On the theory of exponential integer parts

Emil Jeřábek*

Institute of Mathematics, Czech Academy of Sciences

Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

April 10, 2024

Abstract

We axiomatize the first-order theories of exponential integer parts of real-closed exponential fields in a language with 2^x, in a language with a predicate for powers of 2, and in the basic language of ordered rings. In particular, the last theory extends IOpen by sentences expressing the existence of winning strategies in a certain game on integers; we show that it is a proper extension of IOpen, and give upper and lower bounds on the required number of rounds needed to win the game.

1 Introduction

A classical result of Shepherdson [13] characterizes models of the arithmetical theory IOpen (induction for quantifier-free formulas in the language $\mathcal{L}_{\mathrm{OR}} = \langle 0, 1, +, \cdot, < \rangle$) as exactly those that are (nonnegative parts of) integer parts of real-closed fields. Here, an integer part (IP) of an ordered ring R is a discrete subring $I \subseteq R$ such that every element of R is within distance 1 from an element of I. An analogue for exponential ordered fields $\langle R, \exp \rangle$ (with $\exp(1) = 2$) was introduced by Ressayre [11]: an exponential integer part (EIP) of R is an IP $I \subseteq R$ such that $I_{\geq 0}$ is closed under exp. (We will find it more convenient to call the nonnegative part $I_{\geq 0}$ the EIP of R rather than I itself, and we usually denote $\exp \restriction I_{\geq 0}$ as 2^x.) We are interested in the question what models of IOpen are EIP of real-closed exponential fields (RCEF), and in particular, what is the first-order theory of such structures.

The question whether the theory of EIP of RCEF in $\mathcal{L}_{\mathrm{OR}}$ coincides with IOpen was raised by Jeřábek [7]; he provided an upper bound on the theory, proving that every countable model of the weak arithmetic VTC^0 (or rather, the equivalent one-sorted arithmetical theory Δ^{b}_1-CR) is an EIP of a RCEF, despite the fact that the "natural" integer exponentiation function in this theory is only defined for small integers.

Extensions of Shepherdson's theorem to RCEF were studied previously by Boughattas and Ressayre [2] and Kovalyov [9]. Their work differs from ours in two main respects. First, they approach Shepherdson's characterization from the other side, focusing on problems such

*Supported by the Czech Academy of Sciences (RVO 67985840) and GA ČR project 23-04825S.

as: what additional axioms must be added to RCEF to ensure that their EIP are models of such and such theory (e.g., open induction in a language with exponentiation). Second, they mostly study IPs closed under the binary powering operation $x^y = \exp(y \log x)$ in a language including x^y: in this case, the ambient exponential field can be canonically reconstructed from the structure of the IP (using the integer x^y operation, we can define rational approximations of $\exp(x)$ for rational x, which yields an exponential function on the completion of the fraction field). Such a direct construction seems impossible if we have only 2^x instead of x^y in the language, let alone when we work only with the basic language $\mathcal{L}_{\mathrm{OR}}$; thus, we will instead rely on model-theoretic tools such as the joint consistency theorem and recursively saturated models.

Our main contribution is an axiomatization of the theories of EIP of RCEF in $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$, in $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ (where P_2 is a predicate for the set of powers of 2), and in $\mathcal{L}_{\mathrm{OR}}$, denoted TEIP_{2^x}, TEIP_{P_2}, and TEIP (respectively). The first two theories are extensions of IOpen by finitely many axioms expressing basic algebraic properties of 2^x and P_2. The most important theory, TEIP, is more involved: it extends IOpen with an infinite sequence of sentences expressing that a certain game on positive integers (designed so that playing powers of 2 is a winning strategy) is a win for the second player. We note that there is a general result on axiomatizing conservative fragments of given theories by means of game sentences of similar kind due to Svenonius [15], which is instrumental in the argument that countable recursively saturated models are resplendent (Barwise and Schlipf [1]). However, in contrast to the rather opaque game considered by Svenonius, mimicking the Henkin completion procedure, our game on integers has simple and transparent rules, which makes it amenable to combinatorial analysis.

We show that TEIP is a proper extension of IOpen. We leave open the problem whether TEIP is finitely axiomatizable over IOpen, but as a partial progress, we prove that formulas obtained by stripping the outermost pair of quantifiers from each axiom of TEIP form a strict hierarchy (even over the true arithmetic $\mathrm{Th}(\mathbb{N})$); this amounts to the fact that if we play our integer game starting with arbitrary numbers that are not powers of 2, the first player needs an unbounded number of rounds to win. To this end, we analyze the game, proving upper and lower bounds on the number of rounds needed to win that are tight for a sizeable set of initial integers.

There is a natural interpretation of $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ in arithmetic where we put $P_2(x)$ iff x has no nontrivial odd divisor ("x is oddless"). We briefly discuss what theories of arithmetic prove TEIP_{P_2} under this interpretation (and hence include TEIP): in particular, this holds for IE_2. On the other hand, not even $\mathrm{Th}(\mathbb{N}) + \mathsf{TEIP}_{P_2}$ can prove that $P_2(x)$ implies x is oddless: it is consistent that an element of P_2 is divisible by 3. In other words, even for strong theories of arithmetic, expansions to models of TEIP_{P_2} are not unique.

The paper is organized as follows. We review the preliminaries in Section 2. We compute the theories of EIP of RCEF in $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$ and $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ in Section 3. In Section 4, we introduce the PowG game and determine the theory TEIP of EIP or RCEF in $\mathcal{L}_{\mathrm{OR}}$. Section 5 is devoted to an analysis of winning strategies in PowG. We discuss the oddless interpretation of P_2 in Section 6, and we end with some concluding remarks and open problems in Section 7.

2 Preliminaries

Let $\mathcal{L}_{\mathrm{OR}} = \langle 0, 1, +, \cdot, < \rangle$. An *ordered ring* is an $\mathcal{L}_{\mathrm{OR}}$-structure $\mathfrak{R} = \langle R, 0, 1, +, \cdot, < \rangle$ such that $\langle R, 0, 1, +, \cdot \rangle$ is a commutative ring, and $<$ is a (strict) total order on R compatible with $+$ and $\cdot$ (i.e., $x \le y$ implies $x + z \le y + z$, and, if $z \ge 0$, also $xz \le yz$). We call $\mathfrak{R}$ *discrete* if there is no element strictly between 0 and 1. An *ordered field* is an ordered ring that is a field. An ordered field $\mathfrak{R} = \langle R, \dots \rangle$ is a *real-closed field* (*RCF*) if it has no proper algebraic extension to an ordered field, or equivalently, if every $a \in R_{>0}$ has a square root in $\mathfrak{R}$, and every polynomial $f \in \mathfrak{R}[x]$ of odd degree has a root in $\mathfrak{R}$, where $R_{>0}$ denotes $\{a \in R : a > 0\}$.

An *integer part* (*IP*) of an ordered ring $\mathfrak{R} = \langle R, \dots \rangle$ is a discrete subring $I \subseteq R$ (considered as an $\mathcal{L}_{\mathrm{OR}}$-substructure) such that for every $a \in R$, there is $z \in I$ such that $z \le a < z + 1$.

The *nonnegative part* of an ordered ring $\mathfrak{R} = \langle R, \dots \rangle$ is its substructure $\mathfrak{R}_{\ge 0}$ with domain $R_{\ge 0} = \{a \in R : a \ge 0\}$. The theory of nonnegative parts of discrete ordered rings is denoted PA^-; it is an extension of Robinson's arithmetic Q. Every $\mathfrak{M} = \langle M, \dots \rangle \models \mathsf{PA}^-$ has a unique (up to isomorphism) extension to a discrete ordered ring $\mathfrak{M}_\pm = \langle M_\pm, \dots \rangle$ such that $(\mathfrak{M}_\pm)_{\ge 0} = \mathfrak{M}$ and $M_\pm = \{a, -a : a \in M\}$, which is called the *extension of* $\mathfrak{M}$ *with negatives*. The extension of PA^- (or equivalently, Q) with the *induction axioms*

$$(\varphi\text{-IND}) \qquad \forall \vec{y}\, \big(\varphi(0, \vec{y}) \wedge \forall x\, \big(\varphi(x, \vec{y}) \to \varphi(x + 1, \vec{y})\big) \to \forall x\, \varphi(x, \vec{y})$$

for all open (= quantifier-free) $\mathcal{L}_{\mathrm{OR}}$-formulas φ is denoted IOpen.

Theorem 2.1 (Shepherdson [13]) *An $\mathcal{L}_{\mathrm{OR}}$-structure $\mathfrak{M}$ is an IP of a RCF if and only if $\mathfrak{M}_{\ge 0} \models \mathsf{IOpen}$.* □

Note that a priori there is no reason for the class of integer parts of RCF to be elementary; indeed, this fails for our case of interest (EIP of RCEF), as we will see.

$\mathfrak{R} = \langle R, 0, 1, +, \cdot, <, \exp \rangle$ is an (*ordered*) *exponential field* if $\langle R, 0, 1, +, \cdot, < \rangle$ is an ordered field, and exp is an ordered group isomorphism $\exp \colon \langle R, +, 0, < \rangle \to \langle R_{>0}, \cdot, 1, < \rangle$. Following Ressayre [11], a *real-closed exponential field* (*RCEF*) is an exponential field $\mathfrak{R} = \langle R, \dots \rangle$ which is real-closed and satisfies $\exp(1) = 2$; if $\exp(x) > x$ for all $x \in R$, we say that it satisfies the *growth axiom*[1] (*GA*). If I is an IP of $\mathfrak{R}$ such that $I_{\ge 0}$ is closed under exp, we call $I_{\ge 0}$ an *exponential integer part* (*EIP*) of $\mathfrak{R}$. (We define $I_{\ge 0}$, rather than I itself, to be an EIP, since we intend to axiomatize first-order theories of EIP as extensions of IOpen, and compare them with other theories of arithmetic such as IE_k, which are formulated such that all elements are nonnegative.) We consider an EIP $I_{\ge 0}$ to be not just a set, but an $\mathcal{L}_{\mathrm{OR}}$-substructure of $\mathfrak{R}$, and we also consider it in some expanded languages: $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$, by inheriting the function $2^x = \exp \restriction I_{\ge 0}$ from $\mathfrak{R}$, and $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$, where the unary predicate P_2 is interpreted as the image of $2^x \colon I_{\ge 0} \to I_{>0}$.

[1] Ressayre includes this in the definition of an exponential field, and actually formulates it as "$\exp(x) > x^n$ for all x somewhat larger than n", where n presumably refers to standard natural numbers. This follows from our GA, since $\exp(x) = \exp(x/2n)^{2n} > (x/2n)^{2n} \ge x^n$ as long as, say, $x \ge (2n)^2$. On the other hand, it is easy to see that if there is $m \in \mathbb{N}$ such that $\exp(x) > x$ holds for all $x \ge m$, then it holds for all $x \in R$, thus our axiom is equivalent to Ressayre's formulation.

Presburger arithmetic is the complete theory of the structure $\langle \mathbb{N}, 0, 1, +, < \rangle$. Models of Presburger arithmetic are exactly the nonnegative parts of *$\mathbb{Z}$-groups*, which are discrete ordered abelian groups $\langle Z, 0, +, < \rangle$ with a least positive element 1 such that $Z/\mathbb{Z}$ is divisible, where we identify $\mathbb{Z}$ with the subgroup of Z generated by 1. There is an (easily proved) baby version of Theorem 2.1: $\mathbb{Z}$-groups are exactly the IPs of divisible ordered abelian groups (where an IP of an ordered group is defined analogously to rings, but without multiplication).

In theories extending PA^-, *existential bounded quantifiers* $\exists x \le t\, \varphi(x, \dots)$ (where t is a term that does not contain x) are defined as shorthands for $\exists x\, (x \le t \land \varphi(x, \dots))$, and *universal bounded quantifiers* $\forall x \le t\, \varphi(x, \dots)$ are shorthands for $\forall x\, (x \le t \to \varphi(x, \dots))$. A *bounded formula* is one that only uses bounded quantifiers. The set of all bounded $\mathcal{L}_{\mathrm{OR}}$-formulas is denoted Δ_0. An $\mathcal{L}_{\mathrm{OR}}$-formula is E_k (resp., U_k) if it can be written with k alternating (possibly empty) blocks of bounded quantifiers followed by a quantifier-free formula, with the first block being existential (resp., universal). If Γ is a formula class such as Δ_0 or E_k, $\mathsf{I}\Gamma$ denotes the theory axiomatized by PA^- (or just Q) and (φ-IND) for formulas $\varphi \in \Gamma$ (thus, $\mathsf{IE}_0 = \mathsf{IOpen}$).

We define the divisibility predicate $x \mid y$ as $\exists z\, xz = y$ (thus all elements divide 0). Over PA^-, the existential quantifier can be bounded by $z \le y$, thus $x \mid y$ is an E_1 formula; it is equivalent to the U_1 formula $\forall q \le y\, \forall r < x\, (y = qx + r \to r = 0)$ over IOpen.

The theory Δ^{b}_1-CR of Johannsen and Pollett [8] is a weak theory of bounded arithmetic in the style of Buss's theories (cf. [5, §V.4]) that corresponds to the complexity class TC^0. It is bi-interpretable (RSUV-isomorphic) to the more commonly used two-sorted Zambella-style theory VTC^0 (see [4]), but since our interest lies in embedding the universe of the theory with its $\mathcal{L}_{\mathrm{OR}}$-structure as EIP in other structures, it is more natural to consider the one-sorted version of the theory. It was proved in Jeřábek [7] that every countable model of Δ^{b}_1-CR is an EIP of a RCEF satisfying GA (despite the fact that the natural exponentiation function in Δ^{b}_1-CR is only defined on an initial segment of small integers). Proper definitions of Δ^{b}_1-CR and VTC^0 as well as more context can be found in the references above; readers unfamiliar with these theories may safely skip the few places where they are mentioned below.

We use $\log x$ to denote the base-2 logarithm of x, with the convention that $\log x = 0$ for $x \le 1$ (i.e., it is really $\max\{0, \log_2 x\}$). We denote the natural logarithm by $\ln x$, and general base-b logarithm by $\log_b x$.

We will also need two tools from model theory. The first is Robinson's joint consistency theorem (see e.g. Hodges [6, Cor. 9.5.8]):

Theorem 2.2 *Let T be a complete $\mathcal{L}$-theory, and for $i = 0, 1$, let $T_i \supseteq T$ be a consistent $\mathcal{L}_i$-theory, where $\mathcal{L}_0 \cap \mathcal{L}_1 = \mathcal{L}$. Then $T_0 \cup T_1$ is consistent.* □

Recursive saturation was introduced by Barwise and Schlipf [1]. Let $\mathfrak{M} = \langle M, \dots \rangle$ be a structure in a finite language $\mathcal{L}$. If $\vec{a} \in M$ and $\Gamma(x, \vec{y})$ is a recursive set of $\mathcal{L}$-formulas, then $\Gamma(x, \vec{a})$ is a *recursive type* of $\mathfrak{M}$, which is *finitely satisfiable* if $\mathfrak{M} \vDash \exists x \bigwedge_{\varphi \in \Gamma'} \varphi(x, \vec{a})$ for each finite $\Gamma' \subseteq \Gamma$, and *realized* by $c \in M$ if $\mathfrak{M} \vDash \Gamma(c, \vec{a})$. Then $\mathfrak{M}$ is *recursively saturated* if every finitely satisfiable recursive type of $\mathfrak{M}$ is realized in $\mathfrak{M}$. We will use the fact that every countable $\mathcal{L}$-structure has a countable recursively saturated elementary extension.

3 Exponential integer parts in a language with 2^x or P_2

We start by axiomatizing the theory of EIP of RCEF in a language with 2^x, which is fairly straightforward.

Definition 3.1 TEIP_{2^x} is a theory in the language $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$ extending IOpen by the axioms

(2^x-IP)	$x > 0 \to \exists y\, x < 2^y \le 2x,$
(2^x-Mul)	$2^{x+y} = 2^x 2^y,$
(2^x-Pos)	$2^x > 0.$

$\mathsf{TEIP}^+_{2^x}$ is defined similarly, but with axiom

(2^x-GA)	$2^x > x$

in place of (2^x-Pos).

By doubling/halving x (which corresponds to shifting y by 1), (2^x-IP) is equivalent to

$$x > 0 \to \exists y\, 2^y \le x < 2 \cdot 2^y,$$

which would match more closely the axioms of TEIP_{P_2} and TEIP that will be given further on, but the version here looks more visually pleasing.

Theorem 3.2 *The first-order theory of EIP of RCEF in $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$ is TEIP_{2^x}. The first-order theory of EIP of RCEF satisfying GA in $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$ is $\mathsf{TEIP}^+_{2^x}$.*

Proof: It is clear that any EIP of a RCEF satisfies the given axioms. Conversely, assume that $\mathfrak{M} = \langle M, 0, 1, +, \cdot, <, 2^x\rangle \vDash \mathsf{TEIP}_{2^x}$. Since $\mathfrak{M} \vDash \mathsf{IOpen}$, $\mathfrak{M}_\pm$ is an IP of a RCF $\mathfrak{R}$ by Theorem 2.1. There exists an elementary extension $\mathfrak{R}^* = \langle R^*, M^*, 0, 1, +, \cdot, <, 2^x\rangle$ of $\langle R, M, 0, 1, +, \cdot, <, 2^x\rangle$ that expands to a RCEF $\langle \mathfrak{R}^*, \exp\rangle$ by Theorem 2.2 (applied with T_0 being the elementary diagram of $\langle R, M, 0, 1, +, \cdot, <, 2^x\rangle$ and T_1 the theory of RCEF, with common language $\mathcal{L}_{\mathrm{OR}}$), using the completeness of the theory RCF. Let $M^*_\pm = M^* \cup \{-a : a \in M\}$, and extend $2^x\colon M^* \to M^*_{>0}$ to a function $2^x\colon M^*_\pm \to R^*_{>0}$ by $2^{-x} = (2^x)^{-1}$. Applying (2^x-IP) with $x = 1$, there exists $y \in M^*$ such that $2^y = 2$; depending on the parity of y, (2^x-Mul) implies $2 = (2^{y/2})^2$ (which is impossible) or $2 = 2^1 \cdot (2^{\lfloor y/2 \rfloor})^2$, thus $2^1 = 2$. Then using (2^x-Mul) and (2^x-Pos), 2^x is strictly increasing, hence it is an ordered group embedding $\langle M^*_\pm, 0, +, <\rangle \to \langle R^*_{>0}, 1, \cdot, <\rangle$.

Putting $B = \{x \in R^* : \exists n \in \mathbb{N}\, |x| \le n\}$, we define a new exponential $\overline{\exp}\colon R^* \to R^*_{>0}$ by

$$\overline{\exp}(a + r) = 2^a \exp(r), \qquad a \in M^*_\pm, r \in B.$$

To see that this is well defined, if $a + r = a' + r'$ with $a, a' \in M^*_\pm$ and $r, r' \in B$, then $n = a - a' = r' - r \in B \cap M^*_\pm = \mathbb{Z}$, hence both $2^{a-a'}$ and $\exp(r' - r)$ coincide with the usual value of 2^n, which implies $2^a \exp(r) = 2^{a'} \exp(r')$. The function $\overline{\exp}$ is defined on all of R^* as $M^*_\pm$ is an IP of R^*.

It follows easily that $\overline{\exp}$ is a homomorphism $\langle R^*, 0, +\rangle \to \langle R^*_{>0}, 1, \cdot\rangle$ using the corresponding properties of 2^x and exp, and $\overline{\exp}(x) > 1$ for $x > 0$, thus $\overline{\exp}$ is strictly increasing. It is also surjective: if $y \in R^*_{>0}$, (2^x-IP) implies that there is $a \in M^*_\pm$ such that $2^{-a}y \in [1,2]$, thus using the surjectivity and monotonicity of exp, $2^{-a}y = \exp(x)$ for some $x \in [0,1]$, whence $y = \overline{\exp}(a+x)$. That is, $\langle R^*, 0, 1, +, \cdot, <, \overline{\exp}\rangle$ is an RCEF, and $\langle M^*_\pm, 0, 1, +, \cdot, <, 2^x\rangle$ is its EIP.

If $\mathfrak{M}$ and $\mathfrak{M}^*$ additionally satisfy (2^x-GA), then $\overline{\exp}(x) > x$ for all x: this holds trivially if $x \le 0$; otherwise, we can write $x = a + r$ with $a \in M$ and $r \in [0,1)$, thus $2^x \ge 2^a \ge a + 1 > x$. □

Next, we move to a language that only has a predicate P_2 for the image of 2^x rather than 2^x itself. It turns out that the resulting theory is the same irrespective of whether we demand the RCEF to satisfy the growth axiom; but whereas in absence of GA, the proof is still straightforward, the GA case is considerably more complicated.

Definition 3.3 TEIP_{P_2} is a theory in the language $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ extending IOpen by the axioms

(P_2-IP) $\qquad x > 0 \to \exists u\,(P_2(u) \wedge u \le x < 2u)$,

(P_2-Div) $\qquad P_2(u) \wedge P_2(v) \wedge u \le v \to \exists w\,(P_2(w) \wedge uw = v)$.

TEIP'_{P_2} is a theory in the language $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ extending IOpen by the axioms

(P_2-IP!) $\qquad x > 0 \to \exists! u\,(P_2(u) \wedge u \le x < 2u)$,

(P_2-Pos) $\qquad \neg P_2(0)$,

(P_2-Mul) $\qquad P_2(u) \wedge P_2(v) \to P_2(uv)$.

Lemma 3.4 TEIP_{P_2} *is equivalent to* TEIP'_{P_2}*, and it proves* $P_2(1)$ *and* $P_2(2)$*.*

Proof:

$\mathsf{TEIP}_{P_2} \vdash \mathsf{TEIP}'_{P_2}$: The existence part of (P_2-IP!) is just (P_2-IP); for uniqueness, if u and u' satisfy the conclusion, and, say, $u \le u'$, then $u \mid u'$ by (P_2-Div), while $u' < 2u$. Thus, the only possibility is $u = u'$.

Applying (P_2-IP) with $x = 1$, we see that $P_2(1)$. Then (P_2-Div) gives $\neg P_2(0)$ as $0 \nmid 1$.

Assume $P_2(u)$ and $P_2(v)$. If $u = 1$ or $v = 1$, then $P_2(uv)$ holds trivially, hence we may also assume $u, v \ge 2$. By (P_2-IP), there is w such that $P_2(w)$ and $w \le uv < 2w$. Since $2u \le uv$, we have $u < w$, hence (P_2-Div) implies $u \mid w$ and $P_2(w/u)$. Moreover, $w/u \le v < 2w/u$, thus $w/u = v$ by the uniqueness part of (P_2-IP!), i.e., $P_2(uv)$.

$\mathsf{TEIP}'_{P_2} \vdash \mathsf{TEIP}_{P_2}$: ($P_2$-IP) follows from ($P_2$-IP!). Assume that $P_2(u)$, $P_2(v)$, and $u \le v$. We have $u > 0$ by (P_2-Pos), whence IOpen implies the existence of $x > 0$ such that $ux \le v < u(x+1)$. By (P_2-IP!), there is w such that $P_2(w)$ and $w \le x < 2w$, i.e., $uw \le v < 2uw$. Then $P_2(uw)$ by (P_2-Mul), hence $uw = v$ by the uniqueness part of (P_2-IP!).

We have already seen that $\mathsf{TEIP}_{P_2} \vdash P_2(1)$. Likewise, an application of (P_2-IP) with $x = 2$ gives $P_2(2)$. □

Lemma 3.5 *If* $\mathfrak{M} = \langle M, 0, 1, +, \cdot, <, P_2\rangle \vDash \mathsf{TEIP}_{P_2}$*, then* $\langle P_2, 1, 2, \cdot, <\rangle$ *is a model of Presburger arithmetic.*

Proof: Let $\mathfrak{R} = \langle R, \dots\rangle$ be a RCF such that $\mathfrak{M}_\pm$ is its IP using Theorem 2.1. Let $P_2^{\pm 1} = \{u, u^{-1} : u \in P_2\} \subseteq R_{>0}$. Using Lemma 3.4, $\langle P_2^{\pm 1}, 1, \cdot, <\rangle$ is a discrete ordered abelian group with a least positive element 2, and it is an IP of the divisible ordered group $\langle R_{>0}, 1, \cdot, <\rangle$. Thus, it is a $\mathbb{Z}$-group, and its "nonnegative" part $\langle P_2, 1, 2, \cdot, <\rangle$ is a model of Presburger. $\square$

For the construction of TEIP in the next section, it will be convenient to consider yet another axiomatization of TEIP_{P_2} that may look less intuitive, but has the advantage that it only involves one positive occurrence of P_2:

Definition 3.6 TEIP''_{P_2} is a theory in the language $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ extending IOpen by the axioms (P_2-IP), (P_2-Pos), and

(P_2-Univ) $$P_2(u) \wedge P_2(v) \wedge P_2(w) \to \neg(uv < w < 2uv).$$

Lemma 3.7 TEIP'_{P_2} *is equivalent to* TEIP''_{P_2}.

Proof:

$\mathsf{TEIP}'_{P_2} \vdash \mathsf{TEIP}''_{P_2}$: For ($P_2$-Univ), if $P_2(u)$, $P_2(v)$, and $P_2(w)$, then $P_2(uv)$ by (P_2-Mul), hence the uniqueness part of (P_2-IP!) precludes $uv < w < 2uv$.

$\mathsf{TEIP}''_{P_2} \vdash \mathsf{TEIP}'_{P_2}$: First, ($P_2$-IP) implies $P_2(1)$, hence (P_2-Univ) gives $P_2(u) \wedge P_2(u') \to \neg(u < u' < 2u)$, which is the uniqueness part of (P_2-IP!); thus, we have (P_2-IP!) and (P_2-Pos). For (P_2-Mul), assuming $P_2(u)$ and $P_2(v)$, there is w such that $P_2(w)$ and $uv \le w < 2uv$ by (P_2-IP); we must have $w = uv$ by (P_2-Univ). $\square$

Theorem 3.8 *The first-order theory of EIP of RCEF in* $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ *is* TEIP_{P_2}.

Proof: In view of Theorem 3.2, it suffices to show that TEIP_{2^x} is a conservative extension of TEIP_{P_2} when $P_2(u)$ is interpreted as $\exists x\, u = 2^x$. Clearly, TEIP_{2^x} proves TEIP_{P_2}.

On the other hand, if $\mathfrak{M} = \langle M, 0, 1, +, \cdot, <, P_2\rangle \vDash \mathsf{TEIP}_{P_2}$, then using IOpen and Lemma 3.5, the structures $\langle M, 0, 1, +, <\rangle$ and $\langle P_2, 1, 2, \cdot, <\rangle$ are both models of Presburger arithmetic, hence elementarily equivalent. It follows from the joint consistency theorem that $\mathfrak{M}$ has an elementary extension $\mathfrak{M}^* = \langle M^*, 0, 1, +, \cdot, <, P_2^*\rangle$ such that $\langle M^*, 0, 1, +, <\rangle$ and $\langle P_2^*, 1, 2, \cdot, <\rangle$ are isomorphic. (Theorem 2.2 is applied here such that $\mathcal{L}_0$ is $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ expanded with constants for elements of M, $\mathcal{L}_1 = \{\overline{s} : s \in \mathcal{L}_0\}$ is a copy of $\mathcal{L}_0$ with a disjoint set of symbols except that we identify $0 = \overline{1}$, $1 = \overline{2}$, $+ = \overline{\cdot}$, and $< = \overline{<}$, T_0 and T_1 are the elementary diagram of $\mathfrak{M}$ formulated using the respective languages, and T is Presburger arithmetic.) If 2^x is such an isomorphism, then $\langle \mathfrak{M}^*, 2^x\rangle \vDash \mathsf{TEIP}_{2^x}$. $\square$

The growth axiom interconnects the structures $\langle M, 0, 1, +, <\rangle$ and $\langle P_2, 1, 2, \cdot, <\rangle$ in a way that seems to preclude a similarly easy proof of the extension of Theorem 3.8 to $\mathsf{TEIP}^+_{2^x}$. One idea that does not work is to use the joint consistency theorem to expand an elementary extension of $\mathfrak{M}$ to a model of $\mathrm{Th}(\langle \mathbb{N}, 0, 1, +, <, 2^x\rangle)$, taking $\mathrm{Th}(\langle \mathbb{N}, 0, 1, +, <, \cdot \restriction P_2\rangle)$ as the common subtheory: since $\mathrm{Th}(\langle \mathbb{N}, 0, 1, +, <, 2^x\rangle)$ is decidable due to Semenov [12], its reduct

$\mathrm{Th}(\langle \mathbb{N}, 0, 1, +, <, \cdot \restriction P_2 \rangle)$ is recursively axiomatizable, thus in principle it might be possible to take its axiomatization by a few natural axioms or schemata and check that it is included in TEIP_{P_2}. This fails for two reasons: first, even though $\mathrm{Th}(\langle \mathbb{N}, 0, 1, +, <, 2^x \rangle)$ is explicitly axiomatized in Cherlin and Point [3], we do not know of a similar axiomatization of $\mathrm{Th}(\langle \mathbb{N}, 0, 1, +, <, \cdot \restriction P_2 \rangle)$ in the literature, and this would likely require some work to devise. Second, $\mathsf{TEIP}^+_{2^x}$ does *not*, in fact, include even the weaker theory $\mathrm{Th}(\langle \mathbb{N}, 0, 1, +, <, P_2 \rangle)$: as we will see below, it does not prove that powers of 2 are not divisible by 3.

In absence of a better idea, we will get our hands dirty and construct the required 2^x obeying GA by a back-and-forth argument (cf. [7, Thm. 6.4]):

Theorem 3.9 *The first-order theory of EIP of RCEF satisfying GA in $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ is TEIP_{P_2}.*

Proof: It suffices to show that $\mathsf{TEIP}^+_{2^x}$ is conservative over TEIP_{P_2}. Let $\mathfrak{M} = \langle M, 0, 1, +, \cdot, <, P_2 \rangle$ be a countable recursively saturated model of TEIP_{P_2}; we will show that it expands to a model of $\mathsf{TEIP}^+_{2^x}$. Let $\mathfrak{R}$ be a RCF whose IP is $\mathfrak{M}_\pm$, $P_2^{\pm 1} = \{u, u^{-1} : u \in P_2\} \subseteq R_{>0}$, $B = \{x \in R : \exists n \in \mathbb{N}\, |x| \le n\}$, and $B^\times = \{x \in R : \exists n \in \mathbb{N}\, n^{-1} \le x \le n\}$. If $u, v \in P_2^{\pm 1}$ and $m \in \mathbb{N}_{>0}$, $u \equiv^\times v \pmod{m}$ means $uv^{-1} = w^m$ for some $w \in P_2^{\pm 1}$; by Lemma 3.5, $u \equiv^\times 2^l \pmod{m}$ for a unique l such that $0 \le l < m$.

Fix enumerations $M = \langle c_i : i \in \omega \rangle$ and $P_2 = \langle d_i : i \in \omega \rangle$. We will construct sequences $\langle a_i : i \in \omega \rangle \subseteq M$ and $\langle b_i : i \in \omega \rangle \subseteq P_2$ so that they satisfy the following properties for each $k \ge 1$ by induction on k:

(i) $a_0 = 1$, $b_0 = 2$, $a_{2i+2} = c_i$, $b_{2i+1} = d_i$.

(ii) For all $\vec{q} \in \mathbb{Q}^k$, $\sum_{i<k} q_i a_i = 0 \implies \prod_{i<k} b_i^{q_i} = 1$. (Here, $b_i^{q_i} \in R_{>0}$.)

(iii) For all $0 \le l < m \in \mathbb{N}$ and $i < k$, $a_i \equiv l \pmod{m} \implies b_i \equiv^\times 2^l \pmod{m}$.

(iv) For all $\vec{q} \in \mathbb{Q}^k$, $\prod_{i<k} b_i^{q_i} > \sum_{i<k} q_i a_i$.

We observe that conditions (ii) and (iii) can be stated with $\iff$ in place of $\implies$. For (iii), this follows from the uniqueness of $l < m$ such that $a_i \equiv l \pmod{m}$, resp. $b_i \equiv^\times 2^l \pmod{m}$. For (ii), this follows from (iv): if $\sum_i q_i a_i \ne 0$, then $\sum_i n q_i a_i \ge 1$ for some $n \in \mathbb{Z}$, thus $\left(\prod_i b_i^{q_i}\right)^n > 1$ by (iv), and in particular, $\prod_i b_i^{q_i} \ne 1$. The same argument actually shows that the conditions imply

$$\sum_{i<k} q_i a_i > 0 \iff \prod_{i<k} b_i^{q_i} > 1, \tag{1}$$

and likewise,

$$\sum_{i<k} q_i a_i > \mathbb{N} \iff \prod_{i<k} b_i^{q_i} > \mathbb{N}: \tag{2}$$

the left-to-right implication follows from (iv), while if $\sum_{i<k} q_i a_i < n$ for some $n \in \mathbb{N}$, then (iv) applied to $n a_0 - \sum_i q_i a_i > 0$ gives $\prod_i b_i^{q_i} < 2^n$.

We also observe that condition (iv) is equivalent to

$$\sum_{i<k} q_i a_i > \mathbb{N} \implies \prod_{i<k} b_i^{q_i} > \sum_{i<k} q_i a_i \tag{3}$$

for all $\vec{q} \in \mathbb{Q}^k$, as other conditions imply the conclusion when $\sum_i q_i a_i > \mathbb{N}$ does not hold: let $r = \sum_i q_i a_i$. If $r \le 0$, there is nothing to prove, as $\prod_{i<k} b_i^{q_i} > 0$. If $0 \le r \in B$, then $r \in \mathbb{Q}$ (if $q_i = n_i/m$ for some $\vec{n}, m \in \mathbb{Z}$, $m > 0$, then $mr = \sum_i n_i a_i \in M \cap B = \mathbb{Z}$ as $\mathfrak{M}$ is a model of Presburger arithmetic). Then in view of (i), $\sum_i q_i a_i - r a_0 = 0$ implies $b_0^{-r} \prod_i b_i^{q_i} = 1$ by (ii), i.e., $\prod_i b_i^{q_i} = 2^r > r$ (referring to the standard exponential).

It is clear that after we finish the construction, the conditions ensure that $a_i \mapsto b_i$ defines an isomorphism $2^x \colon \langle M, 0, 1, +, < \rangle \to \langle P_2, 1, 2, \cdot, < \rangle$, and $\langle \mathfrak{M}, 2^x \rangle \models \mathsf{TEIP}^+_{2^x}$.

We now proceed with the construction. For $k = 1$, we put $a_0 = 1$, $b_0 = 2$ as requested by (i); then (ii)–(iv) hold. Having constructed $\langle a_i : i < k \rangle$ and $\langle b_i : i < k \rangle$ satisfying (ii)–(iv), we will construct a_k and b_k as follows.

Assume that k is even. Put $a_k = c_{k/2-1}$; we need to find a matching $b_k \in P_2$. First, if $a_k + \sum_{i<k} q_i a_i \in B$ for some $\vec{q} \in \mathbb{Q}^k$, then $a_k = \sum_{i<k} q_i a_i$ for some $\vec{q} \in \mathbb{Q}^k$ by the same argument as in the equivalence of (iv) and (3) above, and we define $b_k = \prod_{i<k} b_i^{q_i}$. Write $q_i = n_i/m$ for some $\vec{n} \in \mathbb{Z}^k$ and $m \in \mathbb{N}_{>0}$, and let $0 \le l_i < m$ be such that $a_i \equiv l_i \pmod{m}$. Then $0 \equiv m a_k \equiv \sum_i n_i l_i \pmod{m}$. Using (iii) from the induction hypothesis, $b_i \equiv^\times 2^{l_i} \pmod{m}$, thus $\prod_i b_i^{n_i} \equiv^\times 2^{\sum_i n_i l_i} \equiv^\times 1 \pmod{m}$. This shows that $b_k = \left(\prod_i b_i^{n_i}\right)^{1/m} \in P_2$; moreover, an analogous argument gives (iii). Conditions (ii) and (iv) follow from the induction hypothesis.

Now, assume that $a_k + \sum_i q_i a_i \notin B$ for all $\vec{q} \in \mathbb{Q}^k$. Then condition (ii) will follow from the induction hypothesis for whatever choice of b_k, hence we only need b_k to satisfy (iii) and (3). Condition (3) for $q_k = 0$ follows from the induction hypothesis. For $q_k > 0$, the condition

$$q_k a_k + \sum_{i<k} q_i a_i > \mathbb{N} \implies b_k^{q_k} \prod_{i<k} b_i^{q_i} > q_k a_k + \sum_{i<k} q_i a_i \tag{4}$$

is equivalent to

$$a_k > \sum_{i<k} r_i a_i \implies b_k \prod_{i<k} b_i^{-r_i} > \left[q_k \Big(a_k - \sum_{i<k} r_i a_i \Big) \right]^{1/q_k}, \tag{5}$$

where $r_i = -q_i/q_k$ (using that $a_k - \sum_{i<k} r_i a_i > 0$ implies $a_k - \sum_{i<k} r_i a_i > \mathbb{N}$). Also, we have $q_k \Big(a_k - \sum_i r_i a_i \Big) < \Big(a_k - \sum_i r_i a_i \Big)^2$, thus (5) holds for all $q_k > 0$ and $\vec{q} \in \mathbb{Q}^k$ iff

$$a_k > \sum_{i<k} r_i a_i \implies b_k > \Big(a_k - \sum_{i<k} r_i a_i \Big)^n \prod_{i<k} b_i^{r_i} \tag{6}$$

holds for all $\vec{r} \in \mathbb{Q}^k$ and $n \in \mathbb{N}$. Likewise, (4) for all $q_k < 0$ and $\vec{q} \in \mathbb{Q}^k$ is equivalent to

$$a_k < \sum_{i<k} q_i a_i \implies b_k < \Big(\sum_{i<k} q_i a_i - a_k \Big)^{-n} \prod_{i<k} b_i^{q_i} \tag{7}$$

for all $\vec{q} \in \mathbb{Q}^k$ and $n \in \mathbb{N}$. Thus, to satisfy conditions (ii)–(iv), it is enough to take for b_k any realizer of the type

$$\begin{aligned}\Gamma(x) = \{P_2(x)\} &\cup \{a_k \equiv l \pmod{m} \to x \equiv^\times 2^l \pmod{m} : 0 \le l < m \in \mathbb{N}\} \\ &\cup \Big\{a_k > \sum_{i<k} r_i a_i \to x > \Big(a_k - \sum_{i<k} r_i a_i\Big)^n \prod_{i<k} b_i^{r_i} : \vec{r} \in \mathbb{Q}^k, n \in \mathbb{N}\Big\} \\ &\cup \Big\{a_k < \sum_{i<k} q_i a_i \to x < \Big(\sum_{i<k} q_i a_i - a_k\Big)^{-n} \prod_{i<k} b_i^{q_i} : \vec{q} \in \mathbb{Q}^k, n \in \mathbb{N}\Big\}.\end{aligned}$$

Observe that $\Gamma(x)$ can indeed be expressed as a recursive type in $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ with parameters $\vec{a}, \vec{b}$: e.g., if $r_i = n_i/m$ with $\vec{n} \in \mathbb{Z}^k$ and $m \in \mathbb{N}_{>0}$, then $x > (\cdots)^n \prod_i b_i^{r_i}$ is equivalent to $x^m \prod_{n_i<0} b_i^{-n_i} > (\cdots)^{nm} \prod_{n_i>0} b_i^{n_i}$, etc. Thus, using the recursive saturation of $\mathfrak{M}$, it only remains to check that every finite $\Gamma_0 \subseteq \Gamma$ is satisfiable.

Apart from $P_2(x)$, the formulas in Γ_0 are implications whose premises do not depend on x; we may discard those whose premises are false, and simplify the remaining ones by removing their premises. If $a_k \equiv l_j \pmod{m_j}$ for $j < t$, then $a_k \equiv l \pmod{m}$, where $m = \operatorname{lcm}(m_0, \dots, m_{t-1})$ and $l \equiv l_j \pmod{m_j}$; then $x \equiv^\times 2^l \pmod{m}$ implies $x \equiv^\times 2^{l_j} \pmod{m_j}$ for each $j < t$. Thus, we may assume Γ_0 contains only one congruence $x \equiv^\times 2^l \pmod{m}$. Likewise, we can take the maximum (minimum) right-hand side among the inequalities $x > \cdots$ ($x < \cdots$, resp.), thus we may assume that Γ_0 contains one inequality of the form $x > \cdots$ (we may assume there is at least one by considering e.g. $\vec{r} = \vec{0}$ and $n = 0$, which gives $x > 1$), and at most one inequality of the form $x < \cdots$. If there is no inequality $x < \cdots$, it is easy to see that Γ_0 is satisfiable, hence we may assume that

$$\Gamma_0 = \Big\{P_2(x), x \equiv^\times 2^l \pmod{m}, \Big(a_k - \sum_{i<k} r_i a_i\Big)^n \prod_{i<k} b_i^{r_i} < x, x < \Big(\sum_{i<k} q_i a_i - a_k\Big)^{-n} \prod_{i<k} b_i^{q_i}\Big\}$$

for some $0 \le l < m \in \mathbb{N}$, $\vec{q}, \vec{r} \in \mathbb{Q}^k$, and $n \in \mathbb{N}$, where

$$\sum_{i<k} r_i a_i < a_k < \sum_{i<k} q_i a_i.$$

(We may assume both inequalities use the same n by enlarging one if necessary.) Since $P_2^\pm$ is an IP of $\langle R_{>0}, 1, \cdot, < \rangle$ (cf. Lemma 3.5), there exists an element $x \in P_2$ satisfying $x \equiv^\times 2^l \pmod{m}$ in any interval $[u, v)$ such that $v \ge 2^m u > 0$. Thus, Γ_0 is satisfiable if

$$\Big(\sum_{i<k} q_i a_i - a_k\Big)^{-n} \prod_{i<k} b_i^{q_i} > 2^m \Big(a_k - \sum_{i<k} r_i a_i\Big)^n \prod_{i<k} b_i^{r_i},$$

i.e.,

$$\prod_{i<k} b_i^{q_i - r_i} > 2^m \Big(a_k - \sum_{i<k} r_i a_i\Big)^n \Big(\sum_{i<k} q_i a_i - a_k\Big)^n. \tag{8}$$

Now, using $\sum_i (q_i - r_i) a_i > \mathbb{N}$, we have

$$\Big(\frac{1}{2n+1} \sum_{i<k} (q_i - r_i) a_i\Big)^{2n+1} > 2^m \Big(a_k - \sum_{i<k} r_i a_i\Big)^n \Big(\sum_{i<k} q_i a_i - a_k\Big)^n,$$

whence (8) follows from the instance

$$\prod_{i<k} b_i^{(q_i-r_i)/(2n+1)} > \sum_{i<k} \frac{q_i - r_i}{2n+1} a_i$$

of the induction hypothesis. This finishes the construction of a_k and b_k for k even.

Let k be odd, and put $b_k = d_{(k-1)/2}$; we will find a suitable a_k. If $b_k \prod_{i<k} b_i^{q_i} \in B^\times$ for some $\vec{q} \in \mathbb{Q}^k$, then as in the case of even k, we obtain $b_k = \prod_{i<k} b_i^{q_i}$ for some $\vec{q} \in \mathbb{Q}^k$, and then $a_k = \sum_{i<k} q_i a_i$ will satisfy (ii)–(iv). Thus, we may assume

$$b_k \prod_{i<k} b_i^{q_i} \notin B^\times \tag{9}$$

for all $\vec{q} \in \mathbb{Q}^k$. Then (ii) and (iv) will hold if a_k satisfies

$$b_k^{q_k} \prod_{i<k} b_i^{q_i} > 1 \implies b_k^{q_k} \prod_{i<k} b_i^{q_i} > q_k a_k + \sum_{i<k} q_i a_i > 0$$

for all $q_k \neq 0$ and $\vec{q} \in \mathbb{Q}^k$. Similarly to the case of even k, one can check that this amounts to the conditions

$$\begin{aligned}
b_k > \prod_{i<k} b_i^{q_i} &\implies \sum_{i<k} q_i a_i < a_k < \sum_{i<k} q_i a_i + \Big(b_k \prod_{i<k} b_i^{-q_i}\Big)^{1/n}, \\
b_k < \prod_{i<k} b_i^{q_i} &\implies \sum_{i<k} q_i a_i - \Big(b_k^{-1} \prod_{i<k} b_i^{q_i}\Big)^{1/n} < a_k < \sum_{i<k} q_i a_i
\end{aligned}$$

for all $\vec{q} \in \mathbb{Q}^k$ and $n \in \mathbb{N}_{>0}$. Thus, using recursive saturation, it suffices to show that each finite subset Γ_0 of the type

$$\begin{aligned}
\Gamma(x) = &\big\{x \equiv l \pmod m : 0 \le l < m \in \mathbb{N}, b_k \equiv^\times 2^l \pmod m\big\} \\
&\cup \Big\{x > \sum_{i<k} q_i a_i : \vec{q} \in \mathbb{Q}^k, b_k > \prod_{i<k} b_i^{q_i}\Big\} \\
&\cup \Big\{x < \sum_{i<k} r_i a_i : \vec{r} \in \mathbb{Q}^k, b_k < \prod_{i<k} b_i^{r_i}\Big\} \\
&\cup \Big\{x > \sum_{i<k} s_i a_i - \Big(b_k^{-1} \prod_{i<k} b_i^{s_i}\Big)^{1/n} : \vec{s} \in \mathbb{Q}^k, n \in \mathbb{N}_{>0}, b_k < \prod_{i<k} b_i^{s_i}\Big\} \\
&\cup \Big\{x < \sum_{i<k} t_i a_i + \Big(b_k \prod_{i<k} b_i^{-t_i}\Big)^{1/n} : \vec{t} \in \mathbb{Q}^k, n \in \mathbb{N}_{>0}, b_k > \prod_{i<k} b_i^{t_i}\Big\}
\end{aligned}$$

is satisfiable. (To make the type recursive, we would write it with implications as in the case of even k.) Again, we may assume that Γ_0 consists of one congruence $x \equiv l \pmod m$, one lower bound on x, and one upper bound; it will be satisfiable as long as the difference between the upper and lower bounds is larger than m. Thus, assume that

$$\prod_{i<k} b_i^{q_i}, \prod_{i<k} b_i^{t_i} < b_k < \prod_{i<k} b_i^{r_i}, \prod_{i<k} b_i^{s_i};$$

we need to check that

$$\sum_{i<k} q_i a_i + m < \sum_{i<k} r_i a_i, \tag{10}$$

$$\sum_{i<k} q_i a_i + m < \sum_{i<k} t_i a_i + \Big(b_k \prod_{i<k} b_i^{-t_i}\Big)^{1/n}, \tag{11}$$

$$\sum_{i<k} s_i a_i - \Big(b_k^{-1} \prod_{i<k} b_i^{s_i}\Big)^{1/n} + m < \sum_{i<k} r_i a_i, \tag{12}$$

$$\sum_{i<k} s_i a_i - \Big(b_k^{-1} \prod_{i<k} b_i^{s_i}\Big)^{1/n} + m < \sum_{i<k} t_i a_i + \Big(b_k \prod_{i<k} b_i^{-t_i}\Big)^{1/n}. \tag{13}$$

Since $\prod_i b_i^{r_i - q_i} > \mathbb{N}$ by (9), (10) follows from (2). For (11), we have

$$\sum_{i<k} (q_i - t_i) a_i + m = n\Big(\sum_{i<k} \frac{q_i - t_i}{n} a_i + \frac{m}{n} a_0\Big) < n 2^{m/n} \prod_{i<k} b_i^{(q_i - t_i)/n} < \Big(b_k \prod_{i<k} b_i^{-t_i}\Big)^{1/n},$$

using (iv) and $b_k > n^n 2^m \prod_i b_i^{q_i}$ (from (9)); the argument for (12) is similar. Finally,

$$\begin{aligned}
\sum_{i<k} (s_i - t_i) a_i + m &= (2n+1)\Big(\sum_{i<k} \frac{s_i - t_i}{2n+1} a_i + \frac{m}{2n+1}\Big) \\
&< (2n+1) 2^{m/(2n+1)} \prod_{i<k} b_i^{(s_i - t_i)/(2n+1)} \\
&< \prod_{i<k} b_i^{(s_i - t_i)/(2n)} \le \Big(b_k^{-1} \prod_{i<k} b_i^{s_i}\Big)^{1/n} + \Big(b_k \prod_{i<k} b_i^{-t_i}\Big)^{1/n}
\end{aligned}$$

using (iv),

$$\prod_{i<k} b_i^{s_i - t_i} = \Big(b_k^{-1} \prod_{i<k} b_i^{s_i}\Big)\Big(b_k \prod_{i<k} b_i^{-t_i}\Big) \le \max\Big(\Big\{b_k^{-1} \prod_{i<k} b_i^{s_i}, b_k \prod_{i<k} b_i^{-t_i}\Big\}\Big)^2,$$

and $\prod_{i<k} b_i^{s_i - t_i} > \mathbb{N}$, which follows from (9). □

Example 3.10 There exists a countable model of IOpen that expands to a model of TEIP_{P_2}, but not to a model of TEIP_{2^x}.

Proof: Let $\mathfrak{M}_\pm$ be the ring of Puiseux polynomials $\sum_{q \in Q} a_q x^q$ with $Q \subseteq \mathbb{Q}_{\ge 0}$ finite, a_q real algebraic, and $a_0 \in \mathbb{Z}$, ordered so that $x > \mathbb{N}$. Its nonnegative part $\mathfrak{M}$ is a model of IOpen by Shepherdson [13], and it can be checked readily that $\langle \mathfrak{M}, P_2 \rangle \vDash \mathsf{TEIP}_{P_2}$, where

$$P_2 = \{2^n x^q : q \in \mathbb{Q}_{\ge 0}, n \in \mathbb{Z}, (q > 0 \text{ or } n \ge 0)\}.$$

On the other hand, assume for contradiction that $\langle \mathfrak{M}, 2^x \rangle \vDash \mathsf{TEIP}_{2^x}$. Then 2^x extends to an ordered group embedding $2^x \colon \mathfrak{M}_\pm \to \mathfrak{F}^\times_{>0}$, where $\mathfrak{F}^\times_{>0} = \langle F_{>0}, 1, \cdot, < \rangle$ is the multiplicative group of positive elements of the fraction field $\mathfrak{F}$ of $\mathfrak{M}_\pm$. Since the image of 2^x is an IP of $\mathfrak{F}^\times_{>0}$, 2^x induces an isomorphism of the ordered groups $\mathfrak{M}_\pm/\mathbb{Z}$ and $\mathfrak{F}^\times_{>0}/B^\times$, where $B^\times = \{x \in F_{>0} : \exists n \in \mathbb{N}\, n^{-1} \le x \le n\}$. But every coset of $B^\times$ contains exactly one monomial x^q, $q \in \mathbb{Q}$, thus $\mathfrak{F}^\times_{>0}/B^\times \simeq \langle \mathbb{Q}, 0, +, < \rangle$ is archimedean, whereas $\mathfrak{M}_\pm/\mathbb{Z}$, isomorphic to the additive group of Puiseux polynomials with $a_0 = 0$, is nonarchimedean. This is a contradiction. □

4 Exponential integer parts in $\mathcal{L}_{\mathrm{OR}}$

We now turn to the most interesting case, namely the theory of EIP of RCEF in the basic language of arithmetic $\mathcal{L}_{\mathrm{OR}}$. Our axiomatization of this theory will express the existence of winning strategies in a certain game on integers. We describe the game first to motivate the definition of the theory.

Definition 4.1 Let $\mathfrak{M} \vDash \mathsf{IOpen}$ and $\alpha \le \omega$. The *power-of-2 game* $\mathrm{PowG}_\alpha(\mathfrak{M})$ is played between two players, *Challenger* (C) and *Powerator* (P), in α rounds: in each round $0 \le i < \alpha$, C picks $x_i \in M_{>0}$, and P responds with $u_i \in M_{>0}$ such that $u_i \le x_i < 2u_i$. C wins the game if $u_i u_j < u_h < 2u_i u_j$ for some $h, i, j < \alpha$, otherwise P wins.

More generally, if $t \le \alpha$ is finite, and $u_0, \dots, u_{t-1} \in M_{>0}$, let $\mathrm{PowG}^t_\alpha(\mathfrak{M}, \vec{u})$ denote the $\mathrm{PowG}_\alpha(\mathfrak{M})$ game where the first t responses by P are fixed as $\vec{u}$ (the values of x_i, $i < t$, do not matter, as they do not enter the winning condition; for definiteness, we may imagine $x_i = u_i$). We may write just $\mathrm{PowG}^t_\alpha(\vec{u})$ if $\mathfrak{M}$ is understood from the context.

While not being part of the official rules as we want to keep them simple, we will often use the following alternative conditions:

Observation 4.2

(i) If $u_i \le u_j$ and $u_i \nmid u_j$ for some $i, j < h < \alpha$, then Challenger can win the game in round h by playing $x_h = \lfloor u_j/u_i \rfloor$.

(ii) For any $x_i > 0$, Challenger can force Powerator to respond with u_i such that $x_i \le u_i < 2x_i$.

Proof: (i): P must respond with u_h such that $u_h \le x_h < u_j/u_i < 2u_h$, i.e., $u_h u_i < u_j < 2u_h u_i$.

(ii): Let C play $2x_i - 1$, so that $u_i \le 2x_i - 1 < 2u_i$. □

Remark 4.3 C cannot go wrong by restricting their moves to even numbers: instead of playing $2x + 1$, to which the valid responses of P are in $\{x + 1, \dots, 2x + 1\}$, C can play $2x$ with valid responses in $\{x + 1, \dots, 2x\}$, unless $x = 0$. A move $x_i = 1$, forcing P to reply with $u_i = 1$, can be eliminated as well: let C skip the move. The only way this can affect the game is when we reach a position with $u_j < u_h < 2u_j$ for some h, j (which would make C win as $1 \cdot u_j < u_h < 2 \cdot 1 \cdot u_j$); then C can play $x_l = 2(u_j u_h - 1)$ en lieu of the skipped round, forcing P to reply with $u_j u_h \le u_l < 2u_j u_h$ and lose, as either $u_j u_h < u_l < 2u_j u_h$ or $u_j^2 < u_l = u_j u_h < 2u_j^2$.

The intuition behind the game is that Powerator can win by playing powers of 2:

Lemma 4.4 *If $\langle \mathfrak{M}, P_2 \rangle \vDash \mathsf{TEIP}_{P_2}$, then Powerator has a winning strategy in $\mathrm{PowG}_\alpha(\mathfrak{M})$ for every $\alpha \le \omega$, and more generally, in $\mathrm{PowG}^t_\alpha(\mathfrak{M}, \vec{u})$ for every $t < \omega$, $t \le \alpha$, and $\vec{u} \subseteq P_2$.*

Proof: By Lemmas 3.4 and 3.7, $\langle \mathfrak{M}, P_2 \rangle \vDash \mathsf{TEIP}''_{P_2}$. Given a move x_i of C, let P respond with $u_i \in P_2$ such that $u_i \le x_i < 2u_i$, which exists by (P_2-IP). Then $u_i u_j < u_h < 2u_i u_j$ is impossible by (P_2-Univ). □

Definition 4.5 For any $t \leq n < \omega$, let $\mathrm{PWin}^t_n(u_0, \dots, u_{t-1})$ denote the formula

$$\forall x_t\, \exists u_t \dots \forall x_{n-1}\, \exists u_{n-1} \Big(\bigwedge_{t \leq i < n} (x_i > 0 \to u_i \leq x_i < 2u_i) \wedge \bigwedge_{h,i,j<n} \neg(u_i u_j < u_h < 2u_i u_j) \Big),$$

expressing that Powerator has a winning strategy in $\mathrm{PowG}^t_n(\mathfrak{M}, \vec{u})$.

TEIP is the $\mathcal{L}_{\mathrm{OR}}$-theory axiomatized by $\mathsf{IOpen} + \{\mathrm{PWin}^0_n : n \in \omega\}$.

The basic properties below follow immediately from the definition:

Lemma 4.6 *If $t < n$, then $\mathrm{PWin}^t_n(\vec{u})$ is equivalent to*

$$\forall x_t > 0\, \exists u_t\, \big(u_t \leq x_t < 2u_t \wedge \mathrm{PWin}^{t+1}_n(\vec{u}, u_t)\big).$$

If $t \leq m < n$, then $\mathrm{PWin}^t_n(\vec{u})$ implies $\mathrm{PWin}^t_m(\vec{u})$. □

Theorem 4.7 *The first-order theory of EIP of RCEF in $\mathcal{L}_{\mathrm{OR}}$, with or without GA, is TEIP.*

Proof: In view of Theorems 3.8 and 3.9, it suffices to show that TEIP_{P_2} is a conservative extension of TEIP. Clearly, $\mathfrak{M} \vDash \mathsf{IOpen}$ is a model of TEIP iff Powerator has a winning strategy in $\mathrm{PowG}_n(\mathfrak{M})$ for all $n \in \omega$; in particular, $\mathsf{TEIP}_{P_2} \vdash \mathsf{TEIP}$ follows from Lemma 4.4.

On the other hand, let $\mathfrak{M}$ be a countable recursively saturated model of TEIP; we will expand $\mathfrak{M}$ to a model of TEIP_{P_2}. The basic idea is that due to recursive saturation, P also has a winning strategy in $\mathrm{PowG}_\omega(\mathfrak{M})$, and then if we let C enumerate $M_{>0}$, the responses of P form a set P_2 such that $\langle \mathfrak{M}, P_2 \rangle \vDash \mathsf{TEIP}''_{P_2}$.

Formally, let $\Gamma^t(u_0, \dots, u_{t-1}) = \{\mathrm{PWin}^t_n(\vec{u}) : t \leq n < \omega\}$ for $t < \omega$, and fix an enumeration $\langle a_i : i < \omega \rangle$ of $M_{>0}$. We will construct a sequence $\langle b_i : i < \omega \rangle \subseteq M_{>0}$ such that $b_i \leq a_i < 2b_i$ and $\mathfrak{M} \vDash \Gamma^t(\vec{b})$ by induction on t.

We have $\mathfrak{M} \vDash \Gamma^0$ as $\Gamma^0 \subseteq \mathsf{TEIP}$. Assuming $\mathfrak{M} \vDash \Gamma^t(b_0, \dots, b_{t-1})$, we can take for b_t any realizer of the type $\Gamma^{t+1}(\vec{b}, u_t) \cup \{u_t \leq a_t < 2u_t\}$, hence using recursive saturation, we only need to check its finite satisfiability. In view of Lemma 4.6, it suffices to observe that for any $n > t$, $\mathfrak{M} \vDash \exists u_t\, \big(u_t \leq a_t < 2u_t \wedge \mathrm{PWin}^{t+1}_n(\vec{b}, u_t)\big)$ follows from $\mathfrak{M} \vDash \mathrm{PWin}^t_n(\vec{b})$.

When the construction of $\langle b_i : i < \omega \rangle$ is finished, let $P_2 = \{b_i : i < \omega\}$. Then the properties of $\vec{a}$ and $\vec{b}$ ensure $\langle \mathfrak{M}, P_2 \rangle \vDash \mathsf{TEIP}''_{P_2}$. □

Coupled with Lemma 4.4, the proof gives a characterization of $\mathcal{L}_{\mathrm{OR}}$-reducts of countable models of TEIP_{P_2}:

Corollary 4.8 *A countable model $\mathfrak{M} \vDash \mathsf{IOpen}$ expands to a model of TEIP_{P_2} iff Powerator has a winning strategy in $\mathrm{PowG}_\omega(\mathfrak{M})$.* □

Using our axiomatization of TEIP, it is now easy to answer negatively Question 7.3 from [7].

Example 4.9 The following consequence of TEIP is not provable in IOpen:

$$\forall x\, \exists u \geq x\, \forall y\, \big(0 < y < x \to \exists v\, (v \leq y < 2v \wedge v \mid u)\big). \tag{14}$$

(We can make it Π_1 by further bounding $u < 2x$.) Thus, some models of IOpen have no elementary extension to an EIP of a RCEF.

Proof: First, (14) indeed follows from TEIP (specifically, PWin_3^0) in view of Observation 4.2.

On the other hand, Smith [14] constructed a nonstandard $\mathfrak{M} \vDash \mathsf{IOpen}$ which is a UFD (or even PID): i.e., every $x \in M_{>0}$ can be written as a product of a sequence $\langle p_i : i < k \rangle$ of primes $p_i \in M_{>0}$ of standard length $k \in \mathbb{N}$. It follows that $x^* = \prod_{i:p_i \in \mathbb{N}} p_i$ is the largest standard divisor of x.

Assume for contradiction that (14) holds in $\mathfrak{M}$. Let $x \in M$ be nonstandard, and $u \in M$ satisfy the conclusion of (14). Take $y = 2u^*$ (which is standard, thus $y < x$), and let $v \in M$ be such that $v \le y < 2v$ and $v \mid u$. Then v is a standard divisor of u, but $v > u^*$, a contradiction. $\square$

We mention that $\mathsf{IOpen} \vdash \mathrm{PWin}_2^0$, hence the use of PWin_3^0 in Example 4.9 is the best possible.

5 Analysis of PowG

Unlike TEIP_{2^x} and TEIP_{P_2}, we defined TEIP by an infinite axiom schema, but it is not clear whether this is necessary:

Question 5.1 *Is* TEIP *finitely axiomatizable over* IOpen*?*

We do not know how to resolve this question, but we can at least give a partial answer. Let us observe that if there were only finitely many inequivalent formulas among $\{\mathrm{PWin}_n^1 : n \in \omega\}$, then TEIP would be finitely axiomatizable over IOpen by Lemma 4.6. We will show that this is not the case, though: the formulas $\{\mathrm{PWin}_n^1 : n \in \omega\}$ are strictly increasing in strength, even over $\mathrm{Th}(\mathbb{N})$. This is equivalent to $\{c(u) : u \in \mathbb{N}_{>0} \smallsetminus P_2^{\mathbb{N}}\} = \mathbb{N}_{>0}$, using the notation below:

Definition 5.2 If $\mathfrak{M} \vDash \mathsf{IOpen}$ and $\vec{u} \in M_{>0}^t$, the PowG-*complexity* of $\vec{u}$, denoted $c(\mathfrak{M}, \vec{u})$, is the least $n \in \omega$ such that C has a winning strategy in $\mathrm{PowG}_{t+n}^t(\mathfrak{M}, \vec{u})$; if such an n does not exist, we put $c(\mathfrak{M}, \vec{u}) = \infty$. If $\mathfrak{M} = \mathbb{N}$, we write just $c(\vec{u})$. (Observe that $c(u) \ge n$ iff $\mathbb{N} \vDash \mathrm{PWin}_n^1(u)$.) Let $P_2^{\mathbb{N}}$ denote the set of powers of 2 in $\mathbb{N}$.

Lemma 5.3 *For any* $\vec{u} \in \mathbb{N}_{>0}^t$*,* $c(\vec{u})$ *is finite iff some* u_i *is not a power of* 2*.*

Proof: The left-to-right implication follows from Lemma 4.4. On the other hand, if $c(\vec{u}) = \infty$, i.e., P has a winning strategy in $\mathrm{PowG}_n^t(\vec{u})$ for all $n \ge t$, and $\mathfrak{M}$ is a countable recursively saturated model of $\mathrm{Th}(\mathbb{N})$, then $\mathfrak{M}$ expands to a model $\langle \mathfrak{M}, P_2 \rangle \vDash \mathsf{TEIP}_{P_2}$ such that $\vec{u} \subseteq P_2$ by the proof of Theorem 4.7. Taking one more elementary extension if necessary, it expands to a model $\langle \mathfrak{M}, 2^x \rangle \vDash \mathsf{TEIP}_{2^x}$ such that $\vec{u} \subseteq \mathrm{im}(2^x)$. But TEIP_{2^x} implies that 2^x extends the standard function and maps nonstandard values to nonstandard values, hence $\vec{u} \subseteq P_2^{\mathbb{N}}$.

(The reader is invited to construct a simple explicit winning strategy for C if some u_i is not a power of 2. We will present an optimized one below in Theorem 5.8.) $\square$

For the application to finite non-axiomatizability of $\{\mathrm{PWin}_n^1(u) : n \ge 1\}$, it would be clearly enough to show that $\{c(u) : u \in \mathbb{N}_{>0} \smallsetminus P_2^{\mathbb{N}}\}$ is unbounded. Let us observe that this is, in fact, equivalent to $\{c(u) : u \in \mathbb{N}_{>0} \smallsetminus P_2^{\mathbb{N}}\} = \mathbb{N}_{>0}$:

Lemma 5.4 $\{c(u) : u \in \mathbb{N}_{>0} \smallsetminus P_2^{\mathbb{N}}\}$ *is an initial segment of* $\mathbb{N}_{>0}$.

Proof: There are u such that $c(u) = 1$, see Example 5.11. Let $n > 1$, and assume that there exists $u \notin P_2^{\mathbb{N}}$ such that $c(u) \geq n$. Let u be the smallest such number; we will give a strategy for C showing $c(u) = n$. First, C plays $u - 1$, thus P responds with a v such that $u/2 \leq v < u$. If $u/2 < v$, then $v \nmid u$, thus C can win in the second round by Observation 4.2; otherwise, $v = u/2 \notin P_2^{\mathbb{N}}$, thus $c(u/2) < n$ by the minimality of u, and C can just follow the optimal strategy for $u/2$. □

While our goal is to prove lower bounds on $c(u)$, we will start with upper bounds to get an idea of what is in the realm of possible: it turns out that C can very efficiently exploit irregularities in exponents of the prime factorization of u, hence our lower bounds will need to be somewhat delicate. The main tool of Challenger is the following divide-and-conquer strategy.

Lemma 5.5 *Let* $n > 1$ *and* $u, v, \vec{u} \in \mathbb{N}_{>0}$.

(*i*) *If* $u^n < v < 2u^n$, *then* $c(u, v) \leq \lceil \log \lfloor \log n \rfloor \rceil + 1$.

(*ii*) $c(\vec{u}, u) \leq \max\{c(\vec{u}, u, u^n) + 1, \lceil \log \lfloor \log n \rfloor \rceil + 2\}$.

Proof: (i): Let $k = \lfloor \log n \rfloor$, and put $i_0 = 0$, $j_0 = k$, $v_0 = v$ so that $u^{\lfloor n/2^{i_0} \rfloor} < v_0 < 2u^{\lfloor n/2^{i_0} \rfloor}$ and $u^{\lfloor n/2^{j_0} \rfloor} = u$. Using Observation 4.2, let C play $2u^{\lfloor n/2^{m_1} \rfloor} - 1$ for $m_1 = \lfloor k/2 \rfloor = \lfloor (i_0 + j_0)/2 \rfloor$ so that P responds with a w_1 such that $u^{\lfloor n/2^{m_1} \rfloor} \leq w_1 < 2u^{\lfloor n/2^{m_1} \rfloor}$. If $w_1 = u^{\lfloor n/2^{m_1} \rfloor}$, put $i_1 = i_0$, $j_1 = m_1$, and $v_1 = v_0$; otherwise, $i_1 = m_1$, $j_1 = j_0$, and $v_1 = w_1$. Either way, the responses of P include $u^{\lfloor n/2^{j_1} \rfloor}$ and v_1 satisfying $u^{\lfloor n/2^{i_1} \rfloor} < v_1 < 2u^{\lfloor n/2^{i_1} \rfloor}$, where $i_1 < j_1$ and $j_1 - i_1 \leq \lceil k/2 \rceil$. We continue a binary search in the same way: after $\lceil \log k \rceil$ rounds, the responses of P will include $u' = u^{\lfloor n/2^{i+1} \rfloor}$ and v' such that $u^{\lfloor n/2^i \rfloor} < v' < 2u^{\lfloor n/2^i \rfloor}$ for some $i < k$. If $\lfloor n/2^i \rfloor = 2\lfloor n/2^{i+1} \rfloor$, we have $u'^2 < v' < 2u'^2$, hence P loses. Otherwise $\lfloor n/2^i \rfloor = 2\lfloor n/2^{i+1} \rfloor + 1$; in a final round, C plays u'^2, and P responds with $u'^2 \leq u'' < 2u'^2$. Then $u'^2 < u'' < 2u'^2$ or $u'u'' < v' < 2u'u''$, thus P loses either way.

(ii): In the first round, C makes P respond with a v such that $u^n \leq v < 2u^n$. If $v = u^n$, C continues with the strategy for $\mathrm{PowG}(\vec{u}, u, u^n)$, otherwise with the strategy from (i). □

Remark 5.6 Extending Observation 4.2, Lemma 5.5 (ii) implies the following for $n \geq 2$: if $v \leq u^n$ and $v \nmid u^n$, then $c(u, v) \leq \lceil \log \lfloor \log n \rfloor \rceil + 2$.

Definition 5.7 For any prime p and $n \in \mathbb{N}_{>0}$, $\nu_p(n)$ denotes the p-adic valuation of n: the maximal k such that $p^k \mid n$. (If it comes up, $\nu_p(0)$ is understood as $+\infty$.)

Observe that any $n \in \mathbb{N}_{>0} \smallsetminus P_2^{\mathbb{N}}$ can be written uniquely as $n = 2^{\nu_2(n)} v^r$, where v (which is necessarily odd) is not a perfect power (which implies $v > 1$), and $r > 0$. We have $r = \gcd\{\nu_p(n) : p \text{ odd prime}\}$.

Theorem 5.8 *Let* $u = 2^{\nu_2(u)} v^r$, *where* v *is not a perfect power, and let* $d \nmid r$. *Then*

$$c(u) \leq \lceil \log \lfloor \log d \rfloor \rceil + 4. \tag{15}$$

Proof: In the first round, C can play $\lfloor u^{1/d} \rfloor$ so that P responds with a w such that $w \le u^{1/d} < 2w$, hence $2^i w^d < u < 2^{i+1} w^d$ for some $i < d$: $2^i w^d = u$ is impossible as the odd part of u is not a dth power. It remains to show that for any such w, $c(u, w) \le \lceil \log \lfloor \log d \rfloor \rceil + 3$.

Since $c(u, w^d, 2^i) = 0$, we have $c(u, w, 2^i) \le \lceil \log \lfloor \log d \rfloor \rceil + 2$ by Lemma 5.5 (ii). One more application of Lemma 5.5 gives $c(u, w, 2) \le \max\{\lceil \log \lfloor \log d \rfloor \rceil + 3, \lceil \log \lfloor \log i \rfloor \rceil + 2\} = \lceil \log \lfloor \log d \rfloor \rceil + 3$, thus $c(u, w) \le \lceil \log \lfloor \log d \rfloor \rceil + 4$ (if C plays 2, P has to respond with 2).

We can improve this to $c(u, w) \le \lceil \log \lfloor \log d \rfloor \rceil + 3$ by observing that 2 is needed only in one branch. Mimicking the proof of Lemma 5.5, let C play $2^{i+1} - 1$ so that P responds with a z such that $2^i \le z < 2^{i+1}$. If $z = 2^i$, C wins in $c(u, w, 2^i) \le \lceil \log \lfloor \log d \rfloor \rceil + 2$ more rounds for a total of $\lceil \log \lfloor \log d \rfloor \rceil + 3$. Otherwise, C makes P play 2 in the second round, and wins in $\lceil \log \lfloor \log i \rfloor \rceil + 1$ more rounds by Lemma 5.5 (i) for a total of $\lceil \log \lfloor \log i \rfloor \rceil + 3$. □

Remark 5.9 Ignoring the exact constants, Theorem 5.8 is equivalent to

$$c(u) \le \min\{\log \nu_q(\nu_p(u)) + \log \log q : p,\ q \text{ primes},\ p \text{ odd}\} + O(1).$$

Recall our convention that $\log x = 0$ for $x < 1$.

Theorem 5.10 *Let $u = 2^{\nu_2(u)} v^r$, where v is not a perfect power, and $r > 0$. Then*

$$c(u) \le \lceil \log \log \log \log u \rceil + 4, \tag{16}$$

$$c(u) \le \lceil \log \log \log r \rceil + 4, \tag{17}$$

$$c(u) \le \lceil \log \log \log \nu_2(u) \rceil + 5. \tag{18}$$

Proof: We start with (17). There exists a $d \le n$ such that $d \nmid r$ if $r < \operatorname{lcm}\{1, \dots, n\} = e^{\psi(n)}$, where $\psi(n) = \sum_{p^k \le n} \ln p$ is Chebyshev's function. By the prime number theorem, $\psi(n) \sim n$, hence we can find $d \nmid r$ such that $d \le (1 + o(1)) \ln r$, thus $d \le \log r$ if r is large enough. Then (15) implies (17).

To show that (17) holds for all rather than just sufficiently large r, we need to check small cases. First, if $d = 2, 3$, then $\lceil \log \lfloor \log d \rfloor \rceil = 0 \le \lceil \log \log \log r \rceil$, thus (17) holds unless $6 \mid r$, whence $r \ge 6 > 4$. Next, if $d \le 7$, then $\lceil \log \lfloor \log d \rfloor \rceil = 1 \le \lceil \log \log \log r \rceil$ (using $r > 4$), thus (17) holds unless $2^2 \times 3 \times 5 \times 7 = 420 \mid r$, whence $r \ge 420 > 2^8$. Finally, it follows from known explicit bounds on ψ that $\operatorname{lcm}\{1, \dots, n\} > 2^n$ for $n > 8$ (in fact, it holds for $n \ge 7$): Nagura [10] proved $\psi(n) > 0.916n - 2.318$ for all $n > 0$, which implies $\psi(n) > n \ln 2$ for $n \ge 11$, and one can check the cases $n = 9, 10$ by hand. Thus, if $r > 2^8$, there is a $d \nmid r$ such that $d \le \lceil \log r \rceil$, whence $\lceil \log \lfloor \log d \rfloor \rceil \le \lceil \log \log \lceil \log r \rceil \rceil = \lceil \log \log \log r \rceil$.

Since $r \le \log_3 u \le \log u$, (17) implies (16).

For (18), let C play $2^{\nu_2(u)+1} < u$ in the first round so that P responds with a u' such that $2^{\nu_2(u)} < u' \le 2^{\nu_2(u)+1}$. If $u' = 2^{\nu_2(u)+1} \nmid u$, then C can win in the next round by Observation 4.2. Otherwise, C can win in $\lceil \log \log \log \log_3 u' \rceil + 4 \le \lceil \log \log \log \nu_2(u) \rceil + 4$ further rounds by (the proof of) (16). □

Example 5.11 $c(u) = 1$ iff $u = 5, 6, 7, 17$.

Proof: If $u = 5, 6, 7$, C wins by playing 2, forcing P to respond with 2, as $2^2 < u < 2 \cdot 2^2$. If $u = 17$, C plays 4, and P responds with $v = 3, 4$; then $v^2 < u < 2v^2$. Conversely, if $c(u) = 1$, let $2x$ be the winning move of C (assumed even by Remark 4.3); then $v^2 < u < 2v^2$ or $u^2 < v < 2u^2$ for all $v \in (x, 2x]$, i.e., $[x+1, 2x] \subseteq \left[\lfloor\sqrt{u/2}\rfloor + 1, \lceil\sqrt{u}\rceil - 1\right] \cup [u^2+1, 2u^2-1]$. There is a gap between the last two intervals as $\lceil\sqrt{u}\rceil - 1 < u < u^2+1$, thus $[x+1, 2x] \subseteq \left[\lfloor\sqrt{u/2}\rfloor + 1, \lceil\sqrt{u}\rceil - 1\right]$ or $[x+1, 2x] \subseteq [u^2+1, 2u^2-1]$. The latter makes $u^2 \le x$ and $2x < 2u^2$, which is impossible. The former amounts to $\sqrt{u/2} - 1 < x < \frac{1}{2}\sqrt{u}$; in particular, $\sqrt{2u} - 2 < \sqrt{u}$, thus $\sqrt{u} < 2/(\sqrt{2}-1) = 2(\sqrt{2}+1)$ and $x < \sqrt{2}+1$, i.e., $x = 1$ (in which case $4 < u < 8$) or $x = 2$ (in which case $16 < u < 18$). □

Example 5.12 We have $c(u) \le 2$ whenever u satisfies one of the following conditions:

(i) $u > 8$ and $16 \nmid u$.

(ii) The odd part of u is not a square.

(iii) $u < 2304$ is not a power of 2. (With some effort, one can check that $c(2304) = 3$.)

(iv) $u = \prod_{i<k} p_i^{e_i}$ for primes $p_0 < \cdots < p_{k-1}$, and there is $i < k$ such that $p_i > 2\prod_{j<i} p_j^{e_j}$.

Proof: Observe that C can force P to play 1, 2 (by playing the same), and in the first round, also 4 (by playing 6: if P responds with $5, 6$, C wins in the second round by Example 5.11) and 8 (by playing 8; if P responds with $5, 6, 7$, we use Example 5.11 again).

(i): C makes P play 8 in the first round, and then plays $\lceil u/8\rceil - 1$, thus P responds with v such that $u/16 < v < u/8$ ($v = u/16$ is impossible by assumption); C wins as $8v < u < 2 \cdot 8v$.

(ii): C plays $\lfloor\sqrt{u}\rfloor$, thus P responds with v such that $\frac{1}{2}\sqrt{u} < v \le \sqrt{u}$; since $u \ne v^2, 2v^2$, we have $v^2 < u < 2v^2$ (and C wins) or $2v^2 < u < 4v^2$. In the latter case, C plays $\lceil u/v\rceil - 1$, thus P responds with w such that $w < u/v \le 2w$. Then C wins as either $vw < u < 2vw$, or $w = u/(2v)$ and $w^2 < u < 2w^2$.

(iii): For $u = 3$, C forces P to play 1 and 2. For $4 < u < 8$, C makes P play 2 as in Example 5.11. For $8 < u < 64$, we can use (i), unless $u = 48$, in which case we use (ii). For $64 < u < 128$, C makes P play 8 and wins as $8^2 < u < 2 \cdot 8^2$. For $128 < u < 256$, C makes P play 4, and then plays 32 so that P responds with $16 < v \le 32$: either $4^2 < v < 2 \cdot 4^2$, or $v = 32$ and $4 \cdot 32 < u < 2 \cdot 4 \cdot 32$, thus C wins. For $256 < u < 512$, C makes P play 4, and then plays 31, thus P plays $16 \le v < 32$. Either $4^2 < v < 2 \cdot 4^2$, or $v = 16$ and $16^2 < u < 2 \cdot 16^2$. For $512 < u < 1024$, C makes P play 8, and then plays 127 so that either $8^2 < v < 2 \cdot 8^2$ or $8 \cdot 64 < u < 2 \cdot 8 \cdot 64$. For $1024 < u < 2048$, C makes P play 4, and then plays 32 so that either $4^2 < v < 2 \cdot 4^2$ or $32^2 < u < 2 \cdot 32^2$. (One can also do $4096 < u < 8192$ and $16384 < u < 32768$ using similar arguments.) For $2048 < u < 2304 = 16 \cdot 144$, one of (i) or (ii) is applicable.

For $u = 2304 = 48^2$, P can survive two rounds by playing in the first one an element of $\{u^n 2^l : n \in \mathbb{N}, |l| \le 4\} \cup \{u^{n+1/2} 2^l : n \in \mathbb{N}, |l| \le 1\}$, but it is a bit tedious to check all cases.

(iv): The assumption implies (and, actually, is equivalent to) that for some $x < u$, namely $x = \prod_{j<i} p_j^{e_j}$, there is no divisor $v \mid u$ such that $x < v \le 2x$. Thus, C can play $2x$, and win in the second round by Observation 4.2 (i). □

The significance of point (iv) of Example 5.12 is that the upper bounds from Theorems 5.8 and 5.10 cannot be asymptotically optimal: there are u for which these bounds are arbitrarily large, yet $c(u) = 2$ (e.g., take $u = (2p)^{n!}$ for a large n, where $p > 2^{n!+1}$ is a prime). Nevertheless, we will show that the bounds are tight up to an additive constant under suitable conditions precluding (iv) and similar cases (viz., in the decomposition $u = 2^{\nu_2(u)} v^r$, v is sufficiently smaller than $2^{\nu_2(u)}$).

We now come to the main technical part of our lower bound on $c(u)$. Recall that the 1-norm of a vector $\vec{x} \in \mathbb{R}^t$ is $\|\vec{x}\|_1 = \sum_{i<t} |x_i|$.

Lemma 5.13 *Let $v \in \mathbb{N}_{>0}$, and define the sequences $\langle D_k, N_k, B_k : k \in \mathbb{N}_{>0}\rangle$ by $D_1 = 1$, $N_1 = 3$, $B_1 = 0$, $D_{k+1} = D_k \operatorname{lcm}\{1, \dots, N_k\}$, $N_{k+1} = N_k^2$, and $B_{k+1} = 2N_k B_k + N_k^2 \lceil D_k \log v\rceil$. Then the following holds for all $k \geq 1$ and all $\vec{u} \in \mathbb{N}^t_{>0}$ of the form $u_i = 2^{l_i} v^{r_i}$, $l_i, r_i \in \mathbb{N}$, for each $i < t$:*

If

$$D_k \mid r_i \tag{19}$$

for each $i < t$, and

$$\|\vec{n}\|_1 \leq N_k \ \& \ \sum_{i<t} n_i r_i > 0 \implies \sum_{i<t} n_i l_i \geq B_k \tag{20}$$

for all $\vec{n} \in \mathbb{Z}^t$, then $c(\vec{u}) \geq k$.

Proof: We prove the statement by induction on k. We may assume v is not a power of 2 (whence $v \geq 3$), as otherwise $c(\vec{u}) = \infty$ trivially satisfies the conclusion.

For $k = 1$, we have to show that there are no $h, i, j < t$ such that $u_i u_j < u_h < 2u_i u_j$. Fixing h, i, j, put $\vec{n} = e^h - e^i - e^j$, where e^g denotes the gth standard unit vector (i.e., if h, i, j are distinct, then $n_h = 1$ and $n_i = n_j = -1$). Clearly, $\|\vec{n}\|_1 \leq 3 = N_1$, thus we may apply (20): if $r_h - r_i - r_j > 0$, then $l_h - l_i - l_j \geq 0 = B_1$, hence $u_h/(u_i u_j) = 2^{l_h - l_i - l_j} v^{r_h - r_i - r_j} \geq v > 2$. Likewise, if $r_h - r_i - r_j < 0$, we may apply (20) to $-\vec{n}$, and obtain $u_h/(u_i u_j) \leq v^{-1} < 1$. Finally, if $r_h - r_i - r_j = 0$, then $u_h/(u_i u_j)$ is a power of 2, hence it cannot be strictly between 1 and 2.

Assume the statement holds for k, and that $\vec{u}$, $\vec{l}$, and $\vec{r}$ satisfy (19) and (20) for $k+1$ in place of k. Using the induction hypothesis, it suffices to show that for every $x \geq 1$, there exists $u_t = 2^{l_t} v^{r_t}$ such that $u_t \leq x < 2u_t$, and $\langle \vec{u}, u_t\rangle \in \mathbb{N}^{t+1}_{>0}$ satisfies (19) and (20) for k. We will write $r = r_t$ and $l = l_t$ for short. Observe that $u_t \leq x < 2u_t$ amounts to $l = \lfloor \log x - r \log v \rfloor$, thus we can only vary r; we will check that (19) and (20) translate to conditions on $r \in \mathbb{Z}$ that are satisfiable together, using our assumptions on $\vec{u}$. (We also need to ensure $r, l \geq 0$, but this easily follows from (20), hence we need not worry about it.)

Condition (19) clearly holds for $i < t$ as $D_k \mid D_{k+1}$, thus we only need to make sure r is a multiple of D_k. Condition (20) also holds automatically when $n_t = 0$, as $N_k \leq N_{k+1}$ and $B_k \leq B_{k+1}$. The other cases give upper or lower bounds on r, depending on the sign of n_t. For $n_t > 0$ (renamed to n, and the rest of $\vec{n}$ negated), (20) amounts to

$$\|\vec{n}\|_1 + n \leq N_k \ \& \ r > \sum_{i<t} \frac{n_i r_i}{n} \implies l \geq \frac{B_k}{n} + \sum_{i<t} \frac{n_i l_i}{n}$$

for all $\vec{n} \in \mathbb{Z}^t$ and $n \in \mathbb{N}_{>0}$, i.e.,

$$\|\vec{n}\|_1 + n \le N_k \implies r \le \sum_{i<t} \frac{n_i r_i}{n} \quad \text{or} \quad \log x - r \log v \ge \left\lceil \frac{B_k}{n} + \sum_{i<t} \frac{n_i l_i}{n} \right\rceil .$$

The largest integer multiple $r = D_k r'$ that satisfies this condition is characterized by

$$r' \le U_{\vec{n},n} := \max \left\{ \sum_{i<t} \frac{n_i r_i}{D_k n}, \left\lfloor \frac{1}{D_k \log v} \left(\log x - \left\lceil \frac{B_k}{n} + \sum_{i<t} \frac{n_i l_i}{n} \right\rceil \right) \right\rfloor \right\}$$

for all $\vec{n} \in \mathbb{Z}^t$ and $n \in \mathbb{N}_{>0}$ such that $\|\vec{n}\|_1 + n \le N_k$, using the fact that for $1 \le n \le N_k$, $D_k n \mid D_{k+1} \mid r_i$.

Likewise, the cases of (20) with $n_t < 0$ (renamed to $-m$, and the rest of $\vec{n}$ to $\vec{m}$) amount to

$$\|\vec{m}\|_1 + m \le N_k \implies r \ge \sum_{i<t} \frac{m_i r_i}{m} \quad \text{or} \quad \log x - r \log v < \left\lfloor -\frac{B_k}{m} + \sum_{i<t} \frac{m_i l_i}{m} \right\rfloor + 1$$

for all $\vec{m} \in \mathbb{Z}^t$ and $m \in \mathbb{N}_{>0}$, and the least multiple of D_k with this property is characterized by

$$r' \ge L_{\vec{m},m} := \min \left\{ \sum_{i<t} \frac{m_i r_i}{D_k m}, \left\lfloor \frac{1}{D_k \log v} \left(\log x + \left\lceil \frac{B_k}{m} - \sum_{i<t} \frac{m_i l_i}{m} \right\rceil - 1 \right) \right\rfloor + 1 \right\}$$

for all $\vec{m} \in \mathbb{Z}^t$ and $m \in \mathbb{N}_{>0}$ such that $\|\vec{m}\|_1 + m \le N_k$. Thus, an r that satisfies all the necessary conditions exists iff for every $\vec{n}, \vec{m} \in \mathbb{Z}^t$ and $n, m \in \mathbb{N}_{>0}$,

$$\text{(21)} \qquad \|\vec{n}\|_1 + n \le N_k \ \&\ \|\vec{m}\|_1 + m \le N_k \implies L_{\vec{m},m} \le U_{\vec{n},n}.$$

This clearly holds if $\frac{1}{m} \sum_i m_i r_i \le \frac{1}{n} \sum_i n_i r_i$, hence we may assume $\frac{1}{m} \sum_i m_i r_i > \frac{1}{n} \sum_i n_i r_i$. Then the assumption (20) for $\vec{u}$, applied to $n\vec{m} - m\vec{n}$, implies

$$\sum_{i<t} \frac{m_i l_i}{m} - \sum_{i<t} \frac{n_i l_i}{n} \ge \frac{B_{k+1}}{nm} \ge \frac{B_k}{m} + \frac{B_k}{n} + \lceil D_k \log v \rceil,$$

using the bounds

$$\|n\vec{m} - m\vec{n}\|_1 \le n\|\vec{m}\|_1 + m\|\vec{n}\|_1 \le \big(n + \|\vec{n}\|_1\big)\big(m + \|\vec{m}\|_1\big) \le N_k^2 = N_{k+1}$$

and

$$B_{k+1} = 2N_k B_k + N_k^2 \lceil D_k \log v \rceil \ge (n+m) B_k + nm \lceil D_k \log v \rceil.$$

It follows that

$$\left\lceil \frac{B_k}{n} + \sum_{i<t} \frac{n_i l_i}{n} + \frac{B_k}{m} - \sum_{i<t} \frac{m_i l_i}{m} \right\rceil \le -\lceil D_k \log v \rceil \le -D_k \log v,$$

thus

$$\left\lceil \frac{B_k}{n} + \sum_{i<t} \frac{n_i l_i}{n} \right\rceil + \left\lceil \frac{B_k}{m} - \sum_{i<t} \frac{m_i l_i}{m} \right\rceil \le 1 - D_k \log v$$

and

$$\left(\log x + \left\lceil \frac{B_k}{m} - \sum_{i<t} \frac{m_i l_i}{m} \right\rceil - 1 \right) + D_k \log v \le \log x - \left\lceil \frac{B_k}{n} + \sum_{i<t} \frac{n_i l_i}{n} \right\rceil .$$

This yields (21). $\square$

Theorem 5.14 *Let $u = 2^l v^r$, where $v > 1$, $r > 0$, and $l/\log v \geq 10^8$. Then*

$$c(u) \geq \min\big\{\lfloor \log\lceil \log_3 d\rceil\rfloor + 1 : d \nmid r\big\} \cup \big\{\lfloor \log\log_3\log_4(l/\log v)\rfloor + 3\big\}. \tag{22}$$

We may use the simpler bounds $\lceil \log\log_3 d\rceil$ or $\lfloor \log\lceil \log d\rceil\rfloor$ in place of $\lfloor \log\lceil \log_3 d\rceil\rfloor + 1$.

Proof: Applying Lemma 5.13 with $t = 1$, we see that $c(u) \geq k$ whenever $D_k \mid r$ and $l \geq B_k$; it remains to estimate these quantities. Expanding the recurrences, we have

$$N_k = 3^{2^{k-1}}, \qquad D_k = \prod_{i=0}^{k-2} L(3^{2^i}), \qquad \text{where } L(n) = \operatorname{lcm}\{1, \ldots, n\}.$$

Observe that $L(n)L(m) \mid L(nm)$: whenever $1 \leq a \leq n$ and $1 \leq b \leq m$, we have $ab \mid L(nm)$. Thus,

$$D_k \;\Big|\; L\Big(\prod_{i=0}^{k-2} 3^{2^i}\Big) = L\big(3^{2^{k-1}-1}\big),$$

and a sufficient condition for $D_k \mid r$ is that $d > 3^{2^{k-1}-1}$ for all $d \nmid r$. Since

$$d > 3^{2^{k-1}-1} \iff \lceil \log_3 d\rceil \geq 2^{k-1} \iff \log\lceil \log_3 d\rceil + 1 \geq k,$$

we see that $D_k \mid r$ holds for any k such that

$$k \leq \min\{\lfloor \log\lceil \log_3 d\rceil\rfloor + 1 : d \nmid r\}.$$

We also observe that $\lfloor \log\lceil \log_3 d\rceil\rfloor + 1 \geq \lceil \log\lceil \log_3 d\rceil\rceil = \lceil \log\log_3 d\rceil$ and $\lfloor \log\lceil \log_3 d\rceil\rfloor + 1 = \lfloor \log(2\lceil \log_3 d\rceil)\rfloor \geq \lfloor \log\lceil \log d\rceil\rfloor$, as $\log d \leq 2\log_3 d$ implies $\lceil \log d\rceil \leq 2\lceil \log_3 d\rceil$.

The recurrence for B_k resolves to

$$B_k = N_k \sum_{i=1}^{k-1} 2^{k-1-i}\lceil D_i \log v\rceil \leq 3^{2^{k-1}} \sum_{i=1}^{k-1} 2^{k-1-i}(D_i + 1)\log v =: B'_k \log v.$$

Recalling Chebyshev's function from the proof of Theorem 5.10, we have $\ln L\big(3^{2^j}\big) = \psi\big(3^{2^j}\big) \sim 3^{2^j}$, whence $\ln D_i = \sum_{j\leq i-2} \psi\big(3^{2^j}\big) \sim 3^{2^{i-2}}$. It follows that the above sum for B'_k is dominated by the $i = k-1$ term, and $\ln B'_k \sim 3^{2^{k-3}}$; thus, for all sufficiently large k, $\log_4 B'_k < 3^{2^{k-3}}$ and $k > 3 + \log\log_3\log_4 B'_k$. That is, $l \geq B_k$ if $k \leq \lfloor \log\log_3\log_4(l/\log v)\rfloor + 3$, provided the latter is large enough.

For an explicit bound, we claim that $\log\log_3\log_4 B'_k < k - 3$ for all $k \geq 5$, thus (22) holds whenever $l/\log v \geq B'_4 = 99{,}353{,}223$. For $k = 5$, direct computation gives $B'_5 \approx 6.333 \times 10^{46}$ and $\log\log_3\log_4 B'_5 < 1.9865$ (this can be verified e.g. in Sage, along with the value of B'_4 given above). Assume $k \geq 6$. Nagura [10] proved $\psi(n) < 1.086n$ for all $n > 0$, thus

$$\log_4 D_{k-1} < 1.086 \log_4 e \sum_{i\leq k-3} 3^{2^i} < 0.7834\, \alpha_{k-3}\, 3^{2^{k-3}},$$

where $\alpha_j = \sum_{i\leq j} 3^{2^i - 2^j}$. For $j \geq 1$, $3^{2^j}(\alpha_j - 1) = \sum_{i<j} 3^{2^i} \geq 3 > \alpha_j$, thus $\alpha_{j+1} = 1 + 3^{-2^j}\alpha_j < \alpha_j$, i.e., α_j is decreasing. Since $\alpha_3 = 1 + 3^{-4} + 3^{-6} + 3^{-7} = 2218/2187 < 1.0142$, we get

$$\log_4 D_{k-1} < 0.7834\, \alpha_3\, 3^{2^{k-3}} < 0.795 \times 3^{2^{k-3}}$$

and

$$\log_4(N_k D_{k-1}) < 0.795 \times 3^{2^{k-3}} + 2^{k-1}\log_4 3 \le \left(0.795 + \frac{2^5}{3^{2^3}}\log_4 3\right) 3^{2^{k-3}} < 0.799 \times 3^{2^{k-3}}.$$

Since $D_{i+1}/D_i = L\bigl(3^{2^{i-1}}\bigr) \ge 6$, we have

$$\begin{aligned}\frac{B'_k}{N_k D_{k-1}} - 1 &= \frac{2^{k-1}-1}{D_{k-1}} + \sum_{i=1}^{k-2} 2^{k-1-i}\frac{D_i}{D_{k-1}} < \frac{2^{k-1}-1}{D_{k-1}} + 3\frac{D_{k-2}}{D_{k-1}} \\ &\le \frac{31}{D_5} + \frac{3}{L\bigl(3^{2^3}\bigr)} < 4 \times 10^{-2846},\end{aligned}$$

thus $\log_4(B'_k/(N_k D_{k-1})) < 4 \times 10^{-2846}\log_4 e < 3 \times 10^{-2846}$, and $\log_4 B'_k < 0.8 \times 3^{2^{k-3}}$. □

Example 5.15 $k+1 \le c\bigl(6^{2^{2^k}}!\bigr) \le k+4$ for all $k \ge 0$.

Proof: We write $u = 6^{2^{2^k}!} = 2^l v^r$ where $v = 3$ and $l = r = 2^{2^k}!$. The least d not dividing r is the least prime larger than 2^{2^k}, thus $2^{2^k} < d < 2^{2^k+1}$ by Bertrand's postulate, and $c(u) \le k+4$ by Theorem 5.8. For a lower bound, we have $c(36) = 2$ and $c(6^4) \ge 2$ by Examples 5.11 and 5.12, thus we may assume $k \ge 2$. Since $n! > 4^n$ for $n \ge 9$, we have $4^{3^{2^{k-1}}}\log 3 < 4^{3^{2^{k-1}}+1} < 4^{4^{2^{k-1}}} = 4^{2^{2^k}} < 2^{2^k}!$ for $k \ge 2$, i.e., $\log\log_3\log_4(2^{2^k}!/\log 3) > k-1$, and $2^{2^k}/\log 3 > 10^8$. Thus, Theorem 5.14 gives $c(u) \ge \lfloor\log\lceil\log_3 d\rceil\rfloor + 1 \ge k$.

To improve this to $c(u) \ge k+1$, we may apply Lemma 5.13 directly. We know $l \ge B_{k+2}$ from the proof of Theorem 5.14, thus it suffices to show that $D_{k+1} \mid r$. Any prime $p \mid D_{k+1}$ is bounded by $3^{2^{k-1}}$; since $\nu_p(L(n)) = \lfloor\log_p n\rfloor$, we have

$$\nu_p(D_{k+1}) = \sum_{i=0}^{k-1}\Bigl\lfloor \log_p 3^{2^i}\Bigr\rfloor \le \left\lfloor \sum_{i=0}^{k-1} 2^i\frac{\log 3}{\log p}\right\rfloor \le \left\lfloor\frac{2^k}{\log_3 p}\right\rfloor,$$

while $\nu_p(r) = \sum_{i\ge 1}\lfloor 2^{2^k}/p^i\rfloor \ge \lfloor 2^{2^k}/p\rfloor$. It remains to observe that $2^{2^k}/p \ge 2^k/\log_3 p$ as $p/\log_3 p \le 3^{2^{k-1}}/2^{k-1} \le 2^{2^k}/2^k$. □

Theorem 5.16 *If T is any Σ_1-sound $\mathcal{L}_{\mathrm{OR}}$-theory, then the formulas $\{\mathrm{PWin}^1_k(u) : k \ge 1\}$ are pairwise inequivalent over T.*

Proof: Since T remains Σ_1-sound after adding any set of true Π_1 sentences, we may assume $T \supseteq \mathsf{I}\Delta_0$. In view of Lemma 4.6, it suffices to prove $T \nvdash \mathrm{PWin}^1_k(u) \to \mathrm{PWin}^1_{k+1}(u)$ for any $k \ge 1$. By Example 5.15 and Lemma 5.4, there exists $n \in \mathbb{N}$ such that $c(n) = k$, i.e., $\mathbb{N} \vDash \mathrm{PWin}^1_k(\overline{n}) \wedge \neg\mathrm{PWin}^1_{k+1}(\overline{n})$. We observe that the existential quantifiers in Definition 4.5 can be bounded with $u_i \le x_i$, thus $\neg\mathrm{PWin}^1_{k+1}$ is equivalent to a Σ-formula (i.e., a formula built using existential and bounded universal quantifiers from a Δ_0 formula). It follows that $\neg\mathrm{PWin}^1_{k+1}(\overline{n})$ is provable in $\mathsf{Q} \subseteq T$, and if we assume that T is Σ-sound, then $T \nvdash \neg\mathrm{PWin}^1_k(\overline{n})$.

If we only have the weaker assumption that T is Σ_1-sound, we need to be a bit more careful. If we fix $t, k \ge 1$ and $v > 1$, then D_k, N_k, and B_k are constants, and properties (19) and (20) can be written as a Δ_0 formula $\alpha^t_{v,k}(\vec{u})$: $\vec{r}$ and $\vec{l}$ are bounded by $\vec{u}$, and we can express the condition $u_i = 2^{l_i} v^{r_i}$ by a bounded formula as the graph of powering $x^y = z$ is Δ_0-definable [5, §V.3(c)]; also, there is only a constant number of choices for $\vec{n}$. Then the Π_1 sentences

$$\forall \vec{u}\,\bigl(\alpha^t_{v,1}(\vec{u}) \to \mathrm{PWin}^t_t(\vec{u})\bigr), \tag{23}$$

$$\forall \vec{u}, x\,\bigl(\alpha^t_{v,k+1}(\vec{u}) \land x > 0 \to \exists u_t \le x\,(x < 2u_t \land \alpha^{t+1}_{v,k}(\vec{u}, u_t))\bigr) \tag{24}$$

are true in $\mathbb{N}$ and imply $\alpha^t_{v,k}(\vec{u}) \to \mathrm{PWin}^t_{t+k-1}(\vec{u})$. Thus, if we fix k and $n = 6^{2^{2^{k-1}}}!$ from Example 5.15, there is a true Π_1 sentence that implies $\mathrm{PWin}^1_k(\overline{n})$, while $\mathsf{Q} \vdash \neg\mathrm{PWin}^1_{k+4}(\overline{n})$. Using the Σ_1-soundness of T, there is a model $\mathfrak{M} \vDash T + \mathrm{PWin}^1_k(\overline{n}) + \neg\mathrm{PWin}^1_{k+4}(\overline{n})$. By the argument in Lemma 5.4, there is $m \le n$ such that $\mathfrak{M} \vDash \mathrm{PWin}^1_k(\overline{m}) \land \neg\mathrm{PWin}^1_{k+1}(\overline{m})$. □

Remark 5.17 Without going into the details, we claim that the lower bound in Lemma 5.13 can be formalized for standard k, t, and v in the theories $\mathsf{I\Delta_0}$ and $\mathsf{\Delta^b_1}$-CR (or equivalently, $\mathsf{VTC^0}$); that is, these theories prove (23) and (24). It follows that Theorem 5.16 holds for all consistent extensions of $\mathsf{I\Delta_0}$ or $\mathsf{\Delta^b_1}$-CR, regardless of their Σ_1-soundness.

6 Oddless interpretation

We determined the $\mathcal{L}_{\mathrm{OR}}$-fragment of TEIP_{P_2} to be TEIP in Section 4. But for completeness, we mention that there is another natural approach of relating TEIP_{P_2} to $\mathcal{L}_{\mathrm{OR}}$-theories which places an upper bound on the strength of TEIP: it is common to define the set of powers of 2 in arithmetical theories by the formula

$$\mathrm{Pow}_2(u) \iff \forall x\,(x \mid u \to x = 1 \lor 2 \mid x),$$

expressing that u has no nontrivial odd divisors (hence we may call such elements "oddless"). Let π_2 denote the interpretation of $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ in $\mathcal{L}_{\mathrm{OR}}$ which is absolute on $\mathcal{L}_{\mathrm{OR}}$, and interprets P_2 by Pow_2. We are particularly interested in relating TEIP and friends to standard fragments of bounded arithmetic using π_2.

Recall that $x \mid y$ is an E_1 formula equivalent to an U_1 formula over IOpen, thus Pow_2 is equivalent to a U_1 formula (the quantifier over x in the definition can be clearly bounded by u).

Observation 6.1 IOpen *proves* $\mathrm{Pow}_2(u) \land v \mid u \to \mathrm{Pow}_2(v)$. □

Theorem 6.2 *The smallest theory that interprets* TEIP_{P_2} *via* π_2 *is the theory* $\mathsf{TEIP}_{\mathrm{Pow}_2}$*, extending* IOpen *by the axioms*

$$(\mathrm{Pow}_2\text{-IP}) \qquad \forall x > 0\,\exists u\,\bigl(\mathrm{Pow}_2(u) \land u \le x < 2u\bigr),$$

$$(\mathrm{Pow}_2\text{-Div}) \qquad \forall u, v\,\bigl(\mathrm{Pow}_2(u) \land \mathrm{Pow}_2(v) \land u \le v \to u \mid v\bigr).$$

It is included in $\mathsf{IE}_1 +$

$$(\mathrm{Pow}_2\text{-Cof}) \qquad \forall x\,\exists u > x\,\mathrm{Pow}_2(u),$$

in IE_2*, and in* $\mathsf{\Delta^b_1}$-CR *(or equivalently,* $\mathsf{VTC^0}$*).*

Proof: (Pow_2-IP) and (Pow_2-Div) are almost literally the π_2-translations of axioms (P_2-IP) and (P_2-Div). The only difference is that to get (P_2-Div), we should also require $\mathrm{Pow}_2(v/u)$; but this follows from Observation 6.1.

It is well known that IE_1 proves that any two integers have a gcd (even with Bézout cofactors; see the argument in Wilmers [17, Lemma 2.4]). This implies (Pow_2-Div): if $\mathrm{Pow}_2(u)$ and $\mathrm{Pow}_2(v)$, let $d = \gcd(u, v)$. Then $u' = u/d$ and $v' = v/d$ are coprime, hence one of them is odd. Being divisors of the oddless u or v, this implies $u' = 1$ or $v' = 1$, i.e., $u \mid v$ or $v \mid u$.

Working in IE_1, let $x > 0$ be given, and assume there exists an oddless $v > x$. The E_1 formula $\varphi(u) \equiv \exists u' \leq x\,(u' \geq u \wedge u' \mid v)$ satisfies $\varphi(0) \wedge \neg\varphi(x+1)$, thus using E_1-induction, there is u such that $\varphi(u) \wedge \neg\varphi(u+1)$; then u is the largest divisor of v such that $u \leq x$. Since $v/u > 1$ must be even, we have $2u \mid v$, hence $x < 2u$ by the maximality of u, and $\mathrm{Pow}_2(u)$ by Observation 6.1. Thus, $\mathsf{IE}_1 + (\mathrm{Pow}_2\text{-Cof}) \vdash (\mathrm{Pow}_2\text{-IP})$.

IE_2 proves the E_2 formula $\exists u \leq 2x\,(u > x \wedge \mathrm{Pow}_2(u))$ by induction on x, as it is easy to see that $\mathrm{Pow}_2(u)$ implies $\mathrm{Pow}_2(2u)$.

In VTC^0, there is a canonical 2^n function from unary to binary integers, and every binary $X > 0$ can be written as $X = 2^n X'$ with X' odd. It follows easily that $\mathrm{Pow}_2(X)$ holds iff X is in the image of 2^n. Then (Pow_2-IP) follows as $2^{n-1} \leq X < 2^n$ for n given by the length function $|X|$ of VTC^0, and (Pow_2-Div) follows from $2^m = 2^n 2^{m-n}$ (for $n \leq m$). ☐

Corollary 6.3 *The theories* $\mathsf{TEIP}_{\mathrm{Pow}_2}$, $\mathsf{IE}_1 + (\mathrm{Pow}_2\text{-Cof})$, IE_2, *and* Δ^{b}_1-CR *contain* TEIP.

Any model of any of these theories has an elementary extension $\mathfrak{M} = \langle M, \dots\rangle$ *which is an EIP of a RCEF* $\langle \mathfrak{R}, \exp\rangle$ *satisfying GA such that* $\exp[M] = \{u \in M : \mathfrak{M} \vDash \mathrm{Pow}_2(u)\}$. ☐

We mention that Corollary 6.3 does not quite reprove the main result of [7], which guarantees that every countable model of Δ^{b}_1-CR is outright an EIP of a RCEF satisfying GA, without taking an elementary extension first.

If T is $\mathsf{TEIP}_{\mathrm{Pow}_2}$ or any of the stronger $\mathcal{L}_{\mathrm{OR}}$-theories from Theorem 6.2, and $\mathfrak{M} \vDash T$, it is a natural question whether the expansion $\langle \mathfrak{M}, \mathrm{Pow}_2^{\mathfrak{M}}\rangle$ of $\mathfrak{M}$ to a model of TEIP_{P_2} is unique: is it necessary that P_2 consists of oddless numbers for *every* expansion of a model of T to a model of TEIP_{P_2}, perhaps if T is sufficiently strong? In other words, is $T + \mathsf{TEIP}_{P_2}$ equivalent to the expansion of T by the definition $P_2(u) \leftrightarrow \mathrm{Pow}_2(u)$?

Our results from the previous section give a negative answer, even when T is as strong as the true arithmetic:

Theorem 6.4 *Let* T *be a* Σ_1*-sound* $\mathcal{L}_{\mathrm{OR}}$*-theory. Then*

$$T + \mathsf{TEIP}_{P_2} \nvdash P_2(u) \to 3 \nmid u,$$

thus there exists a model $\langle \mathfrak{M}, P_2^{\mathfrak{M}}\rangle \vDash T + \mathsf{TEIP}_{P_2}$ *such that* $P_2^{\mathfrak{M}} \nsubseteq \mathrm{Pow}_2^{\mathfrak{M}} \nsubseteq P_2^{\mathfrak{M}}$.

Proof: Since adding true Π_1 sentences preserves Σ_1-soundness, we may assume $T \supseteq \mathsf{I}\Delta_0 \supseteq \mathsf{TEIP}_{\mathrm{Pow}_2}$. By the proof of Theorem 5.16, for each k there exists $n \in \mathbb{N}$ divisible by 3 (in fact, a power of 6) such that $T + \mathrm{PWin}^1_k(\overline{n})$ is consistent. Thus by compactness, there exists a countable $\mathfrak{M} \vDash T$ and $u \in M$ such that $3 \mid u$ and $\mathfrak{M} \vDash \{\mathrm{PWin}^1_k(u) : k \geq 1\}$. We may assume $\mathfrak{M}$ to be recursively saturated; then by the proof of Theorem 4.7, there exists $P_2 \subseteq M$ such that $\langle \mathfrak{M}, P_2 \rangle \models \mathsf{TEIP}_{P_2}$ and $u \in P_2$. Clearly, $\mathfrak{M} \not\models \mathrm{Pow}_2(u)$. On the other hand, since $\langle \mathfrak{M}, \mathrm{Pow}_2^{\mathfrak{M}} \rangle \models \mathsf{TEIP}_{P_2}$, there is $v < u < 2v$ such that $\mathfrak{M} \models \mathrm{Pow}_2(v)$, and we cannot have $v \in P_2$. □

Let us mention that we do get uniqueness (for sufficiently strong T, namely including (Pow_2-Div)) if we extend TEIP_{P_2} with an axiom ensuring the downward closure of P_2 under divisibility:

Proposition 6.5 *An $\mathcal{L}_{\mathrm{OR}}$-structure $\mathfrak{M} \models$ (Pow_2-Div) has at most one expansion to a model of* TEIP_{P_2} +

$$(P_2\text{-Down}) \qquad \forall u, v \,\bigl(P_2(u) \land v \mid u \to P_2(v)\bigr),$$

namely $\langle \mathfrak{M}, \mathrm{Pow}_2^{\mathfrak{M}} \rangle$.

This follows from the next lemma, characterizing extensions of TEIP_{P_2} in which P_2 is provably defined by Pow_2.

Lemma 6.6 *These theories are equivalent:*

(i) $\mathsf{TEIP}_{P_2} + \forall u \,\bigl(P_2(u) \leftrightarrow \mathrm{Pow}_2(u)\bigr)$.

(ii) $\mathsf{TEIP}_{P_2} + \forall u \,\bigl(P_2(u) \to \mathrm{Pow}_2(u)\bigr) +$ (Pow_2-Div).

(iii) $\mathsf{TEIP}_{P_2} + \forall u \,\bigl(\mathrm{Pow}_2(u) \to P_2(u)\bigr) +$ (Pow_2-Cof).

(iv) $\mathsf{TEIP}_{P_2} +$ (P_2-Down) + (Pow_2-Div).

Proof:

(i) → (iv): (P_2-Down) follows from $\forall u \,\bigl(P_2(u) \leftrightarrow \mathrm{Pow}_2(u)\bigr)$ using Observation 6.1, and $\forall u \,\bigl(\mathrm{Pow}_2(u) \to P_2(u)\bigr)$ and (P_2-Div) imply (Pow_2-Div).

(iv) → (ii): We will show $\mathsf{TEIP}_{P_2} + (P_2\text{-Down}) \vdash P_2(u) \to \mathrm{Pow}_2(u)$. Assume $P_2(u)$, and let $v \mid u$ be such that $v > 1$. Then $P_2(v)$ by (P_2-Down), and $P_2(2)$ by Lemma 3.4, thus v is even by (P_2-Div).

(ii) → (i): We need to show $\mathrm{Pow}_2(u) \to P_2(u)$. Assuming $\mathrm{Pow}_2(u)$, (P_2-IP) gives $v \le u < 2v$ such that $P_2(v)$. Then $\forall u \,\bigl(P_2(u) \to \mathrm{Pow}_2(u)\bigr)$ yields $\mathrm{Pow}_2(v)$, thus $v \mid u$ by (Pow_2-Div). Since $1 \le u/v < 2$, we obtain $v = u$, i.e., $P_2(u)$.

(i) → (iii): TEIP_{P_2} proves $\forall x \,\exists u > x \, P_2(u)$, which together with $\forall u \,\bigl(P_2(u) \to \mathrm{Pow}_2(u)\bigr)$ yields (Pow_2-Cof).

(iii) → (i): We need to show $P_2(u) \to \mathrm{Pow}_2(u)$. Assuming $P_2(u)$, let $v > u$ be such that $\mathrm{Pow}_2(v)$. Then $P_2(v)$ as well, hence $u \mid v$ by (P_2-Div). We get $\mathrm{Pow}_2(u)$ by Observation 6.1. □

7 Discussion

We managed to axiomatize the first-order consequences of being an EIP of RCEF. While we obtained a simple finite list of "obvious" axioms in languages including 2^x of P_2, the axiomatization in the basic language of arithmetic involves an unexpected infinite schema of axioms expressing the existence of winning strategies in PowG.

Unlike the original Shepherdson's theorem, our results only characterize EIP of RCEF up to elementary equivalence, as models of the resulting first-order theories may require an elementary extension to become an EIP of a RCEF. (We know this is sometimes necessary for models of TEIP and TEIP_{P_2} from Example 3.10; we do not have a similar example for TEIP_{2^x}, but it seems very likely that it should exist as well.) We leave open the problem whether a more precise characterization is possible, at least for countable structures.

Another problem we left open is whether TEIP is finitely axiomatizable over IOpen. Theorem 5.16 provides some heuristic support for a negative answer, though the evidence it provides is quite limited (notice that Theorem 5.16 exhibits a strict hierarchy even over $\mathrm{Th}(\mathbb{N})$, whereas TEIP clearly *is* finitely axiomatizable over sufficiently strong theories, e.g. IE_2).

While TEIP is a strict extension of IOpen, it is not quite clear how much stronger it really is. In terms of literal inclusion of theories, TEIP is contained in IE_2 and $\Delta^{\mathsf{b}}_1\text{-}\mathsf{CR}$, but we do not know if it is contained in IE_1. But perhaps a better assessment of the relative strength of TEIP is to estimate the minimal complexity of sentences separating TEIP from IOpen. In particular, a problem suggested by L. Kołodziejczyk is to determine what Diophantine equations are solvable in (extensions with negatives of) models of TEIP, and whether they are the same as those solvable in models of IOpen (or equivalently, in $\mathbb{Z}$-rings, cf. Wilkie [16]); recall that it is an old open question, going back to Shepherdson [13], whether solvability of Diophantine equations in models of IOpen is decidable. A closely related question is whether TEIP is $\forall_1$-conservative over IOpen.

References

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

[2] Sedki Boughattas and Jean-Pierre Ressayre, *Arithmetization of the field of reals with exponentiation extended abstract*, RAIRO – Theoretical Informatics and Applications 42 (2008), no. 1, pp. 105–119.

[3] Gregory Cherlin and Françoise Point, *On extensions of Presburger arithmetic*, in: Proceedings of the 4th Easter Conference on Model Theory (Gross Köris) (B. I. Dahn, ed.), Seminarberichte vol. 86, Humboldt-Universität zu Berlin, 1986, pp. 17–34.

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

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

[6] Wilfrid Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications vol. 42, Cambridge University Press, 1993.

[7] Emil Jeřábek, *Models of* VTC^0 *as exponential integer parts*, Mathematical Logic Quarterly 69 (2023), no. 2, pp. 244–260.

[8] Jan Johannsen and Chris Pollett, *On the* Δ^b_1*-bit-comprehension rule*, in: Logic Colloquium '98: Proceedings of the 1998 ASL European Summer Meeting held in Prague, Czech Republic (S. R. Buss, P. Hájek, and P. Pudlák, eds.), ASL, 2000, pp. 262–280.

[9] Konstantin Kovalyov, *Analogues of Shepherdson's Theorem for a language with exponentiation*, arXiv:2306.02012 [math.LO], 2023, `https://arxiv.org/abs/2306.02012`.

[10] Jitsuro Nagura, *On the interval containing at least one prime number*, Proceedings of the Japan Academy 28 (1952), no. 4, pp. 177–181.

[11] Jean-Pierre Ressayre, *Integer parts of real closed exponential fields*, in: Arithmetic, proof theory, and computational complexity (P. Clote and J. Krajíček, eds.), Oxford Logic Guides vol. 23, Oxford University Press, 1993, pp. 278–288.

[12] Aleksei L. Semenov, *Logical theories of one-place functions on the set of natural numbers*, Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya 47 (1983), no. 3, pp. 623–658 (in Russian), English translation in: Mathematics of the USSR, Izvestiya 22 (1984), no. 3, pp. 587–618.

[13] John C. Shepherdson, *A nonstandard 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, pp. 79–86.

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

[15] Lars Svenonius, *On the denumerable models of theories with extra predicates*, in: The Theory of Models, Proceedings of the 1963 International Symposium at Berkeley, Studies in Logic and the Foundations of Mathematics, North-Holland, 1965, pp. 376–389.

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

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