SCHANUEL'S CONJECTURE AND THE DECIDABILITY OF THE REAL EXPONENTIAL FIELD

A.J. WILKIE
University of Oxford
Mathematical Institute
24–29 St. Giles
Oxford OX1 3LB, UK

In [5] I showed that the theory of the real exponential field, i.e. the theory T_{exp} of the structure $\mathbf{R}_{\mathrm{exp}} := \langle \mathbf{R}; +, \cdot, -, 0, 1, \exp, < \rangle$, is model complete. Subsequently, in the paper[4], Macintyre and I settled, conditionally, an old question of Tarski concerning the decidability of T_{exp}. We showed that if a certain famous conjecture from transcendental number theory, namely Schanuel's conjecture, is true then T_{exp} is, indeed, a decidable theory and in this lecture I am happy to comply with the organizers' suggestion that I explain precisely the rôle played by this conjecture in the verification of the algorithm.

I assume, therefore, that I may take the following (unconditional) proposition on trust. Its proof requires a rather lengthy, and occasionally non-routine, examination of my original model completeness argument.

Proposition
There exists a recursively axiomatized subtheory, T say, of T_{exp} with the property that $T \cup \mathcal{E} \vdash T_{\mathrm{exp}}$, where $\mathcal{E}$ denotes the existential theory of $\mathbf{R}_{\mathrm{exp}}$.

(Perversely, we could not, and still cannot, show unconditionally that T_{exp} has a recursively axiomatized *model complete* subtheory. Such a result would, in any case, have no advantage over the proposition for our present purpose.)

Assuming this proposition, then, it remains for me to show (since T_{exp} is a complete theory) that $\mathcal{E}$ is a recursively enumerable set of $\mathcal{L}(\mathbf{R}_{\mathrm{exp}})$-sentences.

B. T. Hart et al. (eds.), Algebraic Model Theory, 223–230.

Now by the standard tricks (which apply to any expansion *by functions* of the ordered ring structure on $\mathbf{R}$) an arbitrary existential sentence of $\mathcal{L}(\mathbf{R}_{\text{exp}})$ may be effectively put into the form

$$\exists\, x_1 \ldots \exists\, x_n\ p(x_1, ..., x_n, e^{x_1}, ..., e^{x_n}) = 0$$

where $p(x_1, ..., x_n, x_{n+1}, ..., x_{2n})$ is an element of the polynomial ring $\mathbf{Z}[x_1, ..., x_n, x_{n+1}, ..., x_{2n}]$.

We therefore require an effective procedure which, given some $n \geq 1$ and $p(x_1, ..., x_{2n}) \in \mathbf{Z}[x_1, ..., x_{2n}]$ as input (which is clearly effectively codable data), will terminate if and only if the function $\mathbf{R}^n \to \mathbf{R}$, $\langle x_1, ..., x_n \rangle \mapsto p(x_1, ..., x_n, e^{x_1}, ..., e^{x_n})$, which I denote henceforth by F_p, has a zero.

Let us consider the case $n = 1$.

Say $p(x, y) \in \mathbf{Z}[x, y]$, so $F_p(x) = p(x, e^x)$. The Newton Approximation method tells us that if, for some $\alpha \in \mathbf{R}$, $|F_p(\alpha)|$ is small, $|F_p'(\alpha)|$ is not too small and $|F_p''(\alpha)|$ is not too large, then F_p has a nonsingular zero (i.e. a point at which F_p vanishes but its first derivative F_p' does not) close to α.

Now it turns out that the quantitative estimates required here are (a) completely effective and (b) if satisfied by some $\alpha \in \mathbf{R}$ then they are certainly satisfied by some $\alpha \in \mathbf{Q}$. We therefore obtain the following result.

Lemma 1

There is an effective procedure which, given $N \in \mathbf{N}\backslash\{0\}$ and $p(x, y) \in \mathbf{Z}[x, y]$, will terminate and produce $\theta = \theta(N, p) \in \mathbf{N}\backslash\{0\}$ with the property that *if* there exists $\alpha \in \mathbf{Q}$ with $|\alpha| < N$, $|F_p(\alpha)| < \theta^{-1}$ and $|F_p'(\alpha)| > N^{-1}$ *then* F_p has a nonsingular zero (which, in fact, differs from such an α by at most N^{-1}).

(The requirement that $|F_p''(\alpha)|$ be not too large is implied by the condition that $|\alpha| < N$.)

To be able to make use of lemma 1 we of course need to be able to decide effectively, given α, p and N as above, whether or not $|F_p(\alpha)| < \theta^{-1}$ and $|F_p'(\alpha)| > N^{-1}$. That this can be done follows from the next lemma (which I state for arbitrary n) together with the easy observation that given any $p(x, y) \in \mathbf{Z}[x, y]$ one can effectively find $q(x, y) \in \mathbf{Z}[x, y]$ such that $F_p' = F_q$.

Lemma 2

There exists an effective procedure which, given a positive integer n, a polynomial $q(x_1, ..., x_{2n}) \in \mathbf{Z}[x_1, ..., x_{2n}]$ and an n-tuple $\langle \alpha_1, ..., \alpha_n \rangle$ of rational numbers, decides the sign (positive, negative or zero) of the real number $q(\alpha_1, ..., \alpha_n, e^{\alpha_1}, ..., e^{\alpha_n})$.

Proof

With input data as described we can clearly effectively put $q(\alpha_1, ..., \alpha_n, e^{\alpha_1}, ..., e^{\alpha_n})$ (possibly multiplied by a positive real number) into the form

$$\sigma := \sum_{i=0}^{k} a_i e^{i/r}$$

for some $k, r \in \mathbf{N}$, with $r \geq 1$, and $a_0, ..., a_k \in \mathbf{Z}$.

Now since e (and hence $e^{1/r}$) is transcendental it follows that $\sigma = 0$ if and only if $a_0 = ... = a_k = 0$. If $\sigma \neq 0$ then we may approximate σ by rationals (using any standard method, e.g. Taylor series) to successively greater degrees of accuracy, safe in the knowledge that we will eventually trap σ in a rational interval not containing zero. $\square$

Consider now the following algorithm:-

$\mathcal{A}$: On input $p(x,y) \in \mathbf{Z}[x,y]$, at stage i, consider the i^{th} pair, $\langle N, \alpha \rangle$ say, in some fixed enumeration of $(\mathbf{N} \backslash \{0\}) \times \mathbf{Q}$. Calculate $\theta(N,p)$ (cf. lemma 1) and check to see if $|\alpha| < N$, $|F_p(\alpha)| < \theta(N,p)^{-1}$ and $|F_p'(\alpha)| > N^{-1}$ (cf. lemma 2 and the comments immediately preceding it). If yes (to all three checks) halt. Otherwise go on to the $(i+1)^{\text{st}}$ stage.

Clearly the lemmas imply that $\mathcal{A}$ is a recursively enumerable procedure and if it halts on input $p(x,y)$ then F_p has a zero, in fact a nonsingular zero. Conversely, it is very easy to see that if F_p has a *nonsingular* zero then $\mathcal{A}$ halts on input $p(x,y)$. Unfortunately, it may happen that F_p has zeros but that they are all singular. However, we have the following results.

Lemma 3

Let $\alpha \in \mathbf{R}$ and set $I_\alpha = \{q(x,y) \in \mathbf{Z}[x,y] : q(\alpha, e^\alpha) = 0\}$. Then if $\alpha \neq 0$, I_α is a principal ideal of $\mathbf{Z}[x,y]$ (possibly zero). Further, if $q_0(x,y)$ generates I_α and $q_0(x,y) \neq 0$ then α is a nonsingular zero of F_{q_0}.

Proof

Since $\mathbf{Z}$, $\mathbf{Z}[x]$ and $\mathbf{Z}[x,y]$ are unique factorization domains we may use Gauss' lemma freely, and I shall do so below without further mention. Suppose firstly that $\alpha \neq 0$ and that α is algebraic (over $\mathbf{Q}$). Then a theorem of Lindemann (see e.g. [2]) asserts that e^α is transcendental. Thus if $q(x,y) \in \mathbf{Z}[x,y]$ and $q(\alpha, e^\alpha) = 0$ then $q_i(x) \in I_\alpha$ for $i = 0, ..., m$, where $q(x,y) = \sum_{i=0}^{m} q_i(x) \cdot y^i$. It follows that the minimal polynomial (in x) of α

(with relatively prime integer coefficients) generates I_α. If α is transcendental (over $\mathbf{Q}$), then $I_\alpha \cap \mathbf{Z}[x] = \{0\}$ and it again follows (assuming $I_\alpha \neq \{0\}$) that we may take the minimum polynomial (in y) of e^α over $\mathbf{Z}[\alpha]$ (with relatively prime $\mathbf{Z}[\alpha]$ coefficients), and then replace α by x, to obtain a generator for I_α.

Now suppose that $q_0(x,y)$ generates I_α but that α is a singular zero of F_{q_0}. We must show that $q_0(x,y) = 0$.

Choose $q_1(x,y) \in \mathbf{Z}[x,y]$ such that $F'_{q_0} = F_{q_1}$ (cf. the comment before lemma 2). Then $F'_{q_0}(\alpha) = q_1(\alpha, e^\alpha) = 0$, so $q_1(x,y) \in I_\alpha$ and hence $q_1(x,y) = s_1(x,y) \cdot q_0(x,y)$ for some $s_1(x,y) \in \mathbf{Z}[x,y]$. But then $F'_{q_0}(t) = F_{s_1}(t) \cdot F_{q_0}(t)$ (for all $t \in \mathbf{R}$) which, inductively, implies, for all $n \in \mathbf{N}$, $F^{(n)}_{q_0}(t) = F_{s_n}(t) \cdot F_{q_0}(t)$ (for all $t \in \mathbf{R}$) for some $s_n(x,y) \in \mathbf{Z}(x,y]$. However, this implies that $F^{(n)}_{q_0}(\alpha) = 0$ for all $n \in \mathbf{N}$, and hence that F_{q_0} is identically zero (because it is an analytic function). Thus $q_0(t, e^t) = 0$ for all $t \in \mathbf{R}$. However, the exponential function is a transcendental function, so $q_0(x,y) = 0$ as required. □

Corollary 4
Suppose that $\alpha \in \mathbf{R}$, $\alpha \neq 0$, $q(x,y) \in \mathbf{Z}[x,y]$ and that $F_q(\alpha) = 0$. Then α is a nonsingular zero of F_{q_0} for some (irreducible) factor $q_0(x,y)$ of $q(x,y)$.

Proof
Immediate from lemma 3. □

It should now be clear how our algorithm works (still, of course, in the case $n = 1$): given $p(x,y) \in \mathbf{Z}[x,y]$, first evaluate $p(0,1)$ (i.e. $F_p(0)$). If 0 results, halt. Otherwise, factorize $p(x,y)$ (for which algorithms exist, although we only need an enumerative procedure here) and apply algorithm $\mathcal{A}$ simultaneously to each of the (finitely many) factors.

Corollary 4 (and the properties of $\mathcal{A}$) imply that this procedure halts if and only if $\mathbf{R}_{\text{exp}} \models \exists x p(x, e^x) = 0$. Thus we have solved the case $n = 1$ of our problem without having to invoke any unproved conjectures. In fact, most of the above generalizes to the general case. For example, there is a version of Newton's approximation method that works in arbitrary Banach spaces and that can be adapted to give the following result.

Lemma 5
There is an effective procedure which, given $n, N \in \mathbf{N}\backslash\{0\}$ and
$p_1(x_1, ..., x_{2n}), ..., p_n(x_1, ..., x_{2n}) \in \mathbf{Z}[x_1, ..., x_{2n}]$, produces
$\theta = \theta(n, N, p_1, ..., p_n) \in \mathbf{N}\backslash\{0\}$ such that whenever $\alpha_1, ..., \alpha_n \in \mathbf{Q}$, $|\alpha_i| < N$

and $|F_{p_i}(\alpha_1, ..., \alpha_n)| < \theta^{-1}$ (for $i = 1, ..., n$) and

$$\left|\det\left(\frac{\partial F_{p_i}}{\partial x_j}\right)_{1 \leq i,j \leq n} (\alpha_1, ..., \alpha_n)\right| > N^{-1},$$

then there exist $\gamma_1, ..., \gamma_n \in \mathbf{R}$ (with $|\gamma_i - \alpha_i| < N^{-1}$ for $i = 1, ..., n$) such that $F_{p_i}(\gamma_1, ..., \gamma_n) = 0$ for $i = 1, ..., n$ and $\det\left(\frac{\partial F_{p_i}}{\partial x_j}\right)_{1 \leq i,j \leq n} (\gamma_1, ..., \gamma_n) \neq 0$.

Note that the (Jacobian) determinant here can be effectively put into the form F_q for some $q \in \mathbf{Z}[x_1, ..., x_{2n}]$ and so lemma 2, and the comments immediately preceding it, apply equally well here. Also, the fact that lemma 5 refers to (nonsingular) zeros of functions from $\mathbf{R}^n$ to $\mathbf{R}^n$ rather than to zeros of functions from $\mathbf{R}^n$ to $\mathbf{R}$ is dealt with by appealing to the following result. It is a special case of a lemma needed in the paper [5] and I omit its proof which, though not difficult, would distract us too far from our present aim.

Lemma 6

Let $n \in \mathbf{N}$, $n \geq 1$, and $p \in \mathbf{Z}[x_1, ..., x_{2n}]$. Suppose that $F_p(\alpha_1, ..., \alpha_n) = 0$ for some $\alpha_1, ..., \alpha_n \in \mathbf{R}$. Then there exist $p_1, ..., p_n \in \mathbf{Z}[x_1, ..., x_{2n}]$ and $\beta_1, ..., \beta_n \in \mathbf{R}$ such that $F_p(\beta_1, ..., \beta_n) = 0$ *and* the point $\langle \beta_1, ..., \beta_n \rangle$ of $\mathbf{R}^n$ is a *nonsingular* zero of the function $\langle F_{p_1}, ..., F_{p_n} \rangle : \mathbf{R}^n \to \mathbf{R}^n$, i.e. $F_{p_i}(\beta_1, ..., \beta_n) = 0$ for $i = 1, ..., n$ and $\det\left(\frac{\partial F_{p_i}}{\partial x_j}\right)_{1 \leq i,j \leq n} (\beta_1, ..., \beta_n) \neq 0$.

In order to generalize the algorithm that worked in the case $n = 1$ it only remains to generalize corollary 4. In fact, lemma 6 almost does this. The only thing missing is the ability to deduce formally that $F_p(\beta_1, ..., \beta_n) = 0$ from the knowledge that $F_{p_1}(\beta_1, ..., \beta_n) = ... = F_{p_n}(\beta_1, ..., \beta_n) = 0$ (nonsingularly). This would be the case, for example, if we could show that p were in the ideal of $\mathbf{Z}[x_1, ..., x_{2n}]$ generatd by $p_1, ..., p_n$ (just as q is in the ideal generated by q_0 in corollary 4).

With this aim in mind we first observe that, by easy linear algebra, if $\langle \beta_1, ..., \beta_n \rangle$ is a nonsingular zero of the function $\langle F_{p_1}, ..., F_{p_n} \rangle : \mathbf{R}^n \to \mathbf{R}^n$ then $\langle \beta_1, ..., \beta_n, e^{\beta_1}, ..., e^{\beta_n} \rangle$ is a nonsingular zero of the function $\langle p_1, ..., p_n \rangle : \mathbf{R}^{2n} \to \mathbf{R}^n$. (Here, the term 'nonsingular' means that the Jacobian matrix $\left(\frac{\partial p_i}{\partial x_j}\right)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq 2n}}$ has rank n when evaluated at $\langle \beta_1, ..., \beta_n, e^{\beta_1}, ..., e^{\beta_n} \rangle$.)

Elementary differential algebra now tells us that the (field of fractions of the) domain $\mathbf{Z}[\beta_1,...,\beta_n,e^{\beta_1},...,e^{\beta_n}]$ has transcendence degree (over $\mathbf{Q}$) at most n. Now recall that we are trying to show that the ideal of $\mathbf{Z}[x_1,...,x_{2n}]$ consisting of those polynomials that vanish at $\langle\beta_1,...,\beta_n,e^{\beta_1},...,e^{\beta_n}\rangle$ is generated by $p_1,...,p_n$. Actually we will not quite manage this, but even to come close we obviously need to know that there are, essentially, no further polynomial relations holding between $\beta_1,...,\beta_n,e^{\beta_1},...,e^{\beta_n}$. This was guaranteed by Lindemann's theorem in the case $n=1$. For general n we must now introduce Schanuel's conjecture.

Schanuel's Conjecture for R (SC)
Suppose that $n \geq 1$ and that $\gamma_1,...,\gamma_n$ are real numbers linearly independent over $\mathbf{Q}$. Then the field $\mathbf{Q}(\gamma_1,...,\gamma_n,e^{\gamma_1},...,e^{\gamma_n})$ has transcendence degree at least n (over $\mathbf{Q}$).

Corollary of SC
Let $n \geq 1$, $p \in \mathbf{Z}[x_1,...,x_{2n}]$ and consider the function $F_p : \mathbf{R}^n \to \mathbf{R}$. Suppose that (a) it has a zero and (b) if $\alpha_1,...,\alpha_n \in \mathbf{R}$ and $F_p(\alpha_1,...,\alpha_n)=0$ then $\alpha_1,...,\alpha_n$ are linearly independent over $\mathbf{Q}$. Then there exist $\beta_1,...,\beta_n \in \mathbf{R}$ and $q_1,...,q_n,q,s_1,...,s_n \in \mathbf{Z}[x_1,...,x_{2n}]$ such that (1) $\langle\beta_1,...,\beta_n\rangle$ is a zero of F_p and a nonsingular zero of $\langle F_{q_1},...,F_{q_n}\rangle : \mathbf{R}^n \to \mathbf{R}^n$, (2) $\langle\beta_1,...,\beta_n\rangle$ is not a zero of F_q, and (3) $qp = \sum_{i=1}^{n} s_i q_i$ (identically in $x_1,...,x_{2n}$).

Proof
We use the following fact, easily proved by induction on m:-

Let $m,r \geq 1$. Suppose that Q is a prime ideal of $\mathbf{Z}[x_1,...,x_m]$ such that $Q \cap \mathbf{Z} = \{0\}$ and such that (the field of fractions of) $\mathbf{Z}[x_1,...,x_m]/Q$ has transcendence degree r (over $\mathbf{Q}$). Then for some $q \in \mathbf{Z}[x_1,...,x_m]$ with $q \notin Q$, the ideal qQ is generated by $m-r$ elements.

Now by hypothesis (a) of the corollary and the discussion above there exist $\beta_1,...,\beta_n \in \mathbf{R}$ such that $\langle\beta_1,...,\beta_n\rangle$ is a zero of F_p and a nonsingular zero of $\langle F_{p_1},...,F_{p_n}\rangle$ for some $p_1,...,p_n \in \mathbf{Z}[x_1,...,x_{2n}]$, and (hence) the field $\mathbf{Q}(\beta_1,...,\beta_n,e^{\beta_1},...,e^{\beta_n})$ has transcendence degree at most n. Therefore, by (b) and SC, this field has transcendence degree exactly n. It now follows from the fact above (letting $m=2n$, $r=n$ and

$$Q = \{h \in \mathbf{Z}[x_1,...,x_{2n}] : h(\beta_1,...,\beta_n,e^{\beta_1},...,e^{\beta_n}) = 0\})$$

that elements $q,s_1,...,s_n$ and $q_1,...,q_n$ (generating Q) of $\mathbf{Z}[x_1,...,x_{2n}]$ can be found satisfying all the requirements except, possibly, that $\langle\beta_1,...,\beta_n\rangle$ is a *nonsingular* zero of $\langle F_{q_1},...,F_{q_n}\rangle$. However, this easily follows by expressing each qp_i in the form $\sum_{j=1}^{n} s_j^{(i)} q_j$ (note that $p_i \in Q$) for $i = 1, ..., n$, substituting $e^{x_1}, ..., e^{x_n}$ for $x_{n+1}, ..., x_{2n}$, differentiating and, finally, using the fact that $\langle \beta_1, ..., \beta_n \rangle$ is a nonsingular zero of $\langle F_{p_1}, ..., F_{p_n} \rangle$. □

We are now in a position to present the required algorithm, whose correctness the reader can easily verify using the results above. I should also mention the fact, easily established by direct calculation, that a function $\langle F_{q_1}, ..., F_{q_n} \rangle : \mathbf{R}^n \to \mathbf{R}^n$ has a nonsingular zero which is *not* also a zero of F_q if and only if the function $\langle F_{q_1}, ..., F_{q_{n+1}} \rangle : \mathbf{R}^{n+1} \to \mathbf{R}^{n+1}$, where we are regarding $q_1, ..., q_n$ as elements of $\mathbf{Z}[x_1, ..., x_{2n+2}]$ and $q_{n+1}(x_1, ..., x_{2n+2}) := x_{2n+1} \cdot q(x_1, ..., x_{2n}) - 1$, has a nonsingular zero.

The algorithm

Recall that we are given $n \geq 1$ and $p \in \mathbf{Z}[x_1, ..., x_{2n}]$ as input data and we wish to set up a enumerative procedure which will halt precisely if there are $\alpha_1, ..., \alpha_n \in \mathbf{R}$ such that $F_p(\alpha_1, ..., \alpha_n) = 0$. By an obvious reduction argument there is no harm in assuming that (b) (in the statement of the corollary to SC) holds — whether or not (a) does.

So suppose, at stage k say, we are presented with some $q_1, ..., q_n, q, s_1, ..., s_n \in \mathbf{Z}[x_1, ..., x_{2n}]$, $N \in \mathbf{N} \backslash \{0\}$ and $\alpha_1, ..., \alpha_{n+1} \in \mathbf{Q}$ (this being the k'th element of some standard enumeration of all such $(3n+3)$-tuples). We first check that $qp = \sum_{i=1}^{n} s_i q_i$ and, if yes (go on to stage $k+1$ if no), we calculate $\theta = \theta(n+1, N, q_1, ..., q_{n+1})$ (cf. lemma 5 and the remarks above). Now, using the algorithm provided by lemma 2, check to see whether $|\alpha_i| < N$ and $|F_{q_i}(\alpha_i, ..., \alpha_{n+1})| < \theta^{-1}$ (for $i = 1, ..., n+1$) and whether

$$\left| \det \left(\frac{\partial F_{q_i}}{\partial x_j} \right)_{1 \leq i,j \leq n+1} (\alpha_1, ..., \alpha_{n+1}) \right| > N^{-1}.$$

If successful, halt. Otherwise go on to stage $k+1$.

Concluding remarks on Schanuel's conjecture

1. For $n = 1$ SC asserts that if $\alpha \in \mathbf{R}$ and α is linearly independent over $\mathbf{Q}$ — i.e. if $\alpha \neq 0$ — then tr. deg $\mathbf{Q}(\alpha, e^{\alpha}) \geq 1$. This is precisely the theorem of Lindemann used in lemma 3. (Notice, by the way, that the first conclusion of lemma 3 is false if $\alpha = 0$.)
2. Schanuel's conjecture can be (and usually is) formulated over $\mathbf{C}$ and Lindemann's proof still applies, thus settling the case $n = 1$. In fact Lindemann also settled the case for general n when $\alpha_1, ..., \alpha_n$ are all

(complex) algebraic numbers (see [2]). However, all other cases seem to be beyond present methods. Even the substitution of very specific values for α_1, α_2 gives rise to famous unsolved problems, e.g. the transcendence of e^e (set $\alpha_1 = 1$, $\alpha_2 = e$) and the algebraic independence of e and π (set $\alpha_1 = 1$, $\alpha_2 = \sqrt{-1}\pi$).

3. Schanuel also formulated the analogous problem for power series: if $y_1, ..., y_n$ are $\mathbf{Q}$-linearly independent elements of $t\mathbf{C}[[t]]$, is it true that the field $\mathbf{C}(t)(y_1, ..., y_n, \exp(y_1), ..., \exp(y_n))$ has transcendence degree at least n over $\mathbf{C}(t)$? An affirmative answer to this was proved by Ax in [1] and the result has recently been elegantly applied to the model theory of the exponential function. For Bianconi ([3]) has shown that it implies that no nontrivial arc of the sine function can be defined in the structure $\mathbf{R}_{\exp}$.

References

1. J. Ax, *On Schanuel's conjectures*, Ann. Math. **93** (1971), 252–268.
2. A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge 1975.
3. R. Bianconi, *Sine is not definable from Exp in the reals*, preprint.
4. A. Macintyre and A.J. Wilkie, *On the decidability of the real exponential field*, Kreiseliana: About and around Georg Kreisel, A.K. Peters, 1996, pp. 441–467.
5. 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.