On the theory of exponential integer parts

Emil Jeřábek

Institute of Mathematics
Czech Academy of Sciences
jerabek@math.cas.cz
https://users.math.cas.cz/~jerabek/

Mathematical Logic:
Proof Theory, Constructive Mathematics

November 2023, Oberwolfach

Shepherdson's theorem

Integer part (IP) of an ordered* group/ring R:

- discretely ordered subgroup/ring $D \subseteq R$, $\min D_{>0} = 1$
- all elements of R within distance < 1 from D

Theorem (Shepherdson '64)
Integer parts of real-closed fields = models of IOpen

IOpen: Robinson's arithmetic/discretely ordered rings
+ open (= quantifier-free) induction in $\mathcal{L}_{\mathrm{OR}} = \langle +, \cdot, < \rangle$

* ordered structures assumed totally ordered and commutative

Exponential integer parts

Exponential ordered field $\langle R, +, \cdot, <, \exp\rangle$:

- $\langle R, +, \cdot, <\rangle$ ordered field
- isomorphism $\exp\colon \langle R, 0, 1, +, <\rangle \to \langle R_{>0}, 1, 2, \cdot, <\rangle$
- $\pm$ growth axiom (GA): $\exp(x) > x$

Exponential integer part (EIP): IP $D \subseteq R$ s.t. $\exp[D_{>0}] \subseteq D_{>0}$

(Ressayre '93)

Q: What $\mathcal{L}_{\mathrm{OR}}$-structures are EIP of real-closed exponential fields (RCEF)? What is their first-order theory?

Previous work

EIP of extensions of RCEF studied by
(Boughattas & Ressayre '08), (Kovalyov '23)

- language with $x^y = \exp(y \log x)$
- can use direct construction of RCEF R from D: approximate $\exp(x/y)$ with $\frac{1}{t}\lfloor \sqrt[y]{t^y x} \rfloor$
- not possible in $\mathcal{L}_{\mathrm{OR}}$ or $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$ $\Longrightarrow$ we will rely on model-theoretic conservativity results

Upper bound (J '23):
Countable models of the bounded arithmetic Δ^b_1-CR (VTC^0) are EIP of RCEF

Language with 2^x

Theorem: The theory TEIP_{2^x} of EIP of RCEF in $\mathcal{L}_{\mathrm{OR}} \cup \{2^x\}$ is axiomatized by IOpen +

$$x > 0 \to \exists y\, x < 2^y \le 2x$$
$$2^{x+y} = 2^x 2^y$$
$$2^x \ne 0$$

EIP of RCEF + GA: TEIP_{2^x} + GA

Proof sketch:

- joint consistency $\implies$ elementarily embed $\mathfrak{M} \vDash \mathrm{TEIP}_{2^x}$ in an IP of RCEF $\langle R, \exp\rangle$
- new exponential: combine $\exp \restriction [0,1)$ with $2^x \implies$ EIP

Language with P_2

$P_2(x)$: predicate for the image of 2^x

Theorem: The theory TEIP_{P_2} of EIP of RCEF $\pm$ GA in $\mathcal{L}_{\mathrm{OR}} \cup \{P_2\}$ is axiomatized by IOpen +

$$x > 0 \to \exists u \, (P_2(u) \land u \le x < 2u)$$

$$P_2(u) \land P_2(v) \land u \le v \to \exists w \, (P_2(w) \land uw = v)$$

Proof method:

- $\mathfrak{M} \vDash \mathrm{TEIP}_{P_2} \implies \mathfrak{M} \prec \mathfrak{M}^* \vDash \mathrm{TEIP}_{2^x}$: joint consistency
- for $\mathrm{TEIP}_{2^x} + \mathrm{GA}$: messy back-and-forth argument

The power-of-2 game

$\mathrm{PowG}_n(\mathfrak{M})$: in round $i < n$,

- Challenger plays $x_i \in M_{>0}$
- Powerator plays $u_i \in M_{>0}$ s.t. $u_i \le x_i < 2u_i$

Challenger wins if $u_i u_j < u_k < 2u_i u_j$ for some $i, j, k < n$

(NB: $u_i \le u_j$, $u_i \nmid u_j \implies$ Challenger can win next round)

Motivation: $\langle \mathfrak{M}, P_2 \rangle \vDash \mathrm{TEIP}_{P_2} \implies$
"play $u_i \in P_2$" is a winning strategy for Powerator

EIP in $\mathcal{L}_{\mathrm{OR}}$

Theorem: The theory TEIP of EIP of RCEF ± GA in $\mathcal{L}_{\mathrm{OR}}$ is axiomatized by IOpen +

$$\forall x_0\,\exists u_0\,\dots\,\forall x_{n-1}\,\exists u_{n-1}\,\Bigl(\bigwedge_{i<n}(x_i>0\to u_i\le x_i<2u_i)\\ \land\bigwedge_{i,j,k<n}\neg(u_iu_j<u_k<2u_iu_j)\Bigr)$$

for all $n\in\mathbb{N}$ ("Powerator wins PowG_n")

- $\mathfrak{M}\vDash$ TEIP countable, recursively saturated $\implies$ Powerator wins $\mathrm{PowG}_\omega(\mathfrak{M})$
- Challenger enumerates $M_{>0}$ $\implies$ $P_2:=\{u_i:i<\omega\}$ yields $\langle\mathfrak{M},P_2\rangle\vDash\mathrm{TEIP}_{P_2}$

Oddless numbers

Natural algebraic interpretation of P_2 in arithmetic:

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

Lemma: Pow_2 gives an interpretation of TEIP_{P_2} in

- $\mathrm{IOpen} + \forall x > 0 \, \exists u \, \big(\mathrm{Pow}_2(u) \land u \le x < 2u\big)$
  $+ \forall x, y \, \big(\mathrm{Pow}_2(x) \land \mathrm{Pow}_2(y) \land x < y \to x \mid y\big)$
- $\mathrm{IE}_1 + \forall x \, \exists u > x \, \mathrm{Pow}_2(u)$
- IE_2
- Δ^b_1-CR / VTC^0

$\implies$ these theories prove TEIP

Examples

- IOpen doesn't prove the following consequence of TEIP:

$$\forall x\, \exists u > x\, \forall y\, \bigl(0 < y < x \to \exists v\, (v \le y < 2v \wedge v \mid u)\bigr)$$

  - there is a nonstandard $\mathfrak{M} \vDash \mathrm{IOpen}$ which is a UFD (Smith '93)
  - $u \in M \smallsetminus \mathbb{N} \implies u$ has a largest standard divisor u_0
    take $y \in \mathbb{N}$, $y > 2u_0$
- Shepherdson's model of IOpen expands to a model of TEIP_{P_2}, but not to a model of TEIP_{2^x}
- $\mathrm{Th}(\mathbb{N}) + \mathrm{TEIP}_{P_2} \nvdash P_2(x) \to 3 \nmid x$
  - expansion to a model of TEIP_{P_2} not unique
  - Challenger needs an unbounded number of rounds to win from a non-power-of-2 (more below . . .)

Finite axiomatizability

Question: Is TEIP finitely axiomatizable over IOpen?

TEIP =

$$\mathrm{IOpen} + \left\{\forall x_0 > 0\, \exists u_0\, \big(u_0 \le x_0 < 2u_0 \wedge \theta^1_n(u_0)\big) : n \in \mathbb{N}\right\}$$

where $\theta^1_n(u_0)$ denotes

$$\forall x_1\, \exists u_1\, \dots\, \forall x_{n-1}\, \exists u_{n-1} \Big(\bigwedge_{0<i<n} (x_i > 0 \to u_i \le x_i < 2u_i) \wedge \bigwedge_{i,j,k<n} \neg(u_i u_j < u_k < 2u_i u_j)\Big)$$

Partial answer:
$\{\theta^1_n(u) : n \in \mathbb{N}\}$ forms an infinite hierarchy over $\mathrm{Th}(\mathbb{N})$

(see below ...)

PowG **on standard integers**

$\mathrm{PowG}^t_n(u_0, \dots, u_{t-1})$: as $\mathrm{PowG}_n(\mathbb{N})$, but first t rounds fixed

NB: $\mathbb{N} \vDash \theta^1_n(u) \iff$ Powerator wins $\mathrm{PowG}^1_n(u)$

Lemma: If some u_i is not a power of 2, Challenger wins $\mathrm{PowG}^t_n(\vec{u})$ for large enough n

$c(\vec{u}) = \min\{n : \text{Challenger wins } \mathrm{PowG}^t_{t+n}(\vec{u})\}$

Goal: $\{c(u) : u \text{ not a power of } 2\}$ unbounded

Needs delicate bounds, as Challenger can very efficiently exploit irregularities in exponents

Upper bound

Lemma: $v \le u^n$, $v \nmid u^n \implies c(u,v) \le \log\log n + O(1)$

Theorem: $u = 2^{\nu_2(u)} v^r$, $v > 1$ not a perfect power $\implies$

$$\begin{aligned} c(u) &\le \log\log\log \min\{\nu_2(u), r\} + O(1) \\ &\le \log\log\log\log u + O(1) \end{aligned}$$

More precisely: for all d (wlog prime power),

$$d \nmid r \implies c(u) \le \log\log d + O(1)$$

Lower bound

Theorem: For $u = 2^{\nu_2(u)} v^r$, $v > 1$:

$$c(u) \geq \min\left\{\log\log\log\frac{\nu_2(u)}{\log v}, \log\log d : d \nmid r\right\} + O(1)$$

Example: $c\left(6^{2^{2^k}}!\right) = k + O(1)$

Corollary:

- $\{\theta^1_n(u) : n \in \mathbb{N}\}$ forms an infinite hierarchy over $\mathrm{Th}(\mathbb{N})$
- $\mathrm{Th}(\mathbb{N}) + \mathrm{TEIP}_{P_2} \nvdash P_2(x) \to 3 \nmid x$

Problem: Is TEIP finitely axiomatizable over IOpen?

References

- S. Boughattas, J.-P. Ressayre: Arithmetization of the field of reals with exponentiation extended abstract, RAIRO – Theoretical Informatics and Applications 42 (2008), 105–119
- E. J.: Models of VTC^0 as exponential integer parts, Mathematical Logic Quarterly 69 (2023), 244–260
- K. Kovalyov: Analogues of Shepherdson's Theorem for a language with exponentiation, arXiv:2306.02012 [math.LO], 2023
- J.-P. Ressayre: Integer parts of real closed exponential fields, in: Arithmetic, proof theory, and computational complexity, Oxford Univ. Press, 1993, 278–288
- J. Shepherdson: A nonstandard model for a free variable fragment of number theory, Bull. Acad. Polon. Sci. 12 (1964), 79–86
- S. Smith: Building discretely ordered Bezout domains and GCD domains, Journal of Algebra 159 (1993), 191–239