Real closures of models of weak arithmetic

Emil Jeřábek[*] Leszek Aleksander Kołodziejczyk[†]

April 19, 2011

Abstract

D'Aquino et al. (J. Symb. Log. 75(1)(2010)) have recently shown that every real-closed field with an integer part satisfying the arithmetic theory $I\Sigma_4$ is recursively saturated, and that this theorem fails if $I\Sigma_4$ is replaced by $I\Delta_0$. We prove that the theorem holds if $I\Sigma_4$ is replaced by weak subtheories of Buss' bounded arithmetic: PV or Σ^b_1-$IND^{|x|_k}$. It also holds for $I\Delta_0$ (and even its subtheory IE_2) under a rather mild assumption on cofinality. On the other hand, it fails for the extension of *IOpen* by an axiom expressing the Bézout property, even under the same assumption on cofinality.

A discretely ordered subring A of a real-closed field (henceforth often: rcf) R is an *integer part* of R if for every $r \in R$ there exists $a \in A$ such that $a \leq r < a + 1$. It is well-known that every rcf has an integer part [MR93], which is then a model of the weak arithmetic theory *IOpen* (induction for quantifier-free formulas in the language of ordered rings). On the other hand, every model of *IOpen* is an integer part of its real closure (or, more precisely, the real closure of its fraction field).

Recently, d'Aquino et al. [DKS10] studied the question which rcfs have integer parts satisfying more arithmetic, e.g. Peano Arithmetic. It turns out

[*] Institute of Mathematics of the Academy of Sciences, Žitná 25, 115 67 Praha 1, Czech Republic, jerabek@math.cas.cz. Supported by Institutional Research Plan AV0Z10190503, grant IAA100190902 of GA AV ČR, project 1M0545 of MŠMT ČR, and a grant from the John Templeton Foundation.

[†] Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warszawa, Poland, lak@mimuw.edu.pl. Partially supported by grant N N201 382234 of the Polish Ministry of Science and Higher Education.

that at least in the countable case, the answer is relatively straightforward: a countable non-archimedean rcf R has an integer part satisfying *PA* if and only if R is recursively saturated. Moreover, the "only if" direction actually requires neither countability nor full *PA*: to conclude that R is recursively saturated, it is enough to know that R has an integer part satisfying $I\Sigma_4$.

From an arithmetical point of view, $I\Sigma_4$ is still quite a powerful theory, so it is natural to wonder whether it can be replaced by something weaker. D'Aquino et al. point out that it cannot be replaced by $I\Delta_0$, for a rather trivial reason: some nonstandard models of $I\Delta_0$ are *bounded*, in the sense that they contain a cofinal set of the form $\{a^n : n \in \mathbb{N}\}$, whereas an integer part of a recursively saturated ordered field must obviously be *unbounded.* However, the more general question "how much arithmetic in an integer part is enough to guarantee recursive saturation?" is left open in [DKS10].

We take up this very question; though we are not able to provide a complete answer, we do manage to show that the boundary between arithmetic theories which do guarantee recursive saturation and those which do not lies far below $I\Sigma_4$. In particular, boundedness is the *only* reason why a non-archimedean rcf with an integer part satisfying $I\Delta_0$ may fail to be recursively saturated. This remains true if $I\Delta_0$ is replaced by its fragment IE_2 (induction for formulas with just two blocks of bounded quantifiers). Recursive saturation of an rcf also follows from the existence of integer parts satisfying weak fragments of Buss' bounded arithmetic: PV (a canonical theory for polynomial time reasoning), or restricted forms of Σ^b_1 induction, studied by Boughattas and Ressayre [BR10].

On the other hand, some algebraic extensions of *IOpen*, previously studied in the context of independence results [Smi93] and as counterexamples to Tennenbaum's theorem [Moh06], can be satisfied in an integer part of an unbounded but not recursively saturated rcf. We verify this for *IOpen* + *Bézout*, which extends *IOpen* by the Bézout axiom:

$$\forall x \, \forall y \, \exists z \, \exists u \, \exists v \, (z \mid x \wedge z \mid y \wedge xu + yv = z).$$

We also show that the real closure of a recursive discretely ordered ring can never be recursively saturated, and generalize a result of [DKS10] on theories satisfiable in integer parts of recursively saturated rcfs.

On the whole, our results seem to suggest that the property of arithmetic theories T, "every unbounded rcf with an integer part satisfying T is recursively saturated", is best seen as a Tennenbaum-like property, i.e. a structural feature of models that separates theories with "significant arithmetical content" from "algebraic" fragments of arithmetic such as *IOpen*. Earlier properties of this kind include the one arising from Tennenbaum's theorem, i.e. "T has no recursive nonstandard models" [Ten59, She64, Wil85, BO96, Moh06], as well as "every nonstandard model of T has a nonstandard initial segment satisfying *PA*" [McA82, Par84] and "the reduct of every nonstandard model of T to the language of addition is recursively saturated" [CMW82, Wil85]. Of course, each concrete property leads to a different notion of "significant arithmetical content". In our case, interesting questions remain. For example, we do not know whether an unbounded rcf with an integer part satisfying the fragment IE_1 of $I\Delta_0$ has to be recursively saturated.

Our paper consists of this introduction and six further sections. Section 1 has a preliminary character and fixes definitions and notation. In Section 2, we show that real closures of recursive discretely ordered rings are not recursively saturated. In Section 3, we prove our main results about weak arithmetic theories which imply recursive saturation of an rcf when satisfied in its integer part. In Section 4, we construct an unbounded model of $IOpen + B\acute{e}zout$ whose real closure is not recursively saturated. In Section 5 we construct models of extensions of *IOpen* with preassigned real closure. In Section 6 we mention some open problems.

1 Preliminaries

An *ordered ring* $(R, 0, 1, +, \cdot, \leq)$ is a commutative ring endowed with a total order such that the set of nonnegative elements is closed under $+$ and $\cdot$. A *real-closed field (rcf)* (see e.g. Chapter 3 of [Mar02]) is an ordered field in which every positive element has a square root, and every polynomial of odd degree has a root. The theory of real-closed fields, denoted *RCF*, is complete (in particular, it coincides with $\mathrm{Th}(\mathbb{R})$), decidable, and enjoys effective elimination of quantifiers. The last property implies that every rcf is an *o-minimal* structure: every definable subset of R is a finite union of (possibly degenerate) intervals.

Any ordered domain R has a *real closure* $\mathrm{rcl}(R)$: an rcf which is an algebraic extension of R. Real closure is unique up to isomorphism preserving R. More generally, if R is an rcf and X a subset of R, we will write $\mathrm{rcl}(X)$ for the set of elements of R algebraic over X; in other words, the real closure of the subring of R generated by X.

A *discretely ordered ring* is an ordered ring with no element between 0 and 1. Any such ring is necessarily a domain. A discretely ordered ring R is a $\mathbb{Z}$*-ring* if $R/nR \simeq \mathbb{Z}/n\mathbb{Z}$ for every integer $n > 0$. *IOpen* is the theory of discretely ordered rings whose nonnegative parts satisfy the *induction* axioms

$$\phi(0) \wedge \forall x\,(\phi(x) \to \phi(x+1)) \to \forall x\,\phi(x) \qquad (\phi\text{-}IND)$$

for all open (i.e. quantifier-free) formulas ϕ. An easy argument shows that a model of *IOpen* is always a $\mathbb{Z}$-ring.

In some contexts it is more convenient, and for stronger fragments of arithmetic quite standard, to consider ordered semirings with 0 as the least element instead of rings. That is, we can formulate *IOpen* as the theory consisting of the open induction schema on top of the theory of nonnegative parts of discretely ordered rings (denoted PA^-). Models of the latter theory can be extended in a unique way to a full ring, and we will pass from one representation of the model to the other without notice.

An *integer part* of an rcf R is a discretely ordered subring $A \subseteq R$ such that for every $r \in R$ there is $a \in A$ such that $a \leq r < a+1$. Models of *IOpen* are exactly integer parts of rcfs, and in particular, every $A \models IOpen$ is an integer part of $\mathrm{rcl}(A)$. If A is an integer part of R, then the fraction field F of A is dense in R: there is an element of F between any two elements of R.

Basic information on Peano Arithmetic PA and its subsystems $I\Sigma_n$ and $I\Delta_0$ can be found e.g. in [HP93]. $I\Delta_0$ and its fragments ([HP93, Wil85]) are defined as follows (the presentation below is in terms of semirings with a least element rather than rings). *Bounded quantifiers* are introduced by

$$\exists x \leq t\,\phi(x) \Leftrightarrow \exists x\,(x \leq t \wedge \phi(x))$$
$$\forall x \leq t\,\phi(x) \Leftrightarrow \forall x\,(x \leq t \to \phi(x))$$

where t is a term not involving x. A formula ϕ is bounded if all quantifiers in ϕ are bounded; the set of all bounded formulas is denoted Δ_0. A bounded formula in prenex normal form is E_n (resp., U_n) if its quantifier prefix can be divided into n alternating blocks (not necessarily nonempty) of quantifiers of the same type, where the first block is existential (resp., universal). A formula is ∇_n in a theory T if it is, provably in T, equivalent to both a E_n formula and a U_n formula. If Γ is a set of formulas (such as Δ_0 or E_n), then $I\Gamma$ denotes the theory $PA^- + \Gamma\text{-}IND$.

If $A \models PA^-$, a *cut* is an initial segment J of A with no greatest element. If a cut J is closed under multiplication, it is a submodel of A and agrees with A on satisfaction of bounded formulas with parameters from A. In particular, if $\Gamma \subseteq \Delta_0$, then Γ-*IND* is equivalent to a set of bounded formulas, hence a cut in a model of $I\Gamma$, if closed under $\cdot$, is itself a model of $I\Gamma$. If $1 < a \in A$, then $a^{\mathbb{N}}$ denotes the cut $\{x \in A : \exists n \in \mathbb{N}\, x \leq a^n\}$. A model A is *bounded* if there exists $a \in A$ such that $A = a^{\mathbb{N}}$. If J is a cut of A, we write $a < J < b$ for $a \in J$, $b \notin J$.

Buss [Bus86] introduced a hierarchy of theories in the language $L_B = \{0, 1, +, \cdot, \leq, |x|, \#, \lfloor x/2 \rfloor\}$, where $|x| = \lceil \log_2(x+1) \rceil$ and $x \# y = 2^{|x|\cdot|y|}$. We refer the reader to [Kra95, HP93, CN10] for more detailed information. A bounded quantifier whose bounding term is of the form $|t|$ is called *sharply bounded*. Formulas using only sharply bounded quantifiers are called sharply bounded, or Σ^b_0. A formula is Σ^b_1 (resp., Π^b_1) if it can be written in a prenex normal form so that all quantifiers are bounded existential (resp., universal) or sharply bounded. A formula is $\hat{\Sigma}^b_1$, or *strict* Σ^b_1, if it consists of a block of existential bounded quantifiers followed by a sharply bounded formula. More generally, a formula is $\hat{\Sigma}^b_i$ (strict Σ^b_i) if it can be written with i alternating blocks of bounded quantifiers, the first one being existential, followed by a sharply bounded formula; in general Σ^b_i formulas, sharply bounded quantifiers are allowed to intervene anywhere in the quantifier prefix.

If $t(x)$ is a unary term and ϕ a formula, we consider the induction schema

$$\phi(0) \wedge \forall x\, (\phi(x) \to \phi(x+1)) \to \forall x \leq t(a)\, \phi(x). \tag{ϕ-IND^t}$$

All theories in L_B are tacitly assumed to include the open finite theory *BASIC* postulating basic properties of the symbols in the language. With this convention, Buss' theories are defined by $T^i_2 = \Sigma^b_i$-IND, $S^i_2 = \Sigma^b_i$-$\mathit{IND}^{|x|}$. We will also consider the theories Σ^b_1-$\mathit{IND}^{|x|_k}$, where $|x|_k$ denotes k times iterated $|x|$. In any structure for L_B, $\log^{(k)}$ denotes downward closure of the range of $|x|_k$.

PV is an open theory in a language L_{PV} with function symbols for all polynomial-time computable functions, originally introduced inductively using bounded recursion on notation; its axioms include defining equations for these function symbols, and ensure the provability of *IND* for open formulas. Alternatively, we may axiomatize PV by the Σ^b_1-fragment of S^1_2, where we expand the language by adding a function symbol for each provably total Σ^b_1-definable function of S^1_2.

If A is a model of some arithmetic, $S \subseteq \mathbb{N}$ and $A \ni s > \mathbb{N}$, then s *codes* S if for each $n \in \mathbb{N}$, $n \in S$ exactly if the n-th bit of s in binary notation is

1. Other notions of coding are also commonly used, e.g. with the value of the n-th bit replaced by divisibility by the n-th prime. In general, the family of sets coded in A may depend on the choice of coding, but nonstandard models of the theories we study in Section 3 always have nonstandard initial segments satisfying *PA*. For such models, the exact choice of a reasonable coding scheme is immaterial.

Recursive saturation is treated in [BS76]. Let A be a structure in a finite language L. A (consistent, but not necessarily complete) type of A over a finite set of parameters $\bar{a} \in A$, which can be written in the form $\{\phi(\bar{x}, \bar{a}) : \phi(\bar{x}, \bar{y}) \in \Gamma\}$ for a recursive set of formulas Γ, is called a *recursive type*. A is *recursively saturated* if every recursive 1-type of A is realized in A. By Craig's trick, every r.e. type is equivalent to a polynomial-time recursive type; moreover, the definition of recursive saturation does not change if we allow n-types for $n > 1$. Every countable recursively saturated model is *resplendent*: for any $\bar{a} \in A$ and any r.e. theory T in a finite language $L' \supseteq L_{\bar{a}}$ which is consistent with $\mathrm{Th}(A, \bar{a})$, there is an expansion B of $(A, \bar{a})$ to a model of T; moreover, we can make B recursively saturated as well.

2 Connection to Tennebaum

The following simple result shows that at least for $T \supseteq$ *IOpen*, the property "every non-archimedean rcf with an integer part satisfying T is recursively saturated" implies that T satisfies Tennenbaum's Theorem on the nonexistence of recursive nonstandard models.

Proposition 2.1. *If $A \models$ IOpen and* $\mathrm{rcl}(A)$ *is recursively saturated, then $+^A$ and $\leq^A$ cannot be both recursive.*

Proof. Let $X, Y \subseteq \mathbb{N}$ be a recursively inseparable pair of disjoint r.e. sets. By recursive saturation, there exist $x, y \in \mathrm{rcl}(A)$ such that $0 < x < y < 1$, and for every $z \in (x, y)$, $\lfloor 2^{n+1} z \rfloor$ is even whenever $n \in X$, and it is odd whenever $n \in Y$. Since the fraction field of A is dense in $\mathrm{rcl}(A)$, there exist $a, b \in A$ such that $a/b \in (x, y)$. If $+^A$ and $\leq^A$ were recursive,

$$\Big\{ n \in \mathbb{N} : A \models \bigvee_{\substack{k < 2^{n+1} \\ k \text{ even}}} (kb \leq 2^{n+1} a < (k+1)b) \Big\}$$

would be a recursive set separating X, Y, a contradiction. □

Remark. The proposition applies to models of *IOpen* considered as rings. If we take A to be only the non-negative part (as is usual for stronger fragments of arithmetic), we can strengthen the conclusion to state that $+^A$ is not recursive. (If $+^A$ is recursive, $\leq^A$ is also recursive, as $x \leq y$ and its negation are both existentially definable in terms of $+$.)

Remark. We have not been able to show that if every *unbounded* rcf with an integer part satisfying T is recursively saturated, then T has no recursive nonstandard models.

3 Main results

The entirety of this section is devoted to the proof of our main theorem:

Theorem 3.1. *Let A be*

(i) an unbounded model of IE_2, or

(ii) a nonstandard model of Σ_1^b-$IND^{|x|_k}$ for some $k \in \mathbb{N}$, or

(iii) a nonstandard model of PV,

and let R be a real-closed field such that A is an integer part of R. Then R is recursively saturated.

The proof of the main Theorem 5.1 in [DKS10] actually shows the following:

Theorem 3.2. *Let R be a real-closed field with integer part A such that* $\mathrm{rcl}(A)$ *is recursively saturated. Then R is recursively saturated, and if R is countable, then $R \simeq \mathrm{rcl}(A)$.*

Thus, it is enough for our purposes to show that if A satisfies one of the conditions in the statement of Theorem 3.1, then $\mathrm{rcl}(A)$ is recursively saturated. However, condition (ii) by itself may well be too weak to imply this: our arguments below make essential use of the assumption that A is an integer part of $\mathrm{rcl}(A)$, or in other words, that $A \models$ *IOpen*, but it follows from the work of [BR10] that Σ_1^b-$IND^{|x|_k} \nvdash$ *IOpen* for $k \geq 3$. For this reason, what we actually show below is that $\mathrm{rcl}(A)$ is recursively saturated whenever A is:

(i) an unbounded model of IE_2, or

(ii) a nonstandard model of Σ^b_1-$IND^{|x|_k} + IOpen$ for some $k \in \mathbb{N}$, or

(iii) a nonstandard model of PV.

Unbounded models of IE_2. Let $A \models IE_2$ be unbounded. Consider a recursive type $\Gamma(x, \bar{a})$ with $\bar{a} = a_1, \dots, a_k \in R$. We claim that $\Gamma(x, \bar{a})$ is satisfied in R.

Without loss of generality, we may simultaneously assume that (1) $\bar{a} \in A$, (2) Γ consists of open formulas. (1) holds because each element of $\bar{a}$ is definable in R from elements of A, so we may replace it by the parameters used in its definition. To obtain (2) as well, we use quantifier elimination for RCF, which is an effective procedure and hence preserves recursivity of the type. In order to simplify the notation, we may also assume that Γ contains the formula $x > 0$.

If $\Gamma(x, \bar{a})$ is satisfied by some element of $\mathrm{rcl}(\bar{a})$, we are done, so we may assume that no element of $\mathrm{rcl}(\bar{a})$ satisfies $\Gamma(x, \bar{a})$. It follows by o-minimality that each finite subset of $\Gamma(x, \bar{a})$ is satisfied on a non-degenerate interval $I \subseteq R$. The endpoints and length of I are in $\mathrm{rcl}(\bar{a})$; in particular, if we fix $b \in A$ such that $b > a^{\mathbb{N}}$, we have $I < b$ and $\mathrm{lh}(I) > 1/b$, hence I contains an element of the form w/b for some $w \in A \cap (0, b^2)$.

Fix an efficient enumeration of terms and open formulas in the arithmetical language. Let $(r)_i = x$ denote sequence encoding using Gödel's β-function, which is IE_1-provably ∇_1, and let $\theta(r, z, y_0, \dots, y_{k+1})$ denote the formula

$$\begin{aligned}\forall t, u, v \leq z\, [&(t = \ulcorner x_u \urcorner \wedge u \leq k+1 \to (r)_t = y_u)\\ &\wedge (t = \ulcorner u + v \urcorner \to (r)_t = (r)_u + (r)_v)\\ &\wedge (t = \ulcorner u \cdot v \urcorner \to (r)_t = (r)_u \cdot (r)_v)\\ &\wedge (t = \ulcorner u \leq v \urcorner \to \ ((r)_t = 1 \wedge (r)_u \leq (r)_v)\\ &\qquad\qquad\qquad\qquad \vee ((r)_t = 0 \wedge (r)_u > (r)_v))\\ &\wedge (t = \ulcorner u \to v \urcorner \to (r)_t = \max\{1 - (r)_u, (r)_v\})].\end{aligned}$$

(the $k{+}2$ variables $y_0, \dots, y_{k+1}$ will be needed below to accommodate $\bar{a}$, b, and an extra variable w). The meaning of θ is that the sequence r codes the values of terms and open formulas with Gödel number below z and parameters $y_0, \dots, y_{k+1}$ (we may assume that $0, 1$ appear among these). We can choose Gödel numbers so that the identites $t = \ulcorner u + v \urcorner$ etc. above are E_1, hence θ is

U_1. We also assume that the Gödel number of a term or a formula is greater than the Gödel numbers of its subterms and subformulas.

For each open formula $\phi(x, \bar{y})$, we can effectively find an open formula $\phi'(w, v, \bar{y})$ such that $A \models \phi'(w, v, \bar{y})$ iff $R \models \phi(w/v, \bar{y})$. Let the set $\Gamma' = \{\ulcorner \phi' \urcorner : \phi \in \Gamma\}$ be coded by $s \in A$, where s is small nonstandard. Fix some $c \in A$ such that $c > b^{\mathbb{N}}$, and let $\psi(z, \bar{a}, b, c, s)$ be the E_2 formula

$$\exists w \leq b^2 \, \exists r \leq c \, (\theta(r, z, w, b, \bar{a}) \wedge \forall f \leq z \, (f \in s \to (r)_f = 1)),$$

which expresses that some element of the form w/b satisfies all formulas in Γ with Gödel number below z. Since IE_1 proves that any sequence of elements below b and of standard length n can be coded by $r \leq b^{O(n)} \leq c$, it follows easily that $A \models \psi(n)$ for all standard n. By overspill, $A \models \psi(d)$ for some $d > \mathbb{N}$. This means that some element of the fraction field of A satisfies $\Gamma(x, \bar{a})$, and we are done. □

Nonstandard models of Σ_1^b*-IND*$^{|x|_k}$ + *IOpen.* We follow the same outline as the proof for IE_2, and we keep some of the notation. Due to the presence of # in the language, a nonstandard model of Σ_1^b-*IND*$^{|x|_k}$ is always unbounded. The inclusion of *IOpen* in our theory guarantees that the interval I in the argument above contains an element of the form w/b. Thus, all that has to be checked is that Σ_1^b-*IND*$^{|x|_k}$ has enough sequence-coding power to construct, and have overspill for, an analogue of the formula $\psi(z, \bar{a}, b, c, s)$ stating that the fragment of $\Gamma(x, \bar{a})$ up to z is satisfied by some element of the form w/b.

To code sequences, we use the relation $\lfloor x/2^y \rfloor = z$, which can be defined by the Σ_1^b formula

$$(y \geq |x| \wedge z = 0) \vee \exists w \leq x \, \exists v < w \, (w = 2^y \wedge x = wz + v)$$

($x = 2^y$ has a quantifier-free definition). In general, $\lfloor x/2^y \rfloor$ is not a total function in Σ_1^b-*IND*$^{|x|_k}$, but it is defined if $y \in \log^{(k)}$. For such y, $\lfloor x/2^y \rfloor = z$ also has an equivalent Π_1^b definition.

First, we need a universal formula for (standard) open formulas with a fixed tuple of parameters $\bar{a}, b$ and one other free variable w, to be interpreted by elements bounded by b^2. It is not difficult to see that the well-behavedness of $\lfloor x/2^y \rfloor$ for $y \in \log^{(k)}$ makes it possible to write such a formula in a Σ_1^b way (non-strict): we can use a formula similar to ψ and θ from the proof for IE_2, except that we make the universal quantifiers (bounded by z) sharply bounded, and we employ $\lfloor x/2^y \rfloor$ rather than Gödel's β-function.

Second, we note that there are arbitrarily small nonstandard s coding the set of formulas in Γ' by their bit sequences, where the ith bit of s is $\lfloor s/2^i \rfloor - 2\lfloor s/2^{i+1} \rfloor$. This is because a nonstandard model of Σ^b_1-$\mathit{IND}^{|x|_k}$ has a nonstandard initial segment satisfying $I\Delta_0$ (the closure of $\log^{(k)}$ under multiplication, at least if $k > 0$).

Using this, we can write

$$\exists w < b^2 \, \forall \ulcorner \phi' \urcorner < z \; (\ulcorner \phi'(w, v, \bar{y}) \urcorner \in s \Rightarrow A \models \phi'(w, b, \bar{a})) \tag{1}$$

in a Σ^b_1 way: for small z, the quantifier $\forall \ulcorner \phi' \urcorner < z$ can be made sharply bounded, and $\ulcorner \phi' \urcorner \in s$ is Π^b_1. We thus get overspill for (1), and the rest of the argument is as in the case of IE_2. □

Nonstandard models of PV. The overall strategy is similar to the one for Σ^b_1-$\mathit{IND}^{|x|_k}$, but as an additional difficulty we need to get rid of the existential quantifier in front of (1). Using the same notation as above, let s be an element of A coding Γ, and let $f(\bar{a}, b, s, r)$ be a PV-function formalizing the following polynomial-time algorithm:

(i) Write down the list of polynomials $p_0, \dots, p_m \in (\mathbb{Z}[\bar{a}])[x]$ such that every $\phi(x, \bar{a})$, where $\ulcorner \phi \urcorner \in s$, $\ulcorner \phi \urcorner \leq |r|$, is a Boolean combination of atomic formulas equivalent to $p_i(x) \geq 0$.

(ii) For each $i \leq m$, compute the Sturm sequence $p_{i,0} = p_i$, $p_{i,1} = p'_i$, $p_{i,j+1} = -(p_{i,j} \bmod p_{i,j-1})$. Let p_{i,k_i} be the last nonzero member of the sequence.

(iii) Compute $c_i = V_i(0, b) = V_i(0) - V_i(b)$, where $V_i(x)$ is the number of sign changes in the sequence $p_{i,0}(x), \dots, p_{i,k_i}(x)$. (If x is a multiple root of p_i, i.e., $p_{i,j}(x) = 0$ for every j, then we redefine $V_i(x)$ as $V_i(x + 1/b)$.)

(iv) For each $u < c_i$: using binary search, find $w_{i,u} < b^2$ such that

$$V_i(0, w_{i,u}/b) \leq u < V_i(0, (w_{i,u} + 1)/b).$$

(v) If $\phi(w_{i,u}/b, \bar{a})$ holds for all $\ulcorner \phi \urcorner \in s$, $\ulcorner \phi \urcorner \leq |r|$, then return $w_{i,u}$.

Note that if we put $n = |r|$ and $a = \max\{\bar{a}, 2\}$, then $m \leq n \log n$, each p_i is a polynomial of degree at most $\log n$, and $\|p_i\|_1 \leq a^{\log n}$, thus p_i has bit length $O(|a| \log n)$. This implies that step (i) can be done in polynomial time, and it is easy to formalize it in PV.

As for (ii), we have $k_i \leq \deg(p_i) \leq \log n$, and the computation of the sequence in a straightforward way takes $O(\log^3 n)$ arithmetical operations. In order to make it polynomial time, it thus suffices to ensure that coefficients of $p_{i,j}$ have polynomially bounded bit length. This follows from the fact that these coefficients can be expressed in terms of determinants of submatrices of the Sylvester matrix of p_i and p_i', see e.g. [vzGG99, Thm. 6.53]. Instead of formalizing these bounds in PV, we directly incorporate them in the definition of f (i.e., if the bounds are violated at some point, the function aborts the computation and returns, say, 0).

Step (iii) is clearly polynomial.

Step (iv) comprises $\log b^2$ evaluations of $V_i(w/b)$ for some integers $w < b^2$, which takes polynomial time.

In (v), we use the fact that evaluation of open arithmetical formulas can be performed in polynomial time; this follows using estimates similar to step (i).

Assume that Γ is not satisfied by any element of $\mathrm{rcl}(\bar{a})$. We claim that

$$\forall \ulcorner \phi \urcorner \leq |r| \, (\ulcorner \phi(x, \bar{y}) \urcorner \in s \to R \models \phi(f(\bar{a}, b, s, r)/b, \bar{a})) \tag{$*$}$$

holds for every standard r. We know that the conjunction of the ϕ's is satisfied on a non-degenerate interval $I = (\alpha, \beta) \subseteq (0, b)$ of length more than $1/b$ whose endpoints are roots of some of the polynomials p_i. Assume that β is the uth root (counted from 0) of p_i in $(0, b)$. Since p_i has standard degree, the true Sturm sequence for p_i satisfies the above mentioned bounds on coefficients, hence it coincides with the sequence $p_{i,j}$ computed in step (ii). By Sturm's theorem (which works for any rcf), $V_i(x, y)$ is the number of roots of p_i in $(x, y]$ as long as $x < y$ and neither x nor y is a multiple root of p_i. Our definition of $V_i(x)$ ensures that the same holds even if x or y *is* a multiple root, because if, say, x is a root, then there is no root in $(x, x + 1/b]$. It follows that there are at most u roots of p_i in $(0, w_{i,u}/b]$, and at least $u + 1$ roots in $(0, (w_{i,u} + 1)/b]$. Since there is at most one root in $(w_{i,u}/b, (w_{i,u} + 1)/b]$, we must have $\beta \in (w_{i,u}/b, (w_{i,u} + 1)/b]$. In other words, $w_{i,u}/b \in [\beta - 1/b, \beta) \subseteq I$, and $f(\bar{a}, b, s, r)$ is $w_{i,u}$ unless the algorithm found and returned another good $w_{i',u'}$ earlier.

As the evaluation of open formulas in the language $\{0, 1, +, \cdot, \leq\}$ is polynomial-time, the formula $(*)$ can be treated as a PV-formula. Thus, by overspill, $(*)$ also holds for some nonstandard r. Then $f(\bar{a}, b, s, r)/b$ satisfies $\Gamma(x, \bar{a})$.

We note that most of the argument for PV could be adapted to (the RSUV-isomorph of) VTC^0 (cf. e.g. [CN10]), extended by *IOpen*. However, the binary search in step (iv) seems to genuinely require sequential polynomial time. □

Remark. The results of this section show that the property "every nonstandard model of T has a recursively saturated real closure" does not require T to be particularly strong. However, we do not have a single example of a theory with this property which has been proved to be strictly weaker than full bounded induction in its appropriate language.

In particular, even though the theories Σ^b_1-$\mathit{IND}^{|x|_k}$ for $k \geq 3$ are known to be very weak (by [BR10], they do not even prove that powers of 2 have no non-trivial odd divisors), we are not aware of a result separating Σ^b_1-$\mathit{IND}^{|x|_k} + \mathit{IOpen}$ from full S_2, for any k. Interestingly, [BK10] gives such a separation in the case of $\hat{\Sigma}^b_1$-$\mathit{IND}^{|x|_5} + \mathit{IOpen}$, which has a restricted induction scheme for strict Σ^b_1 rather than general Σ^b_1 formulas. However, our proof of Theorem 3.1 part (ii) does rely on induction for non-strict Σ^b_1 formulas.

4 The unsaturated case

Some extensions of *IOpen* by algebraic axioms are known to, on the one hand, disprove various pathological statements consistent with *IOpen*, on the other hand, share many of the model-theoretic features of *IOpen*, such as the failure of Tennenbaum's Theorem. Essentially the strongest well-studied theory of this kind extends *IOpen* by the Bézout axiom:

$$\forall x\, \forall y\, \exists z\, \exists u\, \exists v\, (z \mid x \wedge z \mid y \wedge xu + yv = z).$$

$\mathit{IOpen} + B\acute{e}zout$ is known to disprove e.g. the rationality of $\sqrt{2}$, but not the existence of a greatest prime ([Smi93]). In [Moh06], it is stated (and proved for a slightly weaker theory) that $\mathit{IOpen} + B\acute{e}zout$ has recursive nonstandard models. Here, we prove that the real closure of an unbounded model of $\mathit{IOpen} + B\acute{e}zout$ does not have to be recursively saturated.

Theorem 4.1. *There exists an unbounded countable principal ideal domain $A \models$ IOpen (and therefore a model of Bézout + there exist unboundedly many primes + existence and uniqueness of prime factorization) such that* $\mathrm{rcl}(A)$ *is not recursively saturated.*

Proof. Note that a principal ideal domain (PID) is a Bézout domain and a unique factorization domain (UFD). A UFD with boundedly many primes is bounded. Moreover, a UFD satisfies the first-order axiom stating the existence and uniqueness of prime factorization, formulated using Gödel's β-function (since *IOpen* does not prove that we can multiply together a sequence of integers, we must formulate it so that a factorization is explicitly endowed with a sequence of partial products of the factors): on the one hand, a true prime factorization comprises a sequence of standard length, which exist in *IOpen*. On the other hand, the usual proof of uniqueness of factorization is easily seen to work in this setting whenever at least one of the factorizations has standard length, which we can assume by the existence part.

For the actual construction, we adapt the proof by Smith [Smi93, Thm. 10.7] (building on [Wil78, MM89]) that there exists a nonstandard PID $A \models \mathit{IOpen}$. We make sure that $\operatorname{rcl}(A)$ is not recursively saturated. We assume the reader is familiar with [Smi93], but we will briefly describe Smith's construction so that we can refer to its ingredients. We build an increasing chain of countable discretely ordered UFDs $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$, and let $A = \bigcup_{n\in\mathbb{N}} A_n$ be its union. All the A_n are included in an $\aleph_1$-saturated rcf L, which we fix in advance. Every A_n is endowed with a ring homomorphism $\varphi_n \colon A_n \to \hat{\mathbb{Z}}$, where

$$\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p = \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

(Here, $\mathbb{Z}_p$ denotes the ring of p-adic integers. When A_n is a $\mathbb{Z}$-ring, φ_n is its unique remainder homomorphism.) We make $\varphi_n \subseteq \varphi_m$ for $n \leq m$, and we maintain the condition that each φ_n is *parsimonious*, i.e., for every nonzero $a \in A_n$, there are only finitely many $k \in \mathbb{N}$ such that $k \mid \varphi_n(a)$.

We can take $A_0 = \mathbb{Z}$. The other A_n are constructed as follows:

(i) The "$\hat{\mathbb{Z}}$-construction": for odd n, we define $A_{n+1} = \{a/k : a \in A_n, k \in \mathbb{N}, k \mid \varphi_n(a)\}$. This ensures that A_n is a $\mathbb{Z}$-ring for every even n.

(ii) The "Wilkie construction": for some of the even n, we pick $\beta \in \operatorname{rcl}(A_n)$ which is not at a finite distance from any element of A_n (i.e., $|v-\beta| > m$ for every $v \in A_n$ and $m \in \mathbb{N}$), and we put $A_{n+1} = A_n[v]$, where $v \in L$ is suitably chosen so that $|v - \beta| < 1$, A_{n+1} is discretely ordered, and v is transcendental over A_n.

(iii) The “construction F”: for some of the even n, we pick distinct nonstandard primes $p, q \in A_n$, and we put $A_{n+1} = A_n[v, (pv - 1)/q]$, where $v \in L$, $v > A_n$.

(iv) We include another construction not considered in the original proof: for infinitely many of the even n, we put $A_{n+1} = A_n[v]$, where $v \in L$, $v > A_n$.

Smith shows that this strategy can be carried out correctly: i.e., for each of the constructions (i–iv), A_{n+1} is a discretely ordered UFD, and we can extend φ_n to a parsimonious $\varphi_{n+1}\colon A_{n+1} \to \hat{\mathbb{Z}}$ (the case of (iv) is a simple transcendental extension, and as such it is covered by [Smi93, §6]). Moreover, he shows that the steps can be arranged so that all β, p, q get handled eventually, which ensures that A is a model of *IOpen* (due to the Wilkie construction), a UFD, and every pair of primes has Bézout cofactors (due to construction F). The last two conditions imply that A is a PID. Construction (iv) ensures that A is unbounded. (In fact, A will be unbounded anyway if we can argue that construction F is applied infinitely many times in the chain.)

Let α be a transcendental computable real number, and $\Gamma(x) = \{a < x < b : a, b \in \mathbb{Q}, a < \alpha < b\}$ the corresponding recursive type. We want $\mathrm{rcl}(A)$ to omit Γ, which ensures that it is not recursively saturated. It suffices to arrange that Γ is omitted in every $\mathrm{rcl}(A_n)$. For convenience, we identify α with a fixed element of L realizing Γ. Using this convention, we need to ensure that no element $v \in \mathrm{rcl}(A_n)$ is infinitesimally close to α (i.e., $|v - \alpha| \leq 1/m$ for every $m \in \mathbb{N}$; written as $v \sim \alpha$).

Clearly, $\mathrm{rcl}(A_0)$ omits Γ. Assuming $\mathrm{rcl}(A_n)$ omits Γ, we consider our four constructions of A_{n+1}:

(i) The $\hat{\mathbb{Z}}$-construction preserves the fraction field, and a fortiori the real closure.

(iv) If $v > A_n$, $\mathrm{rcl}(A_n[v])$ is included in the field $F = \mathrm{rcl}(A_n)\langle\langle v^{-1}\rangle\rangle$ of Puiseux series over $\mathrm{rcl}(A_n)$ (see e.g. [BPR06, Cor. 2.98]): elements of F are formal sums of the form

$$a = \sum_{m=-\infty}^{M} a_m v^{m/k},$$

where $a_m \in \mathrm{rcl}(A_n)$, $M, k \in \mathbb{N}$, $k > 0$. Since $v > \mathrm{rcl}(A_n)$, a is dominated by its leading monomial. Thus, assuming $a \sim \alpha$, we must have $a_m = 0$ for all $m > 0$, hence $\alpha \sim a_0 \in \mathrm{rcl}(A_n)$, a contradiction.

(iii) Construction F: since $(pv-1)/q$ belongs to the fraction field of $A_n[v]$, $\operatorname{rcl}(A_n[v,(pv-1)/q]) = \operatorname{rcl}(A_n[v])$ omits Γ by (iv).

(ii) In order for the Wilkie construction not to realize Γ in $\operatorname{rcl}(A_{n+1})$, we need to choose v wisely. Let $\beta \in \operatorname{rcl}(A_n)$ not in finite distance from A_n be given.

Claim. Let $I \subseteq [\beta, \beta+1]$ be an interval of noninfinitesimal length. If $p \in A_n[x,y]$, $p \neq 0$, then there exists a noninfinitesimal interval $J \subseteq I$ such that $p(u,v) \neq 0$ for every $u \sim \alpha$ and $v \in J$.

Proof. Let us call $v \in I$ bad for u if $p(u,v)=0$. Write $p(x,y) = \sum_{i \le d} p_i(x) y^i$, where $p_i \in A_n[x]$. For each u, either there are at most d bad v, or all v are bad; the latter happens when u is a root of all p_i, which in particular means that $u \in \operatorname{rcl}(A_n)$. Thus, there are $m \le d$ bad v for α, let us denote them by $v_1 < \cdots < v_m$. Moreover, let v_0, v_{m+1} be the endpoints of I. Since $v_{m+1} - v_0$ is noninfinitesimal, there is $i \le m$ such that $v_{i+1} - v_i$ is noninfinitesimal, hence we can find rationals c, d such that $v_i < \beta + c < \beta + d < v_{i+1}$. Since the condition of there being no bad v in $[\beta+c, \beta+d]$ is definable with parameters from $\operatorname{rcl}(A_n)$ and satisfied by α, it is satisfied on an interval including α with endpoints in $\operatorname{rcl}(A_n)$. In particular, it is satisfied by all $u \sim \alpha$, hence $J = [\beta+c, \beta+d]$ works. □

Resuming our treatment of the Wilkie construction, let $\{p_k(x) : k \in \mathbb{N}\}$ be an enumeration of nonzero polynomials in $A_n[x]$, and $\{q_k(x,y) : k \in \mathbb{N}\}$ an enumeration of nonzero polynomials in $A_n[x,y]$. We construct a sequence of nested intervals $[\beta, \beta+1] = I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$ of noninfinitesimal length as follows. If $m = 2k$ is even, we find noninfinitesimal $I_{m+1} \subseteq I_m$ such that no $v \in I_{m+1}$ is infinitesimally close to a root of p_k (this is possible as the number of roots of p_k is standard, and I_m has noninfinitesimal length). If $m = 2k+1$ is odd, we use the claim to find a noninfinitesimal $I_{m+1} \subseteq I_m$ such that $q_k(u,v) \neq 0$ for any $u \sim \alpha$ and $v \in I_{m+1}$. By $\aleph_1$-saturation of L, there exists an element $v \in \bigcap_m I_m$. The construction ensures that v is not infinitesimally close to any element of $\operatorname{rcl}(A_n)$, hence $A_n[v]$ is discretely ordered by [Wil78]. Assume for contradiction that there exists $u \sim \alpha$ such that $u \in \operatorname{rcl}(A_n[v])$. Since u is algebraic over $A_n[v]$, there is k such that $q_k(u,v) = 0$, contradicting $v \in I_{2k+2}$. □

5 Constructing integer parts

D'Aquino et al. show a kind of converse statement to their main theorem, that every countable recursively saturated rcf not only has an integer part satisfying (a given extension of) Peano arithmetic (which follows trivially from resplendence), but also is the real closure of a model of (a given extension of) *PA*. We can generalize this result to extensions of *IOpen* (note that this is more general only if we consider unsound theories).

Theorem 5.1. *Let R be a countable recursively saturated rcf, and T a consistent recursively axiomatizable extension of IOpen. Then R has an integer part A such that $A \models T$ and $R = \mathrm{rcl}(A)$.*

Proof. By resplendence and the completeness of RCF, R has an integer part B which is a model of T such that (R, B) is recursively saturated. We would like to argue that $R \simeq \mathrm{rcl}(B)$ by invoking the theorem that a recursively saturated pair of countable elementarily equivalent models are isomorphic. We do not actually know whether $(R, \mathrm{rcl}(B))$ is recursively saturated, however the standard back-and-forth construction of the isomorphism only needs the following types to be realized (using quantifier elimination for RCF):

$$\Gamma(x) = \{\phi(c, \bar{a}) \leftrightarrow \phi(x, \bar{b}) : \phi \text{ open}\},$$
$$\Delta(x) = \{\phi(x, \bar{a}) \leftrightarrow \phi(d, \bar{b}) : \phi \text{ open}\} \cup \{x \in \mathrm{rcl}(B)\},$$

where $\bar{a}, c \in \mathrm{rcl}(B)$, $\bar{b}, d \in R$, $\mathrm{tp}(\bar{a}) = \mathrm{tp}(\bar{b})$, and $\mathrm{rcl}(B)$ is treated as a new unary predicate. Recursive saturation of R immediately implies that Γ is realized; we will show how to realize Δ. By o-minimality, either the type is satisfied in $\mathrm{rcl}(B)$ and we are done, or each finite subset of Δ is satisfied on an open interval $I \subseteq \mathrm{rcl}(B)$, and therefore by an element of the fraction field of B. Let $\bar{a}' \in B$ be such that $\bar{a}$ is definable in terms of $\bar{a}'$. For each open formula ϕ, we can effectively find an open formula $\phi'(x, y, \bar{a}')$ equivalent to $\phi(x/y, \bar{a})$. Then

$$\Delta'(x, y) = \{\phi'(x, y, \bar{a}') \leftrightarrow \phi(d, \bar{b}) : \phi \text{ open}\} \cup \{x, y \in B\}$$

is a recursive type of (R, B), hence it is realized by a pair of elements (u, v), and Δ is realized by u/v.

Thus, there exists an isomorphism $f \colon \mathrm{rcl}(B) \simeq R$, and then $A = f(B)$ is an integer part of R with all the required properties. □

6 Problems

We conclude the paper with a few open problems:

Problem 6.1. *Does the property "every unbounded rcf with an integer part satisfying T is recursively saturated" hold for T equal to:*

(a) IE_1?

(b) $IOpen(\lfloor x/y \rfloor)$?

(c) (the RSUV-isomorph of) VTC^0?

We note that [Wil85] shows that the reduct of a nonstandard model of IE_1 to the language of $+$ and $\leq$ is recursively saturated, but the techniques used to prove that result do not seem to be directly applicable in our case. $IOpen(\lfloor x/y \rfloor)$ is a theory about which little is known, except that it is strictly stronger than *IOpen* ([Kay93]) and contained in (an extension by definitions of) IE_1. VTC^0 plays an important role in the study of connections between weak arithmetic and computational complexity. It is normally formulated in a two-sorted language: after a translation known as the RSUV isomorphism, it becomes a subtheory of PV. Since multiplication is TC^0-complete, VTC^0 is the weakest reasonable theory in this two-sorted setup whose models have the structure of ordered semirings.

Problem 6.2. *Assume that T contains IOpen and every unbounded rcf with an integer part satisfying T is recursively saturated. Can T have recursive nonstandard models (which would then necessarily be bounded)?*

References

[BK10] Sedki Boughattas and Leszek A. Kołodziejczyk, *The strength of sharply bounded induction requires MSP*, Annals of Pure and Applied Logic **161** (2010), no. 4, 504–510.

[BO96] Alessandro Berarducci and Margarita Otero, *A recursive nonstandard model of normal open induction*, Journal of Symbolic Logic **61** (1996), no. 4, 1228–1241.

[BPR06] Saugata Basu, Richard Pollack, and Marie-Françoise Roy, *Algorithms in real algebraic geometry*, second ed., Algorithms and Computation in Mathematics, vol. 10, Springer, 2006.

[BR10] Sedki Boughattas and Jean-Pierre Ressayre, *Bootstrapping, part I*, Annals of Pure and Applied Logic **161** (2010), no. 4, 511–533.

[BS76] Jon Barwise and John Schlipf, *An introduction to recursively saturated and resplendent models*, Journal of Symbolic Logic **41** (1976), no. 2, 531–536.

[Bus86] Samuel R. Buss, *Bounded arithmetic*, Bibliopolis, Naples, 1986, Revision of 1985 Princeton University Ph.D. thesis.

[CMW82] Patrick Cegielski, Kenneth McAloon, and George Wilmers, *Modèles récursivement saturés de l'addition et de la multiplication des entiers naturels*, Logic Colloquium '80 (Dirk van Dalen et al., eds.), Studies in Logic and the Foundations of Mathematics, vol. 108, North-Holland, 1982, pp. 57–68.

[CN10] Stephen A. Cook and Phuong Nguyen, *Logical foundations of proof complexity*, Cambridge University Press, New York, 2010.

[DKS10] Paola D'Aquino, Julia F. Knight, and Sergei Starchenko, *Real closed fields and models of Peano arithmetic*, Journal of Symbolic Logic **75** (2010), no. 1, 1–11.

[HP93] Petr Hájek and Pavel Pudlák, *Metamathematics of first-order arithmetic*, Perspectives in Mathematical Logic, Springer, 1993, Second edition 1998.

[Kay93] Richard Kaye, *Open induction, Tennenbaum phenomena, and complexity theory*, Arithmetic, proof theory, and computational complexity (Peter Clote and Jan Krajíček, eds.), Oxford University Press, 1993, pp. 222–237.

[Kra95] Jan Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, vol. 60, Cambridge University Press, 1995.

[Mar02] David Marker, *Model theory: An introduction*, Springer, 2002.

[McA82] Kenneth McAloon, *On the complexity of models of arithmetic*, Journal of Symbolic Logic **47** (1982), no. 2, 403–415.

[MM89] Angus Macintyre and David Marker, *Primes and their residue rings in models of open induction*, Annals of Pure and Applied Logic **43** (1989), no. 1, 57–77.

[Moh06] Shahram Mohsenipour, *A recursive nonstandard model for open induction with GCD property and confinal primes*, Logic in Tehran (Ali Enayat et al., eds.), Lecture Notes in Logic, no. 26, Association for Symbolic Logic, 2006, pp. 227–238.

[MR93] Marie-Hélène Mourgues and Jean-Pierre Ressayre, *Every real closed field has an integer part*, Journal of Symbolic Logic **58** (1993), no. 2, 641–647.

[Par84] Jeff B. Paris, *O struktuře modelů omezené E_1-indukce*, Časopis pro pěstování matematiky **109** (1984), no. 4, 372–379.

[She64] John C. Shepherdson, *A non-standard model for a free variable fragment of number theory*, Bulletin de l'Académie Polonaise des Sciences. Série des Sciences Mathématiques, Astronomiques et Physiques **12** (1964), no. 2, 79–86.

[Smi93] Stuart T. Smith, *Building discretely ordered Bezout domains and GCD domains*, Journal of Algebra **159** (1993), no. 1, 191–239.

[Ten59] Stanley Tennenbaum, *Non-archimedean models for arithmetic*, Notices of the American Mathematical Society **6** (1959), 270.

[vzGG99] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, Cambridge University Press, 1999.

[Wil78] Alex J. Wilkie, *Some results and problems on weak systems of arithmetic*, Logic Colloquium '77 (Angus Macintyre et al., eds.), Studies in Logic and the Foundations of Mathematics, vol. 96, North-Holland, 1978, pp. 285–296.

[Wil85] George Wilmers, *Bounded existential induction*, Journal of Symbolic Logic **50** (1985), no. 1, 72–90.