RAIRO-Theor. Inf. Appl. **42** (2008) 105–119
DOI: 10.1051/ita:2007048

Available online at:
www.rairo-ita.org

ARITHMETIZATION OF THE FIELD OF REALS WITH EXPONENTIATIONEXTENDED ABSTRACT

Sedki Boughattas[1] and Jean-Pierre Ressayre[1]

Abstract. (1) Shepherdson proved that a discrete unitary commutative semi-ring A^+ satisfies IE_0 (induction scheme restricted to quantifier free formulas) iff A is integral part of a real closed field; and Berarducci asked about extensions of this criterion when exponentiation is added to the language of rings. Let T range over axiom systems for ordered fields with exponentiation; for three values of T we provide a theory $\lfloor T \rfloor$ in the language of rings plus exponentiation such that the models $(A, \exp_A)$ of $\lfloor T \rfloor$ are all integral parts A of models M of T with A^+ closed under $\exp_M$ and $\exp_A = \exp_M \restriction A^+$. Namely $T = \mathrm{EXP}$, the basic theory of real exponential fields; $T = \mathrm{EXP}+$ the Rolle and the intermediate value properties for all 2^x-polynomials; and $T = T_{\exp}$, the complete theory of the field of reals with exponentiation. **(2)** $\lfloor T_{\exp} \rfloor$ is recursively axiomatizable iff $T_{\exp}$ is decidable. $\lfloor T_{\exp} \rfloor$ implies $LE_0(x^y)$ (least element principle for open formulas in the language $<, +, \times, -1, x^y$) but the reciprocal is an open question. $\lfloor T_{\exp} \rfloor$ satisfies "provable polytime witnessing": if $\lfloor T_{\exp} \rfloor$ proves $\forall x \exists y : |y| < |x|^k) R(x, y)$ (where $|y| := \lfloor \log(y) \rfloor$, $k < \omega$ and R is an NP relation), then it proves $\forall x\ R(x, f(x))$ for some polynomial time function f. **(3)** We introduce "blunt" axioms for Arithmetics: axioms which do as if every real number was a fraction (or even a dyadic number). The falsity of such a contention in the standard model of the integers does not mean inconsistency; and bluntness has both a heuristic interest and a simplifying effect on many questions – in particular we prove that the blunt version of $\lfloor T_{\exp} \rfloor$ is a conservative extension of $\lfloor T_{\exp} \rfloor$ for sentences in $\forall \Delta_0(x^y)$ (universal quantifications of bounded formulas in the language of rings plus x^y). Blunt Arithmetics – which can be extended to a much richer language – could become a useful tool in the non standard approach to discrete geometry, to modelization and to approximate computation with reals.

Mathematics Subject Classification. 03H15.

Keywords and phrases. Computation with reals, exponentiation, model theory, o-minimality.

[1] CNRS and Paris 7 University, France; bougatas@logique.jussieu.fr

1. Shepherdson's criterion with exponentiation

1.1. Arithmetizing ordered fields

Let R be a model of the axioms OF of ordered field; an **integral part** of R is a subring A such that for every element x of the field there is a unique element $\lfloor x \rfloor$ of the ring such that $\lfloor x \rfloor < x \leq \lfloor x \rfloor + 1$; $\lfloor x \rfloor$ is called the integral part of x (in A). In general A is not unique; in fact as soon as R is real closed and non archimedean the number of integral parts of R is infinite and large. Nevertheless we sometimes write $A = \lfloor R \rfloor$ to mean that A is an integral part of R. Note that A then satisfies the axioms $DUCR + ED$ of discrete unitary commutative ring + euclidean division (for $\lfloor x/y \rfloor$ is the euclidean quotient of x by y). The converse is true: every model A of $DUCR + ED$ is integral part of a model R of OF – we can take R to be any field in between the fraction field $\mathbb{Q}(A)$ and its Cauchy completion $\mathbb{Q}(A)^c$. We are interested in results of this type, relating extensions of OF with extensions of $DUCR$. We denote $\mathcal{L}$ the language $\{\leq, +, \times, -1\}$ of $DUCR$, tacitly considering $\mathbb{R}, \mathbb{Z}$ as $\mathcal{L}$-structures and not only as sets; henceforth, A tacitly ranges over all models of $DUCR$. We write **rcl** for real closed or real closure and RCF for the theory of rcl fields; remember that RCF axiomatizes the complete theory of $\mathbb{R}$, and is axiomatized by the theory RF of real fields plus the intermediate value scheme IV for all polynomials. IE_0 denotes (the extension of $DUCR$ by) the quantifier free induction scheme of $\mathcal{L}$.

Shepherdson [8] proved that A is a model of IE_0 iff $A = \lfloor R \rfloor$ for some rcl field R – we can take for R the rcl of $\mathbb{Q}(A)$. And Mourgues and Ressayre [3] proved that **every** rcl field has an integral part. Together these results establish a kind of weak duality $A :\longmapsto rcl(\mathbb{Q}(A))$ from IE_0 to RCF and back. We introduce a convenient terminology to discuss results of this kind: if T extends OF then $\lfloor \mathrm{mod}\ T \rfloor$ denotes the class $\{\lfloor R \rfloor; R \text{ satisfies } T\}$; $\lfloor T \rfloor$ denotes the (first order $\mathcal{L}$-) theory of $\lfloor \mathrm{mod}\ T \rfloor$. Thus the preceding result are expressed by: $\lfloor \mathrm{mod}\ T \rfloor = \mathrm{mod}\ \lfloor T \rfloor$ for $T = OF$ and $T = RCF$; and by: $\lfloor OF \rfloor \equiv ED$, $\lfloor RCF \rfloor \equiv IE_0$ (modulo $DUCR$).

Let $\mathcal{L}(...)$ denote $\mathcal{L}$ extended by all function and relation symbols written inside (...); when exp is x^y or a^x ($a > 1$ some constant) we call exp-polynomials the terms of $\mathcal{L}(\exp)$. Berarducci [B] asked for extensions of Shepherdson's criterion when $\mathcal{L}(\exp)$ replaces $\mathcal{L}$. We partially answer his question, keeping the above definition of $\lfloor \mathrm{mod}\ T \rfloor$ and $\mathrm{mod}\ \lfloor T \rfloor$ when $\mathcal{L}(2^x)$ is the language of T while $\mathcal{L}(x^y))$ is the language of $\lfloor T \rfloor$. The reason for choosing 2^x in the first place but x^y in the second one is that for every expansion $(R, 2^x)$ of R which satisfies some basic properties of exponentiation we set $x^y_R := 2^{y \log(x)}$; whereas this kind of relation between x^y and 2^x is not to be expected in $\lfloor (R, 2^x) \rfloor$. Granted this we have to define integral parts $\lfloor (R, 2^x) \rfloor$ so that they come equipped with a function x^y: we say that A is an x^y-integral part of $(R, 2^x)$ (also denoted $(A, x^y) = \lfloor (R, 2^x) \rfloor$) iff $A = \lfloor R \rfloor$ and A^+ is closed under x^y_R; then $x^y_A := x^y_R \restriction A^+$.

Let $T_{\exp}$ denote the complete theory of $(\mathbb{R}, 2^x)$; we prove that $\lfloor \mathrm{mod}\ T_{\exp} \rfloor$ equals $\mathrm{mod}\ \lfloor T_{\exp} \rfloor$ and we axiomatize $\lfloor T_{\exp} \rfloor$. Since every model of $T_{\exp}$ has an x^y-integral part this establishes the same amount of duality between $\lfloor T_{\exp} \rfloor$ and $T_{\exp}$ as do

Shepherdson and Mourgues and Ressayre between IE_0 and RCF. One would like $\llcorner T_{\exp} \lrcorner$ to reduce to $LE_0(x^y)$ (least element scheme for quantifier free formulas of $\mathcal{L}(x^y)$), in analogy with Shepherdson's criterion. Alas $\llcorner T_{\exp} \lrcorner$ implies $LE_0(x^y)$ but the reciprocal is beyond reach; furthermore our axiomatization of $\llcorner T_{\exp} \lrcorner$ is *ad hoc*: it expresses natural properties of reals, not of integers. In contrast Shepherdson's criterion is **not** *ad hoc*: IE_0 is as natural a theory for integers as is IV for reals.

But we are interested in axiomatizations $\llcorner T \lrcorner$ even if they are *ad hoc*: at least they prove that the class of integral parts of models of T is first order; and they are a useful step towards a better axiomatization. In addition we shall prove two other extensions of Shepherdson's criterion with nothing *ad hoc*; they characterize the x^y-integral parts of models of T for $T = \mathrm{EXP}$ – the basic axioms of (real) exponential fields, and for $T = \mathrm{EXP}$ plus $IVR(2^x)$ – which denotes the intermediate value and Rolle properties for all 2^x-polynomials.

1.2. The theory $\llcorner \mathrm{EXP} \lrcorner$

- An exponential **field** – here with exponentiation of base 2 – is a model $(R, 2^x)$ which satisfies the axioms EXP: (i) $2^1 = 2$ and 2^x is a homomorphism of $+$ on (the restriction to positive elements of) $\times$ (ii) 2^x is an ordermorphism such that $2 < x \longrightarrow x^2 < 2^x$ (iii) $\forall x > 0$ $\log(x)$ exists (that is: $\exists y\ 2^y = x$).
- In any such field, x^y denotes $2^{y \log x}$.

Note that the last axiom implies: $y^n < 2^y$ as soon as $n \leq \log(y)$; indeed $y^n \leq y^{\log(y)}$ which for $y = 2^x$ equals $2^{x^2} < 2^y$. It is easy to prove that $\llcorner \mathrm{mod\ EXP} \lrcorner = \mathrm{mod}\ \llcorner \mathrm{EXP} \lrcorner$ and to axiomatize $\llcorner \mathrm{EXP} \lrcorner$: one provides a first, roundabout axiomatization of $\llcorner \mathrm{mod\ EXP} \lrcorner$; it begins with EXP^- which is EXP without its last axiom (of existence of $\log(x)$). Note that in the present context of $\llcorner \mathrm{EXP} \lrcorner$ we think of the quantifiers as ranging over the integers, no longer the reals. This applies also to the next axiom although it is the "exponentiation of fractions" denoted $\llcorner E \lrcorner$:

$$(\forall p, q, x > 0)(\exists a, b > 0)\ |2^p - (a/b)^q| < 1/x.$$

This axiom implies that inside $\mathbb{Q}(A)$ the cut $2^{p/q} := \{a/b | (a/b)^q < 2^p\}$ is a Cauchy cut; so that it defines $2^{p/q}$ as an element of $\mathbb{Q}(A)^c$. The function 2^x is thus defined as a map from $\mathbb{Q}(A)$ into its Cauchy completion; and by the usual argument, this map has an extension sending the totality of $\mathbb{Q}(A)^c$ to $\mathbb{Q}(A)^c$. Then for every sentence ϕ of EXP there is an "**fc-translation of** ϕ", that is: a sentence ϕ^{fc} of $\mathcal{L}(x^y)$ which is true in (A, x^y) iff $(\mathbb{Q}(A)^c, 2^x)$ satisfies ϕ (the superscript fc is chosen in reference to "**C**ompletion of the **F**raction field of A"; such an fc-translation is easy to provide in the present case $\phi \in \mathrm{EXP}$ but it is more complicated than ϕ and it exists only when ϕ is simple enough). Here is our first axiomatization of $\llcorner \mathrm{EXP} \lrcorner$:

- $DUCR + ED + \mathrm{EXP}_- + \llcorner E \lrcorner$,
- EXP^{fc} ($:= \{\phi^{fc}; \phi \in \mathrm{EXP}\}$, the fc-translation of EXP).

This system is an *ad hoc* way to express that (A, x^y) is an x^y-integral part of a model of EXP; but we can reduce it to natural axioms.

Theorem 1. $\lfloor \mathrm{EXP} \rfloor$ *is axiomatized by the following system* $\mathcal{A}_0$*, where all variables tacitly range over positive elements:*

- *ED and* $\exists a, b\ |b^q 2^p - a^q| < 1/x$.
- $x^{y+z} = x^y x^z, x^{-y} x^y = 1$*;* $x^{yz} = (x^y)^z$*;* x^y *strictly increasing with respect to* $x, y > 1$.
- $2 < x \longrightarrow x^2 < 2^x$.
- $\exists y\ 2^y \leq z < 2^{y+1}$*;* $\exists x\ x^z \leq 2^y < (x+1)^z$*;* $\exists y\ 2(x^y) < (x+1)^y$*;* $\exists x\ (x+1)^y < 2(x^y)$.

Here we skip the proof of this theorem, which is lengthy but along familiar lines.

1.3. The theory $\lfloor IVR(2^x) \rfloor$

For a number of other extensions T of OF a systematic and direct fc-translation T^{fc} of T exists, which is heavy but straightforward. It proves that $\lfloor \mathrm{mod}\ T \rfloor = \mathrm{mod}\ \lfloor T \rfloor$; the axiomatization T^{fc} that it provides of $\lfloor \mathrm{mod}\ T \rfloor$ is *ad hoc* but is often a step towards a better one. For instance RCF is axiomatized by IV (over RF), and IV^{fc} is not hard to write down; it is an axiomatization of $\lfloor RCF \rfloor$ – *ad hoc* but which can be finally reduced to IE_0. In the same way it will be easy to provide $IVR(2^x)^{fc}$; it proves the existence of $\lfloor IVR(2^x) \rfloor$ and provides an *ad hoc* axiomatization – but a nice argument does better:

Theorem 2. *Over* $\lfloor \mathrm{EXP} \rfloor$ *the theory* $\lfloor IVR(2^x) \rfloor$ *is axiomatized by* $LE_0(2^x)$ *– least element scheme for quantifier free formulas of* $\mathcal{L}(2^x)$ *with fractional parameters.*

The allowance for **fractional** parameters in the scheme $LE_0(2^x)$ needs to be made precise; it is easy to provide for every open formula $\phi(\bar{x}, X) \in \mathcal{L}(2^x)$ a formula $\phi(\bar{x}, \bar{y}, X)^{fc} \in \mathcal{L}(x^y)$ such that we have for all $\bar{b}, \bar{d}, X$ in A: $[\mathbb{Q}(A)^c, 2^x)$ satisfies $\phi(b_1/d_1, ...b_k/d_k, X)]$ iff (A, x^y) satisfies $\phi(\bar{b}, \bar{d}, X)^{fc}$. And $LE_0(2^x)$ denotes ($\lfloor \mathrm{EXP} \rfloor$ plus) the least element axiom for the formula $\phi(\bar{b}, \bar{d}, X)^{fc}$ – when $\phi(\bar{x}, X)$ ranges over the quantifier free formulas of $\mathcal{L}(2^x)$:

$$\exists X \phi(\bar{b}, \bar{d}, X)^{fc} \longrightarrow \exists \min\ X : \phi(\bar{b}, \bar{d}, X)^{fc}.$$

A difference between Theorem 2 and Shepherdson's criterion is that the latter uses the induction scheme IE_0 which is *a priori* weaker than the least element scheme LE_0: in fact $LE_0(E)$ implies $IE_0(E)$ in any extended language $\mathcal{L}(E)$, but the converse implication is not true in general. Still $LE_0(E)$ is true in the case below; we start to often write $R_{\exp}$ and $A_{\exp}$ in place of $(R, 2^x)$ and (A, x^y).

Proposition 3.

(a) $LE_0(x^y)$ holds in every x^y-integral part of every model of $T_{\exp}$.

(b) If $R_{\exp}$ satisfies EXP + $IVR(2^x)$ *then $LE_0(2^x)$ holds in every 2^x-integral part of R.*

Proof of Proposition 3.

(a) Let $R_{\exp}$ be a model of $T_{\exp}$; Wilkie [10] proved that $T_{\exp}$ is an o-minimal theory hence $\mathcal{R}_{\exp}$ is an o-minimal structure. That is: if $\Phi(x)$ is any formula of $\mathcal{L}(2^x)$ with parameters in R then the interpretation of $\Phi(x)$ in $R_{\exp}$ is a finite union of intervals with endpoints $a_i, b_i \in R \cup \{-\infty, +\infty\}$. Thus if $A = {\llcorner} R {\lrcorner}$ then $\min\ x \in A : \Phi(x)$ can only be one of the following elements:

$$a_i \text{ (in a case where } a_i = {\llcorner} a_i {\lrcorner} \in A);\ {\llcorner} a_i {\lrcorner} + 1;\ \text{or } {\llcorner} b_i {\lrcorner}.$$

Hence the conclusion when $\Phi(x)$ expresses (with the help of $2^{y \log(x)}$) an $E_0(x^y)$ formula.

(b) Let (A, x^y) be a 2^x-integral part of a model $R_{\exp}$ of EXP + $IVR(2^x)$; by a result of van den Dries [9] every non trivial 2^x-polynomial has but a finite number of roots in $(R, 2^x)$. This allows to prove for every quantifier free formula $\Phi(x) \in \mathcal{L}(2^x)$ that the interpretation of $\Phi(x)$ in $R_{\exp}$ is a finite union of intervals with endpoints $a_i, b_i \in R \cup \{-\infty, +\infty\}$. The end of the proof is the same as for (a). □

Proof of Theorem 2.

One direction of the theorem is established by (b) of the preceding proposition.

Conversely we consider a model (A, x^y) of EXP + $LE_0(2^x)$ and we set up to prove that $(\mathbb{Q}(A)^c, 2^x)$ satisfies $IV(2^x)$. Given a 2^x-polynomial $P(\bar{x}, Y)$ and given $\bar{x} \subset \mathbb{Q}(A)^c$ suppose $P(\bar{x}, a) > 0 > P(\bar{x}, b)$; we want a zero of P between a and b. We first assume $\bar{x} \subset \mathbb{Q}(A)$; an induction on the length of the 2^x-polynomial $P(\bar{x}, Y)$ derives from EXP the uniform continuity of $P(\bar{x}, Y)$ for fixed $\bar{x}$ and when Y ranges over $[a, b]$. Thus given $\epsilon > 0$ in $\mathbb{Q}(A)$ we can find $N \in A$ such that the variation of $P(\bar{x}, Y)$ is less than ϵ on every subinterval of $[a, b]$ of length $(b-a)/N$; hence on $[c_i, c_{i+1}]$ where $c_i := a + (b-a)i/N$. We can be sure that on one of these intervals $P(\bar{x}, Y)$ changes its sign – otherwise a contradiction with $IE_0(2^x)$ is easily reached. Assume that A is countable and choose a sequence $(\epsilon_n), n < \omega$ with limit 0 in $\mathbb{Q}(A)$. By iterating for each $n < \omega$ the preceding fact applied with $1/N \leq \epsilon_n$ and with $[a_n, b_n]$ in place of $[a, b]$ we obtain a decreasing chain of subintervals $[a_n, b_n]$ of $[a, b]$ which tends to an element $r \in \mathbb{Q}(A)^c$, such that on the interval $[a_n, b_n]$, $P(\bar{x}, Y)$ changes sign and its variation is less than ϵ_n. Thus r is a root of $P(\bar{x}, Y)$ and $IV(2^x)$ is proved – for fractional parameters only; but by proving the uniform continuity of $P(\bar{x}, Y)$ on every finite $k+1$-dimensional box we extend the result to arbitrary "real" parameters. Note that only $IE_0(2^x)$ has been used; but we need a similar argument – omitted in present version – to prove the Rolle scheme; and it is there that we use $LE_0(2^x)$. □

1.4. The theory $\llcorner T_{\exp} \lrcorner$

Let $M_{\exp}$ be a model of $T_{\exp}$ and $A_{\exp}$ an x^y-integral part of $M_{\exp}$; in a unique way we can identify M with a subfield of $(\mathbb{Q}(A)^c$ and then $M_{\exp} \subset (\mathbb{Q}(A)^c, 2^x) = (M_{\exp})^c$. In addition and because $T_{\exp}$ is o-minimal $M_{\exp}$ satisfies a continuous cell decomposition property of its definable functions which implies that $M_{\exp}$ is an elementary submodel of $(M_{\exp})^c$. Thus $(\mathbb{Q}(A)^c, 2^x)$ is a model of $T_{\exp}$; hence we could axiomatize $\llcorner T_{\exp} \lrcorner$ by $\llcorner \mathrm{EXP} \lrcorner + T_{\exp}^{fc}$ if a direct fc-translation existed for $T_{\exp}$. This is definitely not the case; however there exists an axiomatization $\mathcal{A}$ of $T_{\exp}$ which consists of sentences ϕ simple enough for ϕ^{fc} to exist – thus:

Theorem 4. *$\llcorner T_{\exp} \lrcorner$ exists and is axiomatized by $\llcorner \mathrm{EXP} \lrcorner + \mathcal{A}^{fc}$.*

The proof of Proposition 3(a) shows that $\llcorner T_{\exp} \lrcorner$ implies $LE_0(x^y)$. But the reciprocal is an open question; it could hold if a highly remarkable phenomenon took place in $(\mathbb{R}, 2^x)$: non singular **systems** of 2^x-algebraic equations should reduce to **single** such equations, in a **uniform** way (that is in every model of $T_{\exp}$ in addition to $(\mathbb{R}, 2^x)$). Although this is the analog of a basic property of real algebraic closure, it is very demanding... In view of this uncertainty it is interesting to have a subtheory T of $T_{\exp}$, as strong as we are able to find and for which we know a natural axiomatization of $\llcorner T \lrcorner$; this is what S.I.C. already provided with $T = IVR(2^x)$.

The axiomatization $\mathcal{A}^{fc}$ that we shall give of $\llcorner T_{\exp} \lrcorner$ is *ad hoc*, but the theory $\llcorner T_{\exp} \lrcorner$ itself is definitely not an *ad hoc* one. The first way to see it is to consider a second order form $T_{\exp} + IP(x^y)$ of $\llcorner T_{\exp} \lrcorner$, which is natural:

- Let $IP \subset \mathcal{L}(A(x))$ with $A(x)$ predicate symbol denote the obvious axioms which are satisfied by (R, A) iff $A = \llcorner R \lrcorner$.
- More generally, for any function $f = f(\bar{x}))$ over the reals $IP(f)$ adds to IP that A^+ is closed under f.

We can regard $OF + IP(f)$ as a second order arithmetic of some kind: the elements x of the field are the "reals" or second order objects; among them the "integers" or first order objects are the elements of A – these integers form an f-integral part of these reals. In the sequel a formula of $\mathcal{L}(A(x), ...)$ is called first order if all its quantifiers are restricted to $A(x)$; whereas a second order formula has also quantifiers ranging over the whole field. Note that formulas with no occurrence of the symbol $A(x)$ have all their quantifiers ranging over the reals – we call them **pure** second order; and we denote L^2 the least element scheme asserted for all formulas of the form $A(x)$ *and* $\phi(x, \bar{u})$ where $\phi(x, \bar{u})$ is pure second order. The first order, arithmetical part $IP(x^y)$ of the theory $T_{\exp} + IP(x^y)$ looks rather limited but any way one kind or another of drastic restriction is necessary on a theory $\llcorner T \lrcorner$ of Arithmetics if we want it to correspond to a well behaved theory like $T = T_{\exp}$; for $T_{\exp}$ has excellent algebraic properties while Arithmetics cannot avoid Goedel's incompleteness theorem and Tennenbaum's theorem of non existence of recursive non-standard models. And notwithstanding the limited character of $IP(x^y)$,

the whole scheme L^2 is consequence of $T_{\exp} + IP(x^y)$ – as established by the above proof of Proposition 3(a).

Now comes the promised axiomatization $\mathcal{A}$ of $T_{\exp}$ such that $\mathcal{A}^{fc}$ exists – hence axiomatizes $\lfloor T_{\exp} \rfloor$ and proves $\lfloor \bmod T_{\exp} \rfloor = \bmod \lfloor T_{\exp} \rfloor$. Let $e(x)$ stand for $2^x \restriction]0,1[$ and let $\mathbb{R}_e, \mathcal{L}_e, T_e$ denote $(\mathbb{R}, e(x))$, its language and its complete theory; we shall first provide an axiomatization $\mathcal{A}_e$ of T_e such that $\mathcal{A}_e^{fc}$ exists.

Let $t(\bar{X}, Y) = t$ be a real function;

- Assume that t is $\mathcal{C}^\infty$ with arguments ranging over $[0,1]$) and for each $\bar{x}y \in [0,1]^{k+1}$ that

$$t(\bar{x}, 0) > 0 > t(\bar{x}, 1) \text{ and } t'_Y(\bar{x}, y) < 0;$$

  then f_t denotes the function of domain $]0,1[^k$ defined by

$$0 < f_t(\bar{x}) < 1 \text{ and } t(\bar{x}, f_t(\bar{x})) = 0.$$

  Otherwise $f_t := 0$.
- We denote $\overline{t/Y}$ the function t/Y extended by continuity to $Y = 0$ and restricted to $]0,1[^k \times]-1/2, 1/2[$ – in case this function is $\mathcal{C}^\infty$ on $[0,1]^k \times [-1/2, 1/2]$; $\overline{t/Y} := 0$ otherwise.
- We let $\mathcal{J}$ denote the closure of $\mathcal{L}_e$, $1/X$ and $X^{1/p}$ $(1 < p < \omega)$ under composition and under the operations: $t \longmapsto f_t$, $t \longmapsto \overline{t/Y}$ (t a term of $\mathcal{J}$).

Theorem 5.

(a) Every $f \in \mathcal{J}$ is $\mathcal{C}^\infty$ with open domain and there is a polytime (:= polynomial time computable) algorithm which for every x in the domain of f produces the bits of $f(x)$.
(b) Every 0-definable function $f \in \mathbb{R}_e$ is piecewise in $\mathcal{J}$ (:= $\forall \bar{x} \bigvee_{t \in F} f(\bar{x}) = t(\bar{x})$ for some finite set $F \subset \mathcal{J}$).
(c) T_e is axiomatized by $\mathcal{A}_e := \forall(\mathbb{R}_e) + (\forall x \neq 0)\exists y\ xy = 1$ plus the defining axiom of every function f_t or $\overline{t/Y}$ of $\mathcal{J}$; where $\forall(\mathbb{R}_e)$ denotes the universal theory of $\mathbb{R}_e$.
(d) For any axiomatization $\mathcal{A}$ of T_e, $\mathrm{EXP} + \mathcal{A}$ is an axiomatization of $T_{\exp}$.
(e) For every $\phi \in \mathcal{A}_e$ there is a sentence ϕ^{fc} which naturally expresses in the structure $A_{\exp}$ that $(\mathbb{Q}(A)^c, e(x))$ satisfies ϕ.

Proof of Theorem 5. See [7] for (a); see [5] for (b,c) and [6] for (d); the proof of (e) is an exercise. □

Let $A_{\exp}$ be an x^y-integral part of an exponential field $R_{\exp}$; then $e(x)$ is definable in $R_{\exp}$ and from (c+e) follows that R_e satisfies T_e iff $A_{\exp}$ satisfies $\mathcal{A}_e^{cf}$. Then from (d) follows that $\lfloor T_{\exp} \rfloor$ exists and is axiomatized by $\mathcal{A}_0 + \mathcal{A}_e^{cf}$.

The definition of $\overline{t/Y}$ hence of $\mathcal{J}$ is not effective. The second author has a variant $\mathcal{J}^1$ of $\mathcal{J}$ which still satisfies Theorem 5 and in addition is recursively

presentable – see [7]. But Rambaud's $\mathcal{J}$ though not known to be effective is simpler than $\mathcal{J}^1$ in some ways.

So far we considered arithmetizations $\lfloor T \rfloor$ of a theory $T \supset OF$ which are "true" – in the **standard** model $(\mathbb{Z}, x^y \restriction \mathbb{Z}^+)$. But it is rewarding to allow for the consideration of arithmetizations $\ulcorner T \urcorner$ which are false and thus simpler.

1.5. Blunt Arithmetics $\ulcorner T \urcorner$

Blunt Arithmetics begins with the idea of adding the false but not so contradictory axiom: "**every real is a fraction**" (or even: is a **dyadic** number). This idea can be made precise in diversely encompassing ways; here we only consider the case of $\mathcal{L}(\exp)$. Call **blunt exponentiation** the axiom $\ulcorner E \urcorner :=$

$$(\forall p, q > 0)(\exists a, b > 0)\ 2^p = (a/b)^q;$$

note that if (A, x^y) satisfies $\ulcorner E \urcorner$ then the fraction a/b can be taken as the value of $2^{p/q}$ and this yields a function 2^x on $\mathbb{Q}(A)^+$, such that $(\mathbb{Q}(A), 2^x)$ is interpretable in (A, x^y). Thus for **every** formula $\phi \in \mathcal{L}(2^x)$ there is an "f-translation" $\varphi^f \in \mathcal{L}(x^y)$ which expresses in (A, x^y) that $(\mathbb{Q}(A), 2^x)$ satisfies ϕ; this is much better than the fc-translation. And for every system $T \subset \mathcal{L}(2^x)$ extending EXP, the "blunt form" $\ulcorner T \urcorner$ of $\lfloor T \rfloor$ (or "blunt arithmetization of T") is axiomatized by $\ulcorner E \urcorner$ together with T^f. This axiomatization T^f is clearly *ad hoc*, but often better axiomatizations of the same theory may be found to replace it. To begin with: $\ulcorner E \urcorner + \mathrm{EXP}^f$ axiomatizes $\ulcorner \mathrm{EXP} \urcorner$; it reduces to $\ulcorner E \urcorner + \mathcal{A}_0$ which is no longer *ad hoc*.

Blunt axiom systems are not true except in the simplest case $\ulcorner OF \urcorner = \lfloor OF \rfloor \equiv DUCR + ED$; but they can be **conservative** for $\forall\Delta_0(x^y, ...)$ sentences over true systems of Arithmetic. Then in order to deal with many questions they are usable in place of more complicated true systems. In particular we will prove

Theorem 6. *$\ulcorner T_{\exp} \urcorner$ is a conservative extension of $\lfloor T_{\exp} \rfloor$ for $\forall\Delta_0(x^y)$ sentences.*

Lemma 7. *For every model Z of $\lfloor T_{\exp} \rfloor$ there is a model $\mathcal{Z}$ of $\ulcorner T_{\exp} \urcorner$ such that Z^+ is initial segment of $\mathcal{Z}^+$.*

Proof of Lemma 7 $\longrightarrow$ Theorem 6. Assume that ϕ is a $\forall\Delta_0(x^y)$ consequence of $\ulcorner T_{\exp} \urcorner$ in $\mathcal{L}$ and Z is a model of $\lfloor T_{\exp} \rfloor$; we have to prove that Z satisfies ϕ (relativized to Z^+). Indeed, by the above lemma (a) we have a model $\mathcal{Z}$ of $\ulcorner T_{\exp} \urcorner$ hence of its consequence ϕ; more precisely it is $\mathcal{Z}^+$ which satisfies ϕ. And since ϕ is a $\forall\Delta_0(x^y)$ formula it remains true under restriction to the initial segment Z^+. Conservativity is proved. □

The proof of the lemma rests on the use of **transfinite** series called **transseries**. This requires the development of a whole technology which is exposed in Section 3. Therefore the proof of Lemma 7 and Theorem 6 is to be finished in that section.

2. Polytime witnessing – Existence of Integral parts

2.1. **A) Provable polytime witnessing**

In this subsection $|x|$ stands for $\lfloor \log(x) \rfloor$ – so $2^{|x|} \leq x < 2^{|x|+1}$; Buss calls **sharply bounded** the quantifications that are bounded by $|t|$ for some $t \in \mathcal{L}(x^{|y|})$, and uses $\forall^b, \exists^b$ to denote them. Then Δ_0^b denotes the class of sharply bounded formulas of $\mathcal{L}(\lfloor x/2 \rfloor, |x|, x^{|y|})$, Σ_1^b denotes the closure of Δ_0^b under bounded existential quantification and sharply bounded universal quantification. It has the effect that the class NP consists of the Σ_1^b definable sets. Provable polytime witnessing for an Arithmetics T is the property: if T proves for all (positive) x that $(\exists y : |y| < |x|^k)\phi(x, y)$ where $\phi \in \Sigma_1^b$, then there is a polytime function f such that $\forall x \phi(x, f(x))$ is provable in T.

Theorem 8. *Provable polytime witnessing holds for $T = T_{\exp} + IP(x^y)$ (hence for $\lfloor T_{\exp} \rfloor$ and $\lceil T_{\exp} \rceil$).*

As a corollary of this theorem, every set which is NP inter co-NP provably in $T_{\exp} + IP(x^y)$ reduces to P in the same provable manner; and **if** it turned out **(surprisingly!)** that $T_{\exp} + IP(x^y)$ proves the set of primes to be NP, then factorisation would be in polytime. Thus it is interesting to know whether or not $T_{\exp} + IP(x^y)$ proves the set of primes to be NP; in this context [1] proved that primes are **not** provably NP in $T_{\exp} + IP(2^x)$. But the proof is hard and we do not know whether its method can be extended to the case of $IP(x^y)$.

Provable polytime witnessing has been proved by Buss for S_2^1 – where S_2^1 is the Arithmetics consisting of the basic $\forall$-axioms for $\mathcal{L}(\lfloor x/2 \rfloor, |x|, x^{|y|})$, together with Σ_1^b-induction on the interval $[0, |x|]$ for every x. In two different (even "orthogonal") ways, both $\lfloor T_{\exp} \rfloor$ and S_2^1 are quite weak: on the one hand S_2^1 does not prove 2^x to be total (because by Parikh's theorem every provable function of S_2^1 is bounded by a term in $x^{|y|}$); and on the other hand $\lfloor T_{\exp} \rfloor$ does not imply any significant amount of induction for quantified formulas. Thus one could fear that provable polytime witnessing holds for these two theories only because they are not rich enough: because the results of the form $\forall x(\exists y : |y| < |x|^k)\phi(x, y)$ with $\phi \in \Sigma_1^b$ which they manage to prove all are trivial. Things are not negative to that point. To begin with, T-provable witnessing is significant even if T is weak: of course, the weaker T is, the weaker also is the witnessing property; **but the stronger is** the fact that T **suffices** to prove this property. Moreover for S_2^1, witnessing is remarkable because S_2^1 captures the whole class polytime: a function is polytime iff its graph has a Σ_1^b definition $\Phi(x, y)$ for which S_2^1 proves $\forall x \exists y \Phi(x, y)$. For $\lfloor T_{\exp} \rfloor$, witnessing is remarkable because $\lfloor T_{\exp} \rfloor$ captures – in a sense appropriate to functions over the reals – the class of all 0-definable functions of $\mathbb{R}_{\exp}$.

Our proof of polytime witnessing for $\lfloor T_{\exp} \rfloor$ comes along with a more precise result; denote J the closure under composition of J_0 where J_0 is made of $\lfloor x/y \rfloor, \lfloor X.\log(x) \rfloor$, $x^{|y|}$ and $\lfloor X.f_t(x_1/y_1, ..., x_k/y_k) \rfloor$ for each $t(\bar{x}, Y) \in \mathcal{J}$. Clearly every $f \in J$ is provably total (on the integers) in $T_{\exp} + IP(x^y)$.

Theorem 9.

(a) For every function $f \in J$ there is $n < \omega$ and a polytime algorithm which computes a set $F(\bar{x})$ of cardinal $< n$ such that $f(\bar{x}) \in F(\bar{x})$.

(b) (J-witnessing) If $T_{\exp} + IP(x^y)$ proves $\forall x(\exists y : |y| < |x|^k)\varphi(x,y)$ where $k < \omega, \varphi \in \Sigma_1^b$ then $T_{\exp} + IP(x^y)$ proves $\forall x \vee_{t \in F} \varphi(x, t(x))$ for some finite subset F of J.

Proof of Theorem 9(a). Note that (a) is true even with $n = 1$ for each polytime f hence it is true for each $f \in J_0$ which are not of the form $f = \lfloor X.f_t(x_1/y_1, ..., x_k/y_k) \rfloor$. In view of the latter case we observe that (i) whenever a real y is computed in polytime then in this time too it is easy to compute $a < \omega$ such that $y \in [a, a+1]$ hence $\lfloor y \rfloor$ equals a **or** $a+1$; (ii) however the exact value of $\lfloor y \rfloor$ may be undecidable because of the possibility $y = a + 1$. Because the real functions f_t are polytime computable, point (i) applied to $y = f(\bar{x})$ yields that if $f = \lfloor X.f_t(x_1/y_1, ..., x_k/y_k) \rfloor$ then (a) still holds true (but this time with $n > 1$); and thus (a) finally holds for each $f \in J_0$ hence for each $f \in J$. (Point (ii) explains why we do not strengthen (a) by claiming that J_0 and J are polytime; it is also the reason why the proof of Lem 11 below is not more straightforward). □

As a corollary of Theorem 9 every function which provably in $T_{\exp} + IP(x^y)$ is Σ_1^b definable **and** polynomially bounded in size belongs piecewise to J. And provable polytime witnessing for $T_{\exp} + IP(x^y)$ is another corollary. Thus in order to conclude Theorems 8 and 9 there remains to prove J-witnessing.

Lemma 10. *Assume that $(\mathcal{R}, \mathcal{Z}, 2^x)$ is a model of $T_{\exp} + IP(x^y)$ and A is a subring of $\mathcal{Z}$ which is closed under the interpretation in $(\mathcal{R}, \mathcal{Z}, 2^x)$ of each $f \in J$. Let x_A^y denote $x_{\mathcal{Z}}^y$ restricted to $x \in A$ and to $y \in A$ such that $(\exists b \in A) 2_{\mathcal{Z}}^y < b$; there exists a model $(R, Z, 2^x)$ of $T_{\exp} + IP(x^y)$ such that A^+ is an initial segment of Z^+ and $x_A^y \subset x_Z^y$.*

Proof of Lemma 10 $\longrightarrow$ J-witnessing. Similar to the proof in S. I.E that Lemma 7 implies Theorem 6. □

The next result keeps the assumptions of the preceding lemma and begins the construction of its promised field R. We denote $A_{\exp}$ the expansion of A by the above partial function $\exp_A$; inside $A_{\exp}$ we can define a function $e(x)_A$ on $\mathbb{Q}(A)^c \cap]0, 1[$ – by the method used for 2^x in Section 1.2.

Lemma 11. *There exists a model K_e of T_e such that $A = \lfloor K \rfloor$ and the function $e(x)_A$ agrees with $e(x)_K$.*

Proof of Lemma 11. Set $D = \mathbb{Q}(A) + o_A$; $A = \lfloor \mathbb{Q}(A) \rfloor = \lfloor D \rfloor$ since A satisfies ED. Note that inside $\mathbb{Q}(A)^c$, for each x the limit for $X \in A^+$ of $\lfloor X.x \rfloor / X$ converges to x. With few additional remarks this allows to prove that

i) D is closed under $\mathcal{J}^-$ – where $\mathcal{J}^-$ is defined as $\mathcal{J}$ except that $1/X$ is taken away;

ii) in addition $D \backslash o_A$ is closed under $1/X$.

Set $K^0 := \mathrm{Def}(0)$ where Def means definable closure inside $\mathcal{R}_{\exp}$.

Claim. $K^0 \subset D$.

Proof of Claim. We have $A_0 \subset D$ where $A_0 := \{0\}$; then by (i) $A_1 \subset D$ where $A_1 := \mathcal{J}^-$ closure of A_0. Next because K^0 is archimedean and closed under $1/X$ we have that (ii) implies $A_2 \subset D$ where $A_2 :=$ closure of A_1 under $1/X$. Repeating this ω times we finally obtain $K^0 \subset D$ since K^0 is by T 5.b the closure of $\{0\}$ under $\mathcal{J}^-$ and $1/X$. □

Let K^1 be maximal among the definably closed subfields of $\mathcal{R}_{\exp}$ which are included in D; K^1 is non empty: by the claim it includes K^0. Assume that $c \in D \backslash K^1 + o_A$; then by (ii) $K^1(c)$ is included in D. By a general theorem of o-minimality due to vd Dries, the fact that $\mathbb{R}_e$ is polynomially bounded and K^1 is definably closed in $\mathbb{R}_e$ implies that $K^1(c)$ remains cofinal in Def $K^1(c)$. Then from $K^1(c) \subset D$ follows Def $K^1(c) \subset D$ by a proof similar to that of the Claim. By contradiction we just proved that $K^1 + o_A = D$; thus every element $a \in A$ is A-infinitely close to a unique element a^* of K^1. The map : $a \longmapsto a^*$ is a ring isomorphism up to o_A from A into K^*, and $o_A \cap K^*$ reduces to 0 hence the map is an embedding. Denote A^1 the image of this map; A^1 satisfies the desired conclusion of Lemma 11 (with K^1 in place of K). And since A is isomorphic to A^1, Lemma 11 is proved. □

The next step is to extend the pair (K, A) of L 11 to (R, Z) satisfying: $T_{\exp} + IP(x^y)$ and A^+ initial segment of Z^+; to that end R will be constructed from "transseries" – and this will be exposed in Section 3.

2.2. Integral parts

We recall prior work relevant to the present one:

Theorem 12.
(a) Every rcl field has an integral part.
(b) Every rcl exponential field has a 2^x-integral part.
(c) Every model of $T_{\exp}$ has an x^y-integral part.
(d) In the case of countable structures we can require that the integral parts constructed in (a)–(c) be blunt.

Again the proof of this theorem is based on transseries. Most of it appeared in [6] but one last part was only stated there; it will appear in the full version of the present paper.

To every model A of $\llcorner RCF \lrcorner \equiv IV$ is canonically associated a rcl field, namely rcl $\mathbb{Q}(A)$. For this correspondence to resemble a duality between models of $\llcorner RCF \lrcorner$ and RCF one wants to associate to every rcl field R an integer part $\llcorner R \lrcorner$. This is indeed what (a) of the theorem does; only the "duality" is a weak one since the $\llcorner R \lrcorner$ associated to R in this way is by no means unique. Thus we have a one-many correspondence: $R \longmapsto \llcorner R \lrcorner$ where a true duality would have a canonical map; but this problem depends for its solution on ideas that are outside the scope of this paper. Meanwhile, part (a) of the above theorem is a welcome complement to Shepherdson's criterion; and part (c) is the perfect analog of (a) when exp is added to the language.

3. Transseries and the final proofs

Definition.

- *We call* **group of monomials** *every ordered commutative group* Γ *denoted multiplicatively.*
- *We denote* $K((\Gamma))$ *the set of formal series of the form* $\Sigma_{i<\alpha} a_i \gamma_i$ *where* α *is any ordinal,* $a_i \in K$ *and* γ_i *strictly decreases in* Γ*; Hahn proved that on* $K((\Gamma))$ *there is a natural definition of* $=, +, \times, <$ *which turns it to an ordered field also denoted* $K((\Gamma))$*.*
- *We call "transseries" the elements of* $K((\Gamma))$ *(this goes beyond the strict extension of the word. But as a shorthand for "generalized power series", the word coined by Ecalle is too convenient; and the actual fields* $K((\Gamma))$ *that we consider below do consist of transseries).*
- *We call* **support** *of an element of* $K((\Gamma))$ *the set of "transmonomials"* $\gamma \in \Gamma$ *which occur in the terms of the element.*
- *The order* $<$ *is such that the* K*-finite transseries are those with support* ≤ 1*, the* K*-infinitesimals with support* < 1*.* $K[[\Gamma > 1]]$ *denotes the transseries with support* > 1 *– in other words those having only* K*-infinite terms.*

Transseries help to define natural though non standard models of $T_e, T_{\exp}, \lfloor T_{\exp} \rfloor, \lceil T_{\exp} \rceil$ *which are useful in particular to prove Theorems 4, 5, 7, 9. To begin with, via the next two results they provide models of* T_e *with natural integral parts.*

Proposition 13. $A = \lfloor K \rfloor \longrightarrow A + K[[\Gamma > 1]] = \lfloor K[[\Gamma > 1]] \rfloor$ *and* A^+ *is an initial segment of* $(A + K[[\Gamma > 1]])^+$*.*

Proof of Proposition 13. Easy, see [3]. □

Theorem 14. *For every model* K_E *of* T_e *and every group of monomials* Γ *which is closed under* p^{th} *root,* $p < \omega$ *there is a canonical expansion* $K_E((\Gamma))$ *of* $K((\Gamma))$ *such that* $K_E \prec K_E((\Gamma))$*.*

Proof of Theorem 14. The model has been defined by Neumann – see [2, 4]; the fact that $K_E \prec K_E((\Gamma))$ is a theorem of $[DMM]$. □

We are ready to provide the proofs that were omitted in the preceding sections because they depended on transseries.

Proof of Lemma 7. We are given a pair $(K_{\exp}, A)$ such that $K_{\exp}$ satisfies $T_{\exp}$ hence the induced model K_e satisfies T_e, and $A = \lfloor K \rfloor$; we construct a blunt model $(R_{\exp}, Z)$ of $T_{\exp} + IP(x^y)$ such that A^+ is initial segment of Z^+. Fix a non trivial group of exponents Γ closed under pth root, $p < \omega$. By induction on $n < \omega$ define (K_e^n, Z_n): $K_e^1 := K_e((\Gamma))$ and $Z_1 := A + K[[\Gamma > 1]]$; next we let Γ_2 denote the set of formal objects $2^g, g \in K[[\Gamma > 1]]$ turned to a group of monomials in the natural way: $2^g 2^{g'} := 2^{g+g'}$ and $2^g < 2^{g'}$ iff $g < g'$. Then $(K_e^2, Z_2) := (K_e^1((\Gamma_2)), Z_1 + K^1[[\Gamma_2 > 1]])$; and (K_e^n, Z_n) is defined by iterating n times this construction. By Theorem 14 and Proposition 13 we have that

$K_e^n \prec K_e^{n+1}$, Z_n^+ is initial segment of Z_{n+1}^+ and $Z_n = \llcorner K^n \lrcorner$. Hence $\mathcal{K}_e$ satisfies T_e, A^+ is initial segment of $\mathcal{B}^+$ and $\mathcal{B} = \llcorner R \lrcorner$ if we set $\mathcal{K} = \cup_{n<\omega} K^n, \mathcal{B} = \cup_{n<\omega} Z_n$. We inductively define a function 2^x on R: if $x \in K^{n+1}$ we can uniquely write $x = a + \epsilon$ where $a \in Z_n, 0 \leq \epsilon < 1, \epsilon \in K^{n+1}$; then $2^x := 2^a 2^\epsilon$ where 2^a exists by inductive assumption and 2^ϵ is defined in K_e^{n+1}. It is not difficult to check that $\mathcal{K}_{\exp} := (\mathcal{K}, 2^x)$ satisfies the axioms of EXP – except for the existence of the inverse log of the function 2^x: for instance inside $\mathcal{K}$ it is undefined for $1 \neq x \in \Gamma$.

The next step makes up for this defect; we define a proper embedding φ from $\mathcal{K}_{\exp}$ into itself: if $\sigma = \Sigma_i a_i 2^{\delta_i} \in \mathcal{K}$ set $\varphi(\sigma) = \Sigma_i a_i 2^{2^{\delta_i}}$. It is easy to check that the domain of log inside $\mathcal{K}_{\exp}$ includes the image of φ. Let $(\mathcal{K}_{\exp}^{-1}, \mathcal{B}_{-1})$ denote the extension of $(\mathcal{K}_{\exp}, \mathcal{B})$ such that φ has an extension to an isomorphism of $(\mathcal{K}_{\exp}^{-1}, \mathcal{B}_{-1})$ **onto** $(\mathcal{K}_{\exp}, \mathcal{B})$ ($(\mathcal{K}_{\exp}^{-1}, \mathcal{B}_{-1})$ is unique up to isomorphism over φ). By iterating ω times this construction one obtains a chain of models $(R_{\exp}^{-n}, \mathcal{B}_{-n})$, $n < \omega$. Set $(\mathcal{R}_{\exp}, \mathcal{Z}) = \cup_n (R_{\exp}^{-n}, \mathcal{B}_{-n})$; it is easy to check that $\mathcal{R}_{\exp}$ satisfies $T_{\exp}$ and $\mathcal{Z}$ is an integral part of $\mathcal{R}_{\exp}$. In addition (but this is delicate and skipped here) $\mathcal{Z}^+$ is closed under $x^y_{\mathcal{R}}$. This concludes the proof. □

We skip the proof of Lemma 10 hence Theorems 8 and 9: it is quite similar.

Proof of Theorem. We call **truncations** of a transseries $\Sigma_{i<\alpha} a_i s_i$ all **shorter** series $\Sigma_{i<\beta} a_i s_i$ with $\beta \leq \alpha$. In [3] it is proved that for every rcl field R there is an archimedean subfield K of R, a group of monomials S and an embedding φ over $K(S)$ from R into $K((S))$, with truncation closed image. Thus $\llcorner R \lrcorner_\varphi := \mathbb{Z} + \varphi^{-1}(K[[S > 1]])$ is an integral part of R and Theorem 12(a) is proved. In [R93] it is proved in addition: (i) if R is the underlying field of a model $R_{\exp}$ of EXP then φ can be chosen so that $\llcorner R \lrcorner_\varphi^+$ is closed under 2^x – hence Theorem 12(b) is proved; (ii) if $R_{\exp}$ satisfies $T_{\exp}$ then the latter embedding φ can be required to preserve $e(x)$ from R_e to $K_e((S))$. Finally:

Lemma 15. *$\llcorner R \lrcorner_\varphi$ is closed under x^y_R.*

The proof of this delicate point duly appears in the full version. And the proof of Theorem 12(c) then is easy... □

4. Conclusion

1. It is interesting to look for the generalization of our polytime witnessing theorem; one specific sharp extension should be when the Gamma function is added to $\mathcal{L}(2^x)$ and the factorial added to $\mathcal{L}(x^y)$. But the natural framework for the generalization is no less than all o-minimal expansions of the reals.

2. We expect that the polytime witnessing result which so far only concerns the NP class has a good extension to the whole polynomial time hierarchy. This should be of interest for applications. Another application to look for is the asymptotic analysis of every polynomially bounded o-minimal expansion $\mathcal{R}_E$ of the reals. Here is the reason for: polynomial boundedness implies for every formula $\Phi(a, x) \in \mathcal{L}(E)$ that $\mathcal{R}_E$ satisfies $\exists x \Phi(a, x)$ iff $(\mathcal{R}_E, 2^x)$ satisfies $\exists x < a^{\log(a)} \Phi(a, x)$; and this may

be sharpened and generalized. Now the witnessing result which we proved for $T_{\exp}$ can be extended to the complete theory of $(\mathcal{R}_E, 2^x)$ for many E's; and even with $E = 0$ (*i.e.* in the real algebraic case) it has good chances to lead to an interesting approach to asymptotic studies since it provides a polytime computable witness for $\exists x < a^{\log(a)}\Phi(a, x)$, **hence** for the initial question $\exists x\Phi(a, x)$.

3. Of course the question of finding an **effective** proof of our witnessing theorem is of interest; note that the theorem contains, for an infinity of questions Q, a result of the form: "there exists a polytime algorithm to answer Q". But it does so **without** ever providing the algorithm! (Generally speaking this is the weakness of our method of proof; but at the same time it makes the efficiency of the approach: it tells in advance which effective questions it will be profitable to investigate by effective means. It may also tell in advance which questions of this type are hopeless by proving an undecidability result; in these two ways it offers a speed up to the research on algorithms of many kinds.)

4. We expect that the appropriate framework for the generalization of Shepherdson's criterion is again: all (or nearly all) o-minimal expansions of the reals. A result such as the correspondence between $IVR(2^x)$ and $LE_0(2^x)$ opens a way towards interesting effective investigations: it suggests to replace computations over the reals – when they are expressible and provable within $IVR(2^x)$ – by recursive computations over the integers (since the latter computations exist provably in $LE_0(2^x)$ which is a system for which a whole programming machinery already exists). Here we mention $IVR(2^x), LE_0(2^x)$ rather than $T_{\exp}, \lfloor T_{\exp} \rfloor$ because the latter systems are too obscure at present. By the way, the obscurity of $\lfloor T_{\exp} \rfloor$ makes it all the more interesting that (i) we are able to show provable polytime witnessing for such a system (ii) and the weaker, clearer systems which also have polytime witnessing (as a trivial consequence of (i)) do **not** guarantee **provable** witnessing.

5. We expect that the problem of the relations between $LE_0(2^x), LE_0(x^y)$ and $IVR(2^x), T_{\exp}$ will offer a new way to investigate the well known and hard problems of decidability of $T_{\exp}$ and Shanuel's conjecture for reals.

6. The conservation result of blunt axiom systems can be generalized, and again the natural framework for this extension is no less than all o-minimal expansions of the reals. The potential research discussed in 3, 4, 5 may be tied up to the use of blunt systems because of the simplying effect of bluntness. In addition our conservation result shows that in principle if we base an algorithm on a resource bound axiom system for Arithmetics we can allow ourselves blunt systems for that purpose; and this should be heuristically useful. Réveillès and Richard, and Daurat published papers on a method which turns the effective solution of differential equations to recursive programs on the integers; their method is heuristically based on non standard models and computations. The integer part of these non standard models can be taken to be blunt; but the mentioned work does not use this fact at all. The more so since it is by no means obvious how to take advantage of this possibility; but a whole new perspective is opened if one decides to take up seriously the question: "what algorithms – probably not entirely included in

the Réveillès and Richard ones – are heuristically suggested by bluntness and its conservativeness?".

7. As briefly hinted in the body of the paper, our results also have some interest in the perspective of achieving a true duality between systems similar to RCF, $T_{\exp}$ and systems similar to $\llcorner RCF \lrcorner$, $\llcorner T_{\exp} \lrcorner$. But conceptually new work will have to be done as a prequisite for this matter.

References

[1] S. Boughattas, Trois Théorèmes sur l'induction pour les formules ouvertes munies de l'exponentielle. *J. Symbolic Logic* **65** (2000) 111–154.

[2] L. Fuchs, *Partially Ordered Algebraic Systems*. Pergamon Press (1963).

[3] M.-H. Mourgues and J.P. Ressayré, Every real closed field has an integer part. *J. Symbolic Logic* **58** (1993) 641–647.

[4] S. Priess-Crampe, *Angeordnete Strukturen: Gruppen, Körper, projektive Ebenen*. Springer-Verlag, Berlin (1983).

[5] A. Rambaud, Quasi-analycité, o-minimalité et élimination des quantificateurs. *PhD. Thesis*. Université Paris 7 (2005).

[6] J.P. Ressayre, Integer Parts of Real Closed Exponential Fields, *Arithmetic, Proof Theory and Computational Complexity*, edited by P. Clote and J. Krajicek, Oxford Logic Guides 23.

[7] J.P. Ressayre, *Gabrielov's theorem refined*. Manuscript (1994).

[8] J.C. Shepherdson, A non-standard model for a free variable fragment of number theory. *Bulletin de l'Academie Polonaise des Sciences* **12** (1964) 79–86.

[9] L. van den Dries, Exponential rings, exponential polynomials and exponential functions. *Pacific J. Math.* **113** (1984) 51–66.

[10] 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** (1996) 1051–1094.