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/

Computability in Europe
Lisbon, July 2025

Arithmetic and complexity

Correspondence of theories of bounded arithmetic T and computational complexity classes C:

- provably total computable functions of T are C-functions
- T can reason using C-predicates (comprehension, induction, minimization, ...)

$\Longrightarrow$ "feasible reasoning", "bounded reverse mathematics"

- what can we prove using only concepts computable in C?
- finite combinatorics, elementary number theory, ...
- this talk: can we have tools from complex analysis?
  - generating functions in enumerative combinatorics
  - analytic number theory
  - eigenvalues and eigenvectors, ...

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

Suitable complexity class: uniform $\mathbf{TC}^0$ (contained in $\mathbf{L} \subseteq \mathbf{P}$)

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

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] $\mathfrak{M} \vDash VTC^0 \rightsquigarrow \mathbf{Q}^{\mathfrak{M}} \rightsquigarrow$ topological completion $\mathbf{R}^{\mathfrak{M}}, \mathbf{C}^{\mathfrak{M}}$
  - $\mathbf{R}^{\mathfrak{M}}$ real-closed field, $\mathbf{C}^{\mathfrak{M}}$ algebraically closed
  - 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

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

Comparison with related work

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

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

- BTFA: based on $\mathrm{S}^1_2 \approx \mathrm{V}^1 \supseteq \mathrm{VTC}^0$
- binary strings (numbers), sets of binary strings
- extra principles: collection, WKL
- theory TCA^2 for Riemann integration:
  BTFA-like extension of TCA $=$ theory for **CH**
  TCA $\approx$ (quasipoly) VTC^0, but unary numbers
  reinterpreted as binary $\implies$ exponentially stronger

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

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

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 $a = \lim_n 2^{-n}A[n]$
  $\implies$ complex numbers $z = x + iy$
- double sequences $\{X_{n,m}\}_{n,m\in\mathbf{L}}$
  $\implies$ real/complex sequences $\{a_n\}_{n\in\mathbf{L}}$
  $\implies$ power series $f(z) = \sum_n a_n(z-w)^n$
- analytic functions: $\{w_k, r_k, a_{k,n}\}_{k,n\in\mathbf{L}}$ s.t. (roughly)
  - $f_k(z) = \sum_n a_{k,n}(z - w_k)$ radius of convergence $\ge r_k$
  - domain covered by $\bigcup_k B(w_k, r_k/3)$
  - $|w_k - w_l| < r_k \implies f_l$ is f_k shifted to w_l

Convergence and power series

Sequence with a polynomial modulus of Cauchyness has a limit

- arithmetical operations $+, \cdot$
  more generally: $\{a_n\}_{n\in\mathbf{L}} \mapsto \left\{\sum_{n<N} a_n\right\}_{N\in\mathbf{L}}, \left\{\prod_{n<N} a_n\right\}_{N\in\mathbf{L}}$
- $f(z) = \sum_n a_n z^n$ converges for $|z| <^* r$ if $a_n = O(r^{-n})$
  $x <^* y \iff x \le y(1 - m^{-1})$ for some $m \in \mathbf{L}$

Operations on power series:

- derivatives and primitive functions $f^{(n)}(z)$, $n \in \mathbf{Z_L}$
- shift: $f(z) = \sum_n a_n (z-u)^n \mapsto f(z) \equiv \sum_n b_n (z-v)^n$
- $\sum_{n<N} f_n$, $\prod_{n<N} f_n$
- $f(g(z))$

Contour integration

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

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

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

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

VTC^0_∞ proves

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

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
- ...

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