# Towards analysis in $\mathrm{VTC}^0$

Emil Jeřábek

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

Proof Complexity 2024

University of Oxford, September 2024

# Feasible analytic reasoning

Formalization of mathematical results in bounded arithmetic:

- feasible reasoning, “bounded reverse mathematics”
- uniform propositional proofs
- consistency of computational complexity conjectures

Typically: finite combinatorics, elementary number theory

Some arguments use tools from real/complex analysis:

- eigenvalues and eigenvectors
- generating functions in enumerative combinatorics
- analytic number theory

Can we do such things in bounded arithmetic?

# $\mathbf{TC}^0$ and $\mathrm{VTC}^0$

Minimal complexity class: $\mathbf{TC}^0$

- $+, -, \cdot, /, \sum_{i<n} X_i, \prod_{i<n} X_i$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}(i)$ [HAB'02]
- approximation of functions given by nice power series: exp, log, sin, arctan, $\sqrt[k]{x}, \dots$

Corresponding theory: $\mathrm{VTC}^0$ [NC'06,CN'10]

- formalize basic arithmetic operations incl. $\prod_{i<n} X_i$ [J'22]
- model-theoretic construction of "reals": $\mathfrak{M} \vDash \mathrm{VTC}^0 \rightsquigarrow \mathbf{Q}^{\mathfrak{M}} \rightsquigarrow$ topological completion $\mathbf{R}^{\mathfrak{M}}, \mathbf{C}^{\mathfrak{M}}$
  - $\mathbf{R}^{\mathfrak{M}}$ real-closed field, $\mathbf{C}^{\mathfrak{M}}$ alg. closed [J'15]
  - construction of elementary analytic functions on $\mathbf{C}^{\mathfrak{M}}$: exp, log, trigonometric, hyperbolic, their inverses [J'23]
  - no general theory of analytic functions

Can't quantify over reals, sequences, functions, ...

$\Longrightarrow$ need a more robust setup

# $\mathrm{VTC}^0$ with infinite sets

$\mathrm{VTC}^0$: Zambella-style two-sorted bounded arithmetic

- unary (index/auxiliary) integers: $0, 1, +, \cdot, \le$
- finite sets $\approx$ binary integers $\approx$ binary strings: $\in$, $|X|$

$\mathrm{VTC}^0_\infty$: two-sorted arithmetic with infinite sets

- unary (index/auxiliary) integers: $0, 1, +, \cdot, \le$
- sets of unary integers: $\in$ (no $=$)
- Robinson's arithmetic, induction:
  $0 \in X \land \forall n\,(n \in X \to n+1 \in X) \to \forall n\, n \in X$
- comprehension: $\exists X\, \forall n\,(n \in X \leftrightarrow \varphi)$, $\varphi \in \Sigma^B_0 = \Delta^0_0$
- counting:
  $$\forall X\, \exists C\colon\ C^{(0)} = 0 \land \forall n\, C^{(n+1)} = \begin{cases} C^{(n)} & n \notin X \\ C^{(n)} + 1 & n \in X \end{cases}$$

# Reals in $\mathrm{VTC}^0_\infty$

Encode stuff in $\mathrm{VTC}^0_\infty$:

- finite sets: set $X$ + bound $n$
  $\rightsquigarrow$ binary strings, integers, rationals as usual in $\mathrm{VTC}^0$
- sequences of binary objects: $\{X_n : n \in \mathbf{L}\}$, $X_n \subseteq [0, n^c)$
  ($\mathbf{L}$ = unary integers, $c \in \mathbb{N}$ standard constant)
  encoded by $X$: $X_n = \{i < n^c : \langle n, i\rangle \in X\}$
- real numbers: sequence of integers $\alpha = \{A[n] : n \in \mathbf{L}\}$
  s.t. $|A[n] - 2^{-m} A[n+m]| \le 1$
  - even more formally: $A[0]$ plus $\{A[n] - 2^n A[0] : n \in \mathbf{L}\}$
  - represents $\alpha = \lim_n \alpha[n]$, where $\alpha[n] := 2^{-n} A[n]$
  - "known" $\alpha$ represented by $A[n] = \lfloor 2^n \alpha \rceil := \left\lfloor 2^n \alpha + \frac{1}{2} \right\rfloor$
  - comparison:

$$\alpha \le \beta \iff \forall n\, A[n] \le B[n] + 2$$

$$\alpha \approx \beta \iff \alpha \le \beta \wedge \beta \le \alpha$$

# Related work

Buss '85: variants of $V_1^i$, $U_1^i$ with infinite sets

F. Ferreira, G. Ferreira, A. Fernandes: theories for analysis

- BTFA $\approx \mathrm{S}^1_2 + \mathrm{B}\Sigma^b_\infty +$ recursive comprehension
- binary strings (numbers), sets of binary strings
- cons. over $\mathrm{S}^1_2 + \mathrm{B}\Sigma^b_\infty$, $\Pi^0_2$-cons. over $\mathrm{S}^1_2 \approx \mathrm{V}^1 \supseteq \mathrm{VTC}^0$
- BTFA $+ \Sigma^b_\infty$-WKL $\Pi^1_1$-cons. over BTFA
- for Riemann integration:
- TCA$^2$: BTFA-like extension of TCA = theory for **CH**
- TCA $\approx$ (quasipoly) $\mathrm{VTC}^0$, but unary numbers reinterpreted as binary $\implies$ exponentially stronger

# $\mathrm{VTC}^0_\infty$ vs. $\mathrm{VTC}^0$

$\mathfrak{M} = \langle M_1, M_2, \dots \rangle \vDash \mathrm{VTC}^0_\infty$, $M_2 \subseteq \mathcal{P}(M_1)$
$\rightsquigarrow$ canonical $\mathfrak{M}' = \langle M_1, M_2', \dots \rangle \vDash \mathrm{VTC}^0$:

$$\begin{aligned} M_2' &= \{X \in M_2 : \exists n \in M_1\ X \subseteq [0,n)\} \\ &= \{X \cap [0,n) : X \in M_2, n \in M_1\} \end{aligned}$$

$\mathfrak{M} = \langle M_1, M_2, \dots \rangle \vDash \mathrm{VTC}^0$, $M_2 \subseteq \mathcal{P}(M_1)$
$\rightsquigarrow$ expands to many models of $\mathrm{VTC}^0_\infty$

- minimal: $\mathfrak{M}^\perp = \langle M_1, M_2^\perp, \dots \rangle$, $M_2^\perp =$ subsets of $M_1$ definable by $\mathbf{TC}^0$-formulas with parameters from $M_2$
- maximal: $\mathfrak{M}^\top = \langle M_1, M_2^\top, \dots \rangle$,

$$M_2^\top = \{X \subseteq M_1 : \forall n \in M_1\ X \cap [0,n) \in M_2\}$$

$\mathrm{VTC}^0_\infty$ is a conservative extension of $\mathrm{VTC}^0$

# Universal conservative extensions

In the spirit of Cook & Nguyen's $\widehat{\mathrm{VTC}}^0$ and $\overline{\mathrm{VTC}}^0$, we have

$\widehat{\mathrm{VTC}}^0_\infty$: new function symbols $\min(X \cup \{n\})$, $\{u : \varphi(u, \vec{n}, \vec{X})\}$ for $\varphi \in \Sigma^B_0$, $C(X)$: counting function for $X$

$\overline{\mathrm{VTC}}^0_\infty$: also $\{u : \varphi(u, \vec{n}, \vec{X})\}$ for $\varphi \in \Sigma^B_0(\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty})$

- universally axiomatized
- $\overline{\mathrm{VTC}}^0_\infty \vdash \Sigma^B_0(\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty})$-comprehension, induction
- all $\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty}$-functions $\Delta^B_1$-bit-definable in $\mathrm{VTC}^0_\infty$
- witnessing theorem: $\overline{\mathrm{VTC}}^0_\infty \vdash \forall \vec{n}, \vec{X}\, \exists \vec{m}, \vec{Y}\, \varphi(\vec{n}, \vec{x}, \vec{m}, \vec{Y})$, $\varphi \in \Sigma^1_1(\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty}) \implies$ there are $\mathcal{L}_{\overline{\mathrm{VTC}}^0_\infty}$-terms $\vec{t}$, $\vec{T}$ s.t.

$$\overline{\mathrm{VTC}}^0_\infty \vdash \forall \vec{n}, \vec{X}\, \varphi\big(\vec{n}, \vec{X}, \vec{t}(\vec{n}, \vec{X}), \vec{T}(\vec{n}, \vec{X})\big)$$

# Feasibly Cauchy sequences

sequence of reals $\{\alpha_n : n \in \mathbf{L}\}$
encoded as a double sequence $\{A_n[m] : n, m \in \mathbf{L}\}$

polynomially Cauchy:
$\forall n, m \geq p(k), r > k : \ |A_n[r] - A_m[r]| \leq 2^{r-k}$ for some poly $p$

$\Longrightarrow$ limit $\alpha$ in $\mathrm{VTC}^0_\infty$: $A[n] = \left\lfloor \frac{1}{16} A_{p(n+3)}[n+4] \right\rceil$

(a bit simpler for a sequence of rationals)

Application: define arithmetical operations on reals

- $\alpha + \beta = \lim_n 2^{-n}(A[n] + B[n])$
- $\alpha \cdot \beta = \lim_n 2^{-2n} A[n] B[n]$

# Algebraic properties

$\mathsf{VTC}^0_\infty$ proves $\langle \mathbb{R}, +, \cdot \rangle$ is an ordered field

Adapting [J'15] to $\mathsf{VTC}^0_\infty$:
$\mathbb{R}$ is a real-closed field, $\mathbb{C}$ algebraically closed
(wrt polynomials of standard degree)

Recall: $\mathfrak{M} \vDash \mathsf{VTC}^0 \rightsquigarrow \mathfrak{M}^\perp, \mathfrak{M}^\top \vDash \mathsf{VTC}^0_\infty$
binary rationals $\mathbf{Q}^{\mathfrak{M}} \rightsquigarrow$ topological completion $\mathbf{R}^{\mathfrak{M}}$

Fact: $\mathfrak{M} \vDash \mathsf{VTC}^0$ countable $\implies \mathbf{R}^{\mathfrak{M}} \simeq \mathbb{R}^{\mathfrak{M}^\top}$

In general: $\mathfrak{M}^* \vDash \mathsf{VTC}^0_\infty$ expands $\mathfrak{M} \vDash \mathsf{VTC}^0$
$\implies \mathbb{R}^{\mathfrak{M}^*}$ embeds in $\mathbf{R}^{\mathfrak{M}}$

# Further constructions

real/complex sequence $\{\alpha_n : n \in \mathbf{L}\}$
$\rightsquigarrow$ unique (up to $\approx$) sequences of partial sums and products $\{\sum_{n<m} \alpha_n : m \in \mathbf{L}\}$, $\{\prod_{n<m} \alpha_n : m \in \mathbf{L}\}$ s.t.

$$\sum_{n<0} \alpha_n \approx 0 \qquad \prod_{n<0} \alpha_n \approx 1$$

$$\sum_{n<m+1} \alpha_n \approx \alpha_m + \sum_{n<m} \alpha_n \qquad \prod_{n<m+1} \alpha_n \approx \alpha_m \prod_{n<m} \alpha_n$$

Adapting [J'23]: $\mathrm{VTC}^0_\infty$ has well-behaved definitions of elementary analytic functions
(exp, log, trigonometric, hyperbolic, inv. trig., inv. hyp.)

# What's next?

Develop a reasonable theory of

- sequences, sums
- Taylor series
- basic complex analysis
- ...

to support analytic arguments in combinatorics, number theory

No fixed set of goals

# References


- S. R. Buss: Bounded arithmetic, Bibliopolis, Naples, 1986
- S. Cook, P. Nguyen: Logical foundations of proof complexity, Cambridge Univ. Press, 2010
- A. M. Fernandes, F. Ferreira, G. Ferreira: Analysis in weak systems, in Logic and computation: Essays in honour of Amílcar Sernadas, College Publication, 2017, 231–262
- F. Ferreira: A feasible theory for analysis, J. Symb. Logic 59 (1994), 1001–1011
- F. Ferreira, G. Ferreira: The Riemann integral in weak systems of analysis, J. Univ. Computer Sci. 14 (2008), 908–937
- W. Hesse, E. Allender, D. M. Barrington: Uniform constant-depth threshold circuits for division and iterated multiplication, J. Comp. System Sci. 65 (2002), 695–716
- E. Jeřábek: Open induction in a bounded arithmetic for $\mathbf{TC}^0$, Arch. Math. Logic 54 (2015), 359–394
- E. Jeřábek: Iterated multiplication in $\mathrm{VTC}^0$, Arch. Math. Logic 61 (2022), 705–767
- E. Jeřábek: Elementary analytic functions in $\mathrm{VTC}^0$, Ann. Pure Appl. Logic 174 (2023), 103269
- P. Nguyen, S. Cook: Theories for $TC^0$ and other small complexity classes, Log. Methods Comput. Sci. 2 (2006), art. 3