Towards complex analysis in VTC^0

Emil Jeřábek

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

Proof Complexity 2025

University of Oxford, August 2025

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 complex analysis:

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

Can we do such things in bounded arithmetic?

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

Suitable complexity class: uniform $\mathbf{TC}^0$

- $+, -, \cdot, /, \sum_{i<n} X_i, \prod_{i<n} X_i$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}(i)$ [HAB'02]
- approximation of functions given by nice power series

Corresponding theory: VTC^0 [NC'06,CN'10]

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

Can't quantify over reals, sequences, functions, ...
$\Longrightarrow$ need a more robust setup

NB: Theories for real analysis (Ferreira, Ferreira, Fernandes)
— too strong in several respects

VTC^0 with infinite sets

VTC^0: Zambella-style two-sorted bounded arithmetic

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

VTC^0_∞: two-sorted arithmetic with infinite sets

- unary (index/auxiliary) integers: $0, 1, +, \cdot, \leq$
- sets of unary integers: $\in$ (no $=$)
- Q, induction, comprehension for $\Sigma^B_0 = \Delta^0_0$ formulas:
  $\exists X\, \forall n\, (n \in X \leftrightarrow \varphi)$
- $\exists$ counting functions for sets
- finite sets encoded as a set X + a bound n

VTC^0_∞ is fully conservative over VTC^0

$\forall\exists$ theorems of VTC^0_∞ witnessed by "infinitary $\mathbf{TC}^0$ functions"

NB: [Buss'85] variants of V^i_1, U^i_1 with infinite sets

Objects encodable in VTC^0_∞

- sequences of binary objects: $\{X_n\}_{n\in\mathbf{L}}$, $X_n \subseteq [0, n^c)$
  ($\mathbf{L}$ = unary/logarithmic integers, $c \in \mathbb{N}$ standard constant)
  encoded as $X_n = \{j < n^c : \langle n, j\rangle \in X\}$
- real numbers: sequence of integers $a = \{A[n]\}_{n\in\mathbf{L}}$ s.t. $|A[n] - 2^{-m}A[n+m]| \le 1$
  - represents $a = \lim_n 2^{-n}A[n]$
  - comparison: $a \le b \iff \forall n \in \mathbf{L}\; A[n] \le B[n] + 2$
  - complex numbers $z = x + iy$
- double sequences $\{X_{n,m}\}_{n,m\in\mathbf{L}}$
  $\Longrightarrow$ real/complex sequences $\{a_n\}_{n\in\mathbf{L}}$
  $\Longrightarrow$ power series $f(z) = \sum_n a_n(z-w)^n$
- analytic functions: sequence of power series (see later)

Convergence and power series

Sequence with a polynomial modulus of Cauchyness has a limit

- arithmetical operations $+, \cdot \implies \mathbb{R}$ is an ordered field
  - adapting [J'15] to VTC^0_∞: $\mathbb{R}$ is a RCF, $\mathbb{C}$ ACF
  - more generally: $\{a_n\}_{n\in\mathbf{L}} \mapsto \{\sum_{n<N} a_n\}_{N\in\mathbf{L}}, \{\prod_{n<N} a_n\}_{N\in\mathbf{L}}$
- adapting [J'23]: VTC^0_∞ has well-behaved definitions of elementary analytic functions (exp, log, sin, arctan, ...)

Convergence properties of power series $f(z) = \sum_n a_n z^n$:

- $\sum_n a_n z^n$ converges for $|z| <^* r$ if $a_n = O(r^{-n})$
  $\{a_n z^n\}_{n\in\mathbf{L}}$ unbounded for $|z| \geq r$ if $a_n \neq O(r^{-n})$
- def.: $\sum_n a_n z^n$ has radius of convergence $\geq \varrho$ if $a_n = O(r^{-n})$ for all $r <^* \varrho$
- $r <^* \varrho \implies$ converges polynomially uniformly on $B(0, r)$

Notation: $x <^* y \iff x \leq y(1 - m^{-1})$ for some $m \in \mathbf{L}$

Operations on power series

Derivatives and primitive functions $f^{(n)}(z)$, $n \in \mathbf{Z_L}$:

- explicit formula; same radius of convergence

$\sum_{n<N} f_n$: term-wise

$\prod_{n<N} f_n$, $f(g(z))$: $(g(0)=0)$

- polynomials: evaluate at $\{e^{2\pi ij/m}\}_{j<m}$, interpolate (DFT)
- power series: apply to partial sums

Shift: $f(z) = \sum_n a_n(z-u)^n \mapsto f_v(z) = \sum_n b_n(z-v)^n$

- f radius $\geq \varrho$, $|v-u| <^* \varrho \implies f_v$ radius $\geq \varrho - |v-u|$
- $|w-v| + |v-u| <^* \varrho \implies f(w) = f_v(w)$
  more generally: $f_w = (f_v)_w$

Analytic functions

$f : \Omega \to \mathbb{C}$ represented by $\{w_k, \varrho_k, a_{k,n}\}_{k,n\in\mathbf{L}}$ where

- $f_k(z) := \sum_n a_{k,n}(z - w_k)$ has radius of convergence $\geq \varrho_k$
- domain $\Omega = \bigcup_k B^*(w_k, \varrho_k/3)$
- $|w_k - w_l| <^* \varrho_k \implies f_l = (f_k)_{w_l}$ (f_k shifted to w_l)

$z \in \Omega \implies f(z) := f_k(z)$ for any k s.t. $z \in B^*(w_k, \varrho_k/3)$

- independent of the choice of k
- more generally: $f_z := (f_k)_z$ also independent

Contour integration

Analytic function $f = \bigcup_k f_k$ as above,
$f_k(z) = \sum_n a_{k,n}(z - w_k)^n$ radius $\ge \varrho_k$

γ piecewise linear path with endpoints $\{z_j : j \le \ell\}$

Define $\displaystyle\int_\gamma f(z)\,dz := \sum_{j<\tilde\ell} \bigl(F_{k_j}(\tilde z_j) - F_{k_j}(\tilde z_{j+1})\bigr)$ if

- $\tilde\gamma \equiv \{\tilde z_j : j \le \tilde\ell\}$ subdivision of γ
- $\tilde z_j, \tilde z_{j+1} \in B^*(w_{k_j}, \varrho_{k_j}/3)$ for each $j < \tilde\ell$
- F_k = the primitive function of f_k

VTC^0_∞ proves

- uniqueness
- existence if γ covered by $\bigcup_{k<K} B^*(w_k, \varrho_k/3)$

What's next?

Work in progress

Some goals to pursue:

- Cauchy's residue theorem and calculus of residues
- root counting (argument principle, Rouché's theorem)
- analytic continuation, monodromy
- maximum modulus principle
- ...

Applications in combinatorics, number theory

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 VTC^0, Arch. Math. Logic 61 (2022), 705–767
- E. Jeřábek: Elementary analytic functions in 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