $Sp(n)$.

$n \in \mathbb{N} - \{0\}\}$, a function Log everywhere defined and which coincides with the function log on a neighborhood of 1 and such that for any $a \in G$, $\exp(\mathrm{Log}(a)) = a$. This function Log will have the expected properties (see Lemma 2.5) and in Sec. 3, we will show that it is definable in a Pfaffian expansion of $\overline{\mathbb{R}}$. $\overline{\mathbb{R}}$

Case 1: $\mathrm{SU}(n)$.

Let $a \in \mathrm{SU}(n)$, a' as in Proposition 2.3(1). Thus the conjugate $a' = u^{-1} \cdot a \cdot u$ of a with a suitable matrix $u \in \mathrm{SU}(n)$ is diagonal, and indeed $a' = \mathrm{diag}(e_1, \ldots, e_n)$ with $e_k = e^{i\theta_k}$ for $k = 1, \ldots, n$ and $\prod_{1 \le k \le n} e_k = 1$. Take $-\pi < \theta_k \le \pi$ for every $k = 1, \ldots, n-1$ and $\sum_{1 \le k \le n} \theta_k = 0$. Now put

$$\mathrm{Log}(a') = \mathrm{diag}(i\theta_1, \ldots, i\theta_n).$$

Then put

$$\mathrm{Log}(a) = \mathrm{Log}(u \cdot a' \cdot u^{-1}) := u \cdot \mathrm{Log}(a') \cdot u^{-1}.$$

Observe that, if $b' = \mathrm{diag}(i\theta_1, \ldots, i\theta_n)$, then $a' = \exp(b')$ where exp is the matrix exponential map from the matrix space $M(n, \mathbb{C})$ to $\mathrm{GL}(n, \mathbb{C})$ as defined in Sec. 1. Moreover,

$$a = u \cdot a' \cdot u^{-1} = u \cdot \exp(b') \cdot u^{-1} = \exp(u \cdot b' \cdot u^{-1})$$

(see [18, Proposition 3, p. 4]), whence it makes sense to introduce $\mathrm{Log}(a)$ in the way we have done it.

Notice that u and a' are not unique. However, take another matrix t in $\mathrm{SU}(n)$ such that $a'' = t^{-1} \cdot a \cdot t$ is also diagonal. Then $a'' = \mathrm{diag}(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ for some permutation $\sigma \in S_n$ and the conjugation with $u^{-1} \cdot t$ send a' to a''. It follows that $u^{-1} \cdot t$ is a product of involution matrices, whence t is obtained by composing u with this product. For example, when $n = 2$ one may compose u with $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then the conjugation with $u^{-1} \cdot t$ also sends b' to $b'' = \mathrm{diag}(i\theta_{\sigma(1)}, \ldots, i\theta_{\sigma(n)})$, where $-\pi < \theta_{\sigma(i)} \le \pi$ for $1 \le \sigma(i) < n$ and $\sum_{1 \le k \le n} \theta_{\sigma(k)} = 0$. Thus, it is easily seen that $t \cdot b'' \cdot t^{-1} = u \cdot b' \cdot u^{-1}$.

AQ: Kindly check the renumbering.

Please, leave it as it was

Case 3

Case 3 $\mathrm{Sp}(n)$. By Proposition 2.3(3), a matrix a in $\mathrm{Sp}(n)$ is conjugate over $\mathbb{C}$ to a diagonal matrix of size $2n \times 2n$ with entries $e^{i\theta_k}$, $e^{-i\theta_k}$ $(1 \le k \le n)$, whence we can repeat the same arguments as in Case 1 and introduce a similar Log. #

Case 2 Case ~~3~~: $\mathrm{SO}(n)$.

Now, we refer to (2) in Proposition 2.3. Every $a \in \mathrm{SO}(n)$ is conjugate in $\mathrm{SO}(n)$ to a matrix a' which is block-diagonal with 2×2 blocks of the form

$$a' = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

(with $-\pi < \theta \le \pi$) and possibly a further 1×1 block equal to 1. Note that each 2×2 block is diagonalizable over the field $\mathbb{C}$ of complex numbers. It suffices to conjugate it with the unitary matrix $c = \frac{1+i}{2}\left(\begin{smallmatrix} -1 & 1 \\ i & i \end{smallmatrix}\right)$, whose inverse is $c^{-1} = \frac{1-i}{2}\left(\begin{smallmatrix} -1 & -i \\ 1 & -i \end{smallmatrix}\right)$. One gets in this way $\mathrm{diag}(e^{i\theta}, e^{-i\theta})$. On the other hand, it is easy to see that

$$c \cdot \mathrm{diag}(i\theta, -i\theta) \cdot c^{-1} = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}.$$

Assume momentarily $n = 2$, that is, $a \in \mathrm{SO}(2)$. Hence a consists of a single 2×2 block as before, and indeed a is just $\left(\begin{smallmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{smallmatrix}\right)$ for some θ. As said, $c^{-1} \cdot a \cdot c = \mathrm{diag}(e^{i\theta}, e^{-i\theta})$. Define $\mathrm{Log}(a)$ as

$$c \cdot \mathrm{diag}(i\theta, -i\theta) \cdot c^{-1} = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}.$$

Observe once again that $\exp(\mathrm{diag}(i\theta, -i\theta)) = \mathrm{diag}(e^{i\theta}, e^{-i\theta})$, so that

$$\exp\begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix} = \exp\left(c \cdot \begin{pmatrix} i\theta & 0 \\ 0 & -i\theta \end{pmatrix} \cdot c^{-1}\right) = c \cdot \exp\begin{pmatrix} i\theta & 0 \\ 0 & -i\theta \end{pmatrix} \cdot c^{-1}$$
$$= c \cdot \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \cdot c^{-1} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

For an arbitrary $n \geq 2$ with n even, we proceed block by block to build and manage a'. For an odd n, we take 0 as a last block in the logarithm of a'. As in the unitary case one checks that the choice of u' does not affect the final value of $\mathrm{Log}(a)$.

Now, we state some basic properties of the function Log, the first one directly following from the definition of Log given above.

Lemma 2.5. *Let n be an integer ≥ 2, G be one of the compact Lie groups* $\mathrm{SO}(n)$, $\mathrm{SU}(n)$, $\mathrm{Sp}(n)$, *A be the corresponding Lie algebra:*

(1) Log *maps G to A.*
(2) $\mathrm{Log}(I)$ *equals the zero matrix.*
(3) *For every $a \in G$,* $\exp(\mathrm{Log}(a)) = a$.
(4) *For a_1 and a_2 commuting matrices in G,* $\mathrm{Log}(a_1 \cdot a_2) - (\mathrm{Log}(a_1) + \mathrm{Log}(a_2))$ *is the conjugate of*
   - *a diagonal matrix whose diagonal entries are integer multiples of $2\pi i$ in the unitary and symplectic cases,*
   - *a block diagonal matrix with diagonal 2×2 blocks of the form*
   $$\begin{pmatrix} 0 & -2h\pi \\ 2h\pi & 0 \end{pmatrix},$$
   h an integer, and possibly a 1×1 block of the form $2h'\pi$, with h' again an integer, in the orthogonal case.

In particular, for every $a \in G$, $-\mathrm{Log}(a)$ coincides to $\mathrm{Log}(a)^{-1}$ modulo the conjugate of a matrix as just described.

its ring structure given in the usual definable way. Then $n \times n$-matrices over $\mathbb{C}$ (respectively over $\mathbb{R}$, $\mathbb{H}$) can be regarded as $2n^2$-tuples (respectively n^2-tuples, $4n^2$-tuples) with coefficients in $\mathbb{R}$ and one can view the logarithm map as a subset of $\mathbb{R}^{2n^2}$ (respectively $\mathbb{R}^{n^2}$, $\mathbb{R}^{4n^2}$) — that is, its graph —, so as a $4n^2$-ary (respectively $2n^2$-ary, $8n^2$-ary) relation on $\mathbb{R}$. We will denote the relation obtained in this way by $\mathrm{Log} \restriction G$, the corresponding expansion of $\overline{\mathbb{R}}$ by $(\overline{\mathbb{R}}, \mathrm{Log} \restriction G)$ and the first-order language of this structure by $\mathcal{L}_{\mathrm{Log}}$. Thus $\mathcal{L}_{\mathrm{Log}}$ is the language of ordered rings enriched by a $4n^2$-ary (or $2n^2$-ary, or $8n^2$-ary, according to the case we are dealing with) relation symbol.

AQ: Please check the sentence it seems to be incomplete.

We will denote by $\tan^{-1}$ the inverse of the tangent function on $]-\pi/2, \pi/2[$ and by $r\tan^{-1}$ its restriction to the interval $[0,1]$, $r\tan^{-1} = \tan^{-1} \restriction [0,1]$. We will also denote by $\mathbf{r}\tan^{-1}$ the extension of this restricted $\tan^{-1}$ to the whole $\mathbb{R}$ obtained by ~~putting it identically 0 on $\mathbb{R} - [0,1]$.~~ [redacted] symbol τ, ~~so~~ it provides a common first-order

Using trigonometric identities, we observe that the function $\tan^{-1}$ is quantifier free 0-definable in $(\overline{\mathbb{R}}, r\tan^{-1})$. Namely, $\tan^{-1}(-x) = -\tan^{-1}(x)$, $\tan^{-1}(1) = \pi/4$, $\tan^{-1}(x^{-1}) = \pi/2 - \tan^{-1}(x)$ for $x > 0$ and $\tan^{-1}(x^{-1}) = -\pi/2 - \tan^{-1}(x)$ for $x < 0$. Conversely, $r\tan^{-1}$ is 0-definable in a trivial way in $(\overline{\mathbb{R}}, \tan^{-1})$.

In order to have a continuous function on $\mathbb{R}$, it is sometimes convenient to identify the function $\tan^{-1}$ restricted to $[0,1]$ with the function $\tan^{-1}(\frac{1}{1-x^2})$. Even though in $\mathbb{R}$ these two functions are different, the structures $(\overline{\mathbb{R}}, r\tan^{-1})$ and $(\overline{\mathbb{R}}, ~~x \mapsto~~ \tan^{-1}(\frac{1}{1+x^2}))$ have the same (existentially) definable sets (see the introduction of [21]). The model theory of the expansion of the field $\overline{\mathbb{R}}$ with $\tan^{-1}(\frac{1}{1+x^2})$ relies on the fact that this function belongs to the following Pfaffian chain (see [21]; we will adopt in the following the notation of that paper).

First, let us recall what is a Pfaffian chain $G_1, \ldots, G_m$ on an open O of $\mathbb{R}$, of degree $d \geq 1$. It is a sequence of real analytic functions $G_1, \ldots, G_m$ in O satisfying differential equations $\frac{\partial G_i}{\partial x} = p_i(x, G_1(x), \ldots, G_i(x))$, for $i = 1, \ldots, m$, where $p_i \in \mathbb{R}[x, y_1, \ldots, y_i]$ are polynomials of total degree $\leq d$.

AQ: Please check any missing character?

No.

Coming back to our setting, set $G_3(x) := \tan^{-1}(\frac{1}{1-x^2})$. Let us denote the derivative $\frac{\partial}{\partial x}$ by [redacted]. Now consider:

$\frac{\partial}{\partial x}$ by $'$. Now

(1) $G_1(x) := \frac{1}{1+x^2}$, whence the derivative is $G_1' = -2x \cdot G_1^2$, and one can put $p_1(x, y) = -2x \cdot y^2$;
(2) $G_2(x) := \frac{1}{1-G_1^2}$, whence the derivative is $G_2' = -2G_2^2 \cdot G_1 \cdot G_1' = 4x \cdot G_2^2 \cdot G_1^3$, so that one can put $p_2(x, y, z) = 4x \cdot y^3 \cdot z^2$;
(3) finally $G_3(x)$, whence the derivative is $G_3' = G_2 \cdot G_1' = -2x \cdot G_2 \cdot G_1^2$ and one can put $p_3(x, y, z) = -2x \cdot y^2 \cdot z$.

This is a Pfaffian chain. Note that the total degrees of the polynomials in it do not exceed 6.

where $\bar{p} = (p_1, \ldots, p_n)$ and $\bar{s} = (s_1, \ldots, s_r)$ are finite tuples of non-negative integers ranging over finite sets of indexes, P and S respectively, and the $b_{\bar{p},\bar{s}}$ are in $\mathbb{Z}$.

Let $\mathbb{R}^*$ be the multiplicative group of the field of real numbers $\overline{\mathbb{R}}$ and $\mathbb{R}^{>0}$ its subgroup consisting of the positive elements in $\mathbb{R}^*$. We will be interested in certain subgroups of $\mathbb{R}^{>0}$ (and hence of $\mathbb{R}^*$) and in some finite direct powers of them. The key fact about these subgroups is that they satisfy the so-called *Lang property* [10] see also [1] for this kind of questions (we are going to state it within a few paragraphs).

These subgroups are obtained in the following way. Let $n \geq r$ be as before, $\bar{c} = (c_1, \ldots, c_n)$ a tuple of *positive* integers. Thus look at (the divisible hull of) the subgroup $\Gamma := \Gamma_{\theta_1,\ldots,\theta_r}$ generated by $\theta_1 := \tan^{-1}(c_1), \ldots, \theta_r := \tan^{-1}(c_r)$. Observe that, as $c_i > 0$ for every $1 \leq i \leq n$, the same is true of θ_i for $1 \leq i \leq r$. Then Γ is a finitely generated subgroup of $\mathbb{R}^{>0}$. Notice also that we could have taken arbitrary (possibly zero or negative) integers $c_1, \ldots, c_n$ as well. However, due to the trigonometric identity $\tan^{-1}(-x) = -\tan^{-1}(x)$ the case when some c_i is negative can be easily reduced to ours (with non-negative, and even positive, $c_1, \ldots, c_n$).

Of course the equation $q(c_1, \ldots, c_n, y_1, \ldots, y_r) = 0$ defines a variety of $\mathbb{R}^r$. Let us denote it by $V = V(q, \bar{c})$.

Up to re-indexing $\theta_1, \ldots, \theta_r$, we may also assume that $\theta_1, \ldots, \theta_k$, $k \leq r$, are multiplicatively independent and that k is maximal with that property. So there exists $N \in \mathbb{N}$ such that $\theta_{k+1}, \ldots, \theta_r \in \langle \theta_1^{\frac{1}{N}}, \ldots, \theta_k^{\frac{1}{N}} \rangle$ (here, for θ a positive real and M a positive integer, $\theta^{\frac{1}{M}}$ denotes the unique real Mth root of θ). Then any element of Γ can be written as $\theta_1^{\frac{b_1}{N}} \cdot \ldots \cdot \theta_k^{\frac{b_k}{N}}$ for some $b_1, \ldots, b_k \in \mathbb{Z}$. In particular let us put, for $k+1 \leq h \leq n$, $\theta_h = \theta_1^{\frac{a_{h1}}{N}} \cdot \ldots \cdot \theta_k^{\frac{a_{hk}}{N}}$ for some suitable $a_{h1}, \ldots, a_{hk} \in \mathbb{Z}$.

We will say that Γ is *effectively presented in terms of* $c_1, \ldots, c_n$ if the integers k, N, $a_{h1}, \ldots, a_{hk}$ $(k+1 \leq h \leq n)$ can be effectively found from $(c_1, \ldots, c_n)$.

Next observe that looking for the zeroes of our family of "polynomials"

$$q_{\bar{z}}(c_1, \ldots, c_n, y_1, \ldots, y_r)$$

in Γ is the same as looking for the zeroes in Γ of the single polynomial

$$q(c_1, \ldots, c_r, \ldots, c_n, y_1, \ldots, y_r).$$

Accordingly consider this polynomial $q(c_1, \ldots, c_n, y_1, \ldots, y_r) \in \mathbb{Z}[y_1, \ldots, y_r]$. For a given $\bar{s} = (s_1, \ldots, s_r) \in S$, let $p(\bar{s}) = \sum_{\bar{p} \in P} b_{\bar{p},\bar{s}} c_1^{p_1} \cdot \ldots \cdot c_n^{p_n}$ be the coefficient of the monomial $y_1^{s_1} \cdot \ldots \cdot y_r^{s_r}$ in it.

The support $\mathcal{S} = \mathcal{S}(q, \bar{c})$ of this polynomial with respect to q and $\bar{c} = (c_1, \ldots, c_n)$ is the set of tuples $\bar{s}$ such that the coefficient $p(\bar{s})$ is not zero. Notice that $\mathcal{S}$ is finite and indeed its size is bounded independently of $c_1, \ldots, c_n$ and Γ. A (finite) partition $\mathcal{P}_{\bar{\gamma}}$ of $\mathcal{S} := \bigsqcup_{t \leq t(\bar{\gamma})} \mathcal{S}_t$ of this set of exponents is said to be compatible with an element $\bar{\gamma} \in \Gamma^r$ if it satisfies for all indexes $t \leq t(\bar{\gamma})$ the equality $\sum_{\bar{s} \in \mathcal{S}_t} p(\bar{s}) \cdot \gamma_1^{s_1} \cdot \ldots \cdot \gamma_r^{s_r} = 0$. Clearly even the size of the (finite) set of these partitions is finite and bounded independently of Γ. A partition $\mathcal{P}_{\bar{\gamma}}$ of $\mathcal{S}$ is maximal compatible with $\bar{\gamma} \in \Gamma^n$, if any strictly finer partition of $\mathcal{S}$ is not compatible with $\bar{\gamma}$.

Let $H_{\mathcal{P}_{\bar\gamma}}$ be the subgroup of $(\mathbb{R}^*)^r$ defined by the system of equations

$$y_1^{s_1}\cdot\ldots\cdot y_r^{s_r} = y_1^{s'_1}\cdot\ldots\cdot y_r^{s'_r},$$

where $\bar s, \bar s'$ range over the same S_t $(t \le t(\bar\gamma))$ and $\bar s \ne \bar s'$.

The group Γ^r has the *Lang property* (see [10, Theorem 2]), i.e. given the variety V, there are only finitely many pairs $(\bar\gamma, \mathcal{P})$ (where $\bar\gamma \in \Gamma^r$ and $\mathcal{P} = \mathcal{P}_{\bar\gamma}$ is a partition maximal compatible with $\bar\gamma$) such that $V \cap \Gamma^r = \bigcup_{(\bar\gamma,\mathcal{P})} \bar\gamma\cdot(H_{\mathcal{P}} \cap \Gamma^r)$. (In particular, if the rank of Γ is equal to r, then $H_{\mathcal{P}} \cap \Gamma^r = \{1\}$.) Incidentally, let us recall that, in order to show the finiteness of the number of such $(\bar\gamma, \mathcal{P})$, one uses the finiteness of the number of non-degenerate solutions of a linear recurrence equation, namely an equation of the form $\sum_l d_l \cdot y_l = 0$ (or $= 1$). Here the coefficients d_l are in $\mathbb{Z}$ and one looks for solutions y_l in $\mathbb{R} \cap \Gamma$. In our particular case, the number of solutions of such linear recurrence equation can be bounded just in terms of r and the rank $k \le r$ of the group Γ, and hence in terms of r (see [3]). Indeed the number of cosets of the form $\bar\gamma \cdot H_{\mathcal{P}}$ with $\mathcal{P} = \mathcal{P}_\gamma$ and hence γ satisfying the linear relations

$$\sum_{\bar s \in S_j} p(\bar s)\cdot \gamma_1^{s_1}\cdot\ldots\cdot\gamma_r^{s_r} = 0, \quad t \le t(\bar\gamma) \qquad (\star)$$

(but annihilating no proper sub-sum) is bounded in terms of the rank $k \le r$ of Γ and of the number of terms in the sum (which depends on the variety V).

So there exist a positive integer ℓ, ℓ tuples of integers $(m_{j1}, \ldots, m_{jr})$ of the form $m_{ji} = s_i - s'_i$ $(i = 1, \ldots, r,\ j = 1, \ldots, \ell,\ \bar s, \bar s'$ in the same S_t with $t \le t(\bar\gamma))$ and $g_1, \ldots, g_\ell \in \Gamma$ of the form $g_j = \prod_{i=1}^r \gamma_i^{m_{ji}}$, such that, for every $(u_1, \ldots, u_r) \in \Gamma^r$, $(u_1, \ldots, u_r)$ is in $V \cap \Gamma^r$ if and only if it satisfies

$$u_1^{m_{j1}}\cdot\ldots\cdot u_r^{m_{jr}} = g_j \qquad (\star\star)$$

for all j in some suitable subset of $\{1, \ldots, \ell\}$. Indeed note that, if $(u_1, \ldots, u_r)$ is a tuple of Γ^r satisfying $(\star\star)$, then

$$(u_1, \ldots, u_r)\cdot(\gamma_1, \ldots, \gamma_r)^{-1}$$

satisfies $\prod_{i=1}^r (u_i \cdot \gamma_i^{-1})^{m_{ji}} = 1$ and so is in $H_{\mathcal{P}}$.

Note that (see [3, 10]) one can bound ℓ and the integers m_{ji} only in terms of the exponents of nontrivial terms occurring in the polynomial q defining V, via $c_1, \ldots, c_n$ and of the rank of Γ.

We will say that *the Lang property is effective* if the elements $g_1, \ldots, g_\ell \in \Gamma$ (and the corresponding subsets arising in the way described before) can be effectively found in terms of $\langle\theta_1, \ldots, \theta_k\rangle$.

For every $i = 1, \ldots, r$ write each $\gamma_i := \theta_1^{\frac{\alpha_{1i}}{N}}\cdot\ldots\cdot\theta_k^{\frac{\alpha_{ki}}{N}}$, for some $\alpha_{1i}, \ldots, \alpha_{ki} \in \mathbb{Z}$. Then for every $j = 1, \ldots, \ell$

$$g_j = \theta_1^{\frac{\sum_i \alpha_{1i}\cdot m_{ji}}{N}}\cdot\ldots\cdot\theta_k^{\frac{\sum_i \alpha_{ki}\cdot m_{ji}}{N}}.$$

So in order to check whether the tuple $\bar{\theta}$ (that is, $(\tan^{-1}(c_1), \ldots, \tan^{-1}(c_r))$) satisfies $q_{\bar{z}}(\bar{c}, \bar{\theta}) = 0$ for a given $\bar{z} \in \mathbb{Z}^r$, it suffices to test that a linear system made by equations like

$$\bigwedge_{f=1}^{k} \left(z_f \cdot m_{jf} + \sum_{h=k+1}^{n} a_{hf} \cdot m_{jh} \cdot z_h = \sum_{i=1}^{r} \alpha_{fi} \cdot m_{ji} \right)$$

(where j ranges in some suitable subset of $\{1, \ldots, \ell\}$) can be solved with respect to the α_{fi}.

Here, we have a free choice of $z_{k+1}, \ldots, z_n$ and then $z_1, \ldots, z_k$ are uniquely determined.

In conclusion, we can state the following proposition.

Proposition 4.5. *Let $n \geq r$ be non-negative integers, $q(x_1, \ldots, x_n, y_1, \ldots, y_r)$ a polynomial with integer coefficients. Consider the corresponding family $q_{\bar{z}}$ for $\bar{z} \in \mathbb{Z}^r$. Fix a tuple $\bar{c} = (c_1, \ldots, c_n)$ of positive integers and let $\Gamma := \Gamma_{\tan^{-1}(c_1), \ldots, \tan^{-1}(c_n)}$. Assume* that

(1) ~~*that*~~ *the Lang property is effective for the subgroup Γ,*
(2) *and* ~~*that*~~ *Γ can be effectively presented in terms of $(c_1, \ldots, c_n)$.*

Then there is a procedure deciding, for every tuple $\bar{z}$ in $\mathbb{N}$, whether

$$q(c_1, \ldots, c_n, \tan^{-1}(c_1)^{z_1}, \ldots, \tan^{-1}(c_r)^{z_r}) = 0$$

or not.

5. Effective Model Completeness and Decidability

In Sec. 3, we recalled that the theory of $(\overline{\mathbb{R}}, r\tan^{-1})$ is model complete and o-minimal. But we can say even more. In fact, by using Wilkie's first main theorem of the model completeness of restricted Pfaffian extensions of $\overline{\mathbb{R}}$ [21] and Macintyre–Wilkie's strategy in [14], or Gabrielov's theorem (see [4]) on complements of sub-analytic sets and the subsequent work of Gabrielov–Vorobjov on effective versions in the case of restricted sub-Pfaffian sets, we obtain the following proposition.

Proposition 5.1. *The theory $T_{r\tan^{-1}}$ is effectively model complete.*

Actually the latter approach gives better effective estimates, provided one can decide existential sentences expressing whether a Pfaffian system of equalities and inequalities has a solution. See about that the enlightening discussion in [12, Sec. 4], where the two approaches, by Macintyre–Wilkie–Servi and by Gabrielov–Vorobjov, are compared. In any case, we get the following corollary.

Corollary 5.2. *For every $G = \mathrm{SU}(n), \mathrm{SO}(n), \mathrm{Sp}(n)$ the theory T_{Log} is effectively model complete.*

Using all these properties, one writes down in $\mathcal{L}_\tau$, a list $T^{\mathrm{rec}}_{r\tan^{-1}}$ of first-order properties of models of $T_{r\tan^{-1}}$:

(1) K is an ordered field.
(2) K is definably complete (namely, every bounded (parametrically) definable subset has a supremum).
(3) $(r\tan^{-1})'(x) = \frac{1}{1+x^2}$ when $x \in]0,1[$, $r\tan^{-1}(0) = 0$, $r\tan^{-1}(1) = \frac{\pi}{4}$, $r\tan^{-1}(x) = 0$ when $x \in \mathbb{R} - [0,1]$.
(4) (*The restricted Khovanskii property*) For every $n, N \in \mathbb{N}$ is a positive integer $\mu(n,N)$ such that, if $p_1, \dots, p_n \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_n]$ are polynomials of degree at most N and for every $i = 1, \dots, n$, f_i is the function in $T_{n,r}$ determined by p_i (in the sense that $f_i(\bar{a}) := p_i(\bar{a}, r\tan^{-1}(\bar{a}))$ for all $\bar{a} \in [0,1]^n$), then $|V^{\mathrm{reg}}(f_1, \dots, f_n)| \leq \mu(n,N)$. there
(5) The scheme of sentences ensuring a Puiseux expansion of functions of $M_{n,r}(K)$, $n \geq r$ in $\mathbb{N}$. This is the analogue of scheme A.7 as stated by Macintyre–Wilkie in [14], see also [19, 4.7.20]; it ~~is referred~~ to as the effective Łojasiewicz Inequalities by Macintyre in [12, Theorem 4.2].

Finally, let us consider the decidability issue. First, let us state a property analogous to the weak Schanuel's Conjecture (WSC) in the case of the exponential function in [14, Sec. 5].

WSC$_\tau$: *There exists an effective procedure which, given $r \leq n \in \mathbb{N}$ and $\bar{f} = (f_1, \dots, f_n)$ and g in $T_{n,r}$, produces a nonzero natural number $\eta := \eta(n, r, \bar{f}, g)$ such that for all $\bar{a} \in [0,1]^r \times \mathbb{R}^{n-r}$, if $\bar{a} \in V^{\mathrm{reg}}(\bar{f})$, then either $g(\bar{a}) = 0$ or $|g(\bar{a})| > \eta^{-1}$.*

Proposition 5.4. *The following conditions are equivalent:*

(i) *the theory $T_{r\tan^{-1}}$ is decidable;*
(ii) *the theory $T_{\tan^{-1}}$ is decidable;*
(iii) WSC$_\tau$ *holds.*

Proof. The equivalence between (i) and (ii) is trivial. So let us compare (i) and (iii).

First assume WSC$_\tau$. By Proposition 5.1, given any sentence in $\mathcal{L}_\tau$ one can find in an effective way an existential sentence equivalent to it in $T_{r\tan^{-1}}$. Then it suffices to show that the existential theory of $(\overline{\mathbb{R}}, r\tan^{-1})$ is recursively enumerable. To do that, one proceeds as in the proof in [19] of the implication ($4 \Rightarrow 1$) in Theorem 4.6.8, using WSC$_\tau$, Lemma 5.3 and the fact that the rings $M_{n,r}$ are noetherian differential rings.

Conversely, WSC$_\tau$ is a consequence of the decidability of $T_{r\tan^{-1}}$. This can be shown by the same argument as in [14, Sec. 5]. □

Corollary 5.5. *Modulo* WSC$_\tau$ *the theory T_{Log} is decidable for every $G = \mathrm{SU}(n)$, $\mathrm{SO}(n)$, $\mathrm{Sp}(n)$.*

Recall that Schanuel's Conjecture for the complexes states that if $a_1, \ldots, a_n \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then the transcendence degree of $a_1, \ldots, a_n, e^{a_1}, \ldots, e^{a_n}$ over $\mathbb{Q}$, $\mathrm{trdeg}_{\mathbb{Q}}(a_1, \ldots, a_n, e^{a_1}, \ldots, e^{a_n})$, is $\geq n$.

Note that, if $p(\bar{x}, \bar{y}) \in \mathbb{Z}[\bar{x}, \bar{y}]$ with $\bar{x} = (x_1, \ldots, x_n)$ and $\bar{y} = (y_1, \ldots, y_r)$ for $n \geq r$ in $\mathbb{N}$, we can rewrite in $(\overline{\mathbb{R}}, \mathrm{rtan}^{-1})$ the simple term $p(\bar{x}, \tau(x_1), \ldots, \tau(x_r))$ as follows. For $1 \leq j \leq r$, we can assume $x_j \in [0,1]$ and replace $\tan^{-1}(x_j)$ by y_j (with $y_j \in [0, \frac{\pi}{4}]$) and x_j by $\tan(y_j)$ (recall that $\tau(x) = 0$ whenever x is out of $[0,1]$). Then, we use the identity

$$\tan(y) = \frac{e^{iy} - e^{-iy}}{i(e^{iy} + e^{-iy})}.$$

In this way, we transform our simple term of $\mathcal{L}_\tau$ into a term of the form

$$q(e^{iy_1}, \ldots, e^{iy_r}, \bar{z})$$

($\bar{z}$ a new suitable string of variables) with coefficients in $\mathbb{Z}(i)$.

Moreover, note that $i = e^{i\pi/2}$ and that if $n \cdot y = \sum_h n_h \cdot y_h$ with $n \in \mathbb{N}$ and the n_h in $\mathbb{Z}$, then $e^{i(n \cdot y)} = \prod_h e^{i(n_h \cdot y_h)}$.

Let us denote by SC_τ the following statement.

SC_τ: *Let $r_1, \ldots, r_n \in \mathbb{R}$ be linearly independent over $\mathbb{Q}$. Then the transcendence degree over $\mathbb{Q}$ of $\mathbb{Q}(r_1, \ldots, r_n, e^{i \cdot r_1}, \ldots, e^{i \cdot r_n})$ is $\geq n$.*

Clearly this condition directly refers to the general Schanuel's Conjecture for $\mathbb{C}$ and in this sense it is easier to understand than WSC_τ.

Proposition 5.6. *Modulo* SC_τ *the theory $T_{\mathrm{rtan}^{-1}}$ is decidable, whence $T_{\tan^{-1}}$ is decidable and T_{Log} is also decidable for every $G = \mathrm{SU}(n), \mathrm{SO}(n), \mathrm{Sp}(n)$.*

Proof. As in [14], using SC_τ one shows that a recursive subtheory of $T_{\mathrm{rtan}^{-1}}$ is complete. □

Corollary 5.7. SC_τ *implies* WSC_τ.

Proof. Apply Proposition 5.4. □

Acknowledgments

The first and the third authors were supported by the italian PRIN 2009. The first author is also supported by the italian project FIRB 2010. The second author is research director at the "Fonds de la Recherche Scientifique FRS-FNRS" and was partially supported by the CGRI. We thank our anonymous referee for her/his valuable suggestions.

References

AQ: Please cite refs. 1 and 12 in text.

[1] O. Belegradek and B. Zilber, The model theory of the field of reals with a subgroup of the unit circle, *J. London Math. Soc.* (2) 78(3) (2008) 563–579.

We added it ([1]) on page 16. Reference [12] is on page 1, line 32