Elementary analytic functions in VTC^0

Emil Jeřábek

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

Complexity Theory with a Human Face
June 2022, Špindlerův Mlýn

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

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

2. Elementary analytic functions

Theories vs. complexity classes

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, ...)

Feasible reasoning:

- Given a concept $X \in C$, what can we prove about X while reasoning only with concepts from C?
- Formalization: what does T prove about X?

This talk:
$X =$ elementary integer arithmetic operations $+, \cdot, \leq$

The class $\mathbf{TC}^0$

$$\mathbf{AC}^0 \subseteq \mathbf{ACC}^0 \subseteq \mathbf{TC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{AC}^1 \subseteq \cdots \subseteq \mathbf{P}$$

$\mathbf{TC}^0$ = dlogtime-uniform $O(1)$-depth $n^{O(1)}$-size
unbounded fan-in circuits with threshold gates

= **FOM**-definable on finite structures
representing strings
(first-order logic with majority quantifiers)

= $O(\log n)$ time, $O(1)$ thresholds
on a threshold Turing machine

= Constable's $\mathcal{K}$: closure of $+, -, \cdot, /$ under substitution
and polynomially bounded $\sum$, $\prod$

$\mathbf{TC}^0$ and arithmetic operations

For integers given in binary:

- $+$ and $\leq$ are in $\mathbf{AC}^0 \subseteq \mathbf{TC}^0$
- $\times$ is in $\mathbf{TC}^0$ ($\mathbf{TC}^0$-complete under $\mathbf{AC}^0$ reductions)

$\mathbf{TC}^0$ can also do:

- iterated addition $\sum_{i<n} X_i$
- integer division and iterated multiplication [BCH'86,CDL'01,HAB'02]
- the corresponding operations on $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, ...
- approximate functions given by nice power series:
  - $\sin X$, $\log X$, $\sqrt[k]{X}$, ...
- sorting, ...

$\Longrightarrow$ $\mathbf{TC}^0$ is the right class for basic arithmetic operations

The theory VTC^0

- Zambella-style two-sorted bounded arithmetic
  - unary (auxiliary) integers with $0, 1, +, \cdot, \leq$
  - finite sets = binary integers = binary strings
- Noteworthy axioms:
  - Σ^B_0-comprehension (Σ^B_0 = bounded, w/o SO q'fiers)
  - every set has a counting function
- Correspondence to $\mathbf{TC}^0$:
  - provably total computable (i.e., $\exists\Sigma^B_0$-definable) functions are exactly the $\mathbf{TC}^0$-functions
  - has induction, minimization, ... for $\mathbf{TC}^0$-predicates
- Basic binary integer arithmetic in VTC^0:
  - can define $+, \cdot, \leq$ on binary integers
  - proves integers form a discretely ordered ring (DOR)

TC^0 feasible reasoning

What else can VTC^0 do with basic arithmetic operations?

- [J'22] Iterated multiplication and division
  - formalize a variant of the [HAB'02] algorithm
  - raised as a problem in [Ats'03,NC'06]
- [J'15] Open induction in $\langle +, \cdot, < \rangle$ (*IOpen*)
  - $\approx$ constant-degree polynomial root approximation
  - ideas of [Man'91] $\implies$ (*RSUV* translation of) Σ^b_0-minimization in Buss's language

Elementary analytic functions

1. $\mathbf{TC}^0$ and VTC^0
2. Elementary analytic functions

$\mathbf{TC}^0$ analytic functions

Recall: $\mathbf{TC}^0$ can compute approximations of analytic functions whose power series have $\mathbf{TC}^0$-computable coefficients

Question: Can VTC^0 prove their basic properties?

There's a plethora of such functions $\implies$ let's start small:

Elementary analytic functions (real and complex)

- exp, log
- trigonometric: sin, cos, tan, cot, sec, csc
- inverse trig.: arcsin, arccos, arctan, arccot, arcsec, arccsc
- hyperbolic: sinh, cosh, tanh, coth, sech, csch
- inverse hyp.: arsinh, arcosh, artanh, arcoth, arsech, arcsch

All definable in terms of complex exp and log

VTC^0 setup

Working with rational approximations only is quite tiresome

$\mathfrak{M} \vDash VTC^0 \rightsquigarrow$ DOR $\mathbf{Z}^{\mathfrak{M}} \rightsquigarrow$ fraction field $\mathbf{Q}^{\mathfrak{M}}$
$\rightsquigarrow$ completion $\mathbf{R}^{\mathfrak{M}} \rightsquigarrow$ alg. closure $\mathbf{C}^{\mathfrak{M}} = \mathbf{R}^{\mathfrak{M}}(i)$

Treat the functions as $f \colon \mathbf{C}^{\mathfrak{M}} \to \mathbf{C}^{\mathfrak{M}}$ (or on a subset)

This simplifies development, but approximations still needed:

- translate results back to the language of VTC^0
- use the functions in induction arguments, ...

Further notation: unary integers embed as $\mathbf{L}^{\mathfrak{M}} \subseteq \mathbf{Z}^{\mathfrak{M}}$

$\mathbf{C}^{\mathfrak{M}}_{\mathbf{L}} = \{z \in \mathbf{C}^{\mathfrak{M}} : \exists n \in \mathbf{L}^{\mathfrak{M}}\, |z| \le n\}$, $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} = \mathbf{R}^{\mathfrak{M}} \cap \mathbf{C}^{\mathfrak{M}}_{\mathbf{L}}$, ...

Main results

We can define $\pi \in \mathbf{R}^{\mathfrak{M}}$,

$$\begin{aligned} \exp\colon \mathbf{R}_{\mathbf{L}}^{\mathfrak{M}} + i\mathbf{R}^{\mathfrak{M}} &\to \mathbf{C}_{\neq 0}^{\mathfrak{M}}, \\ \log\colon \mathbf{C}_{\neq 0}^{\mathfrak{M}} &\to \mathbf{R}_{\mathbf{L}}^{\mathfrak{M}} + i(-\pi, \pi] \end{aligned}$$

such that

- $\exp(z_0 + z_1) = \exp z_0 \exp z_1$
- exp is $2\pi i$-periodic
- $\exp \log z = z$
- $\log \exp z = z$ for $z \in \mathbf{R}_{\mathbf{L}}^{\mathfrak{M}} + i(-\pi, \pi]$
- $\exp \restriction \mathbf{R}_{\mathbf{L}}^{\mathfrak{M}}$ increasing bijection $\mathbf{R}_{\mathbf{L}}^{\mathfrak{M}} \to \mathbf{R}_{>0}^{\mathfrak{M}}$, convex
- for small z: $\exp z = 1 + z + O(z^2)$, $\log(1 + z) = z + O(z^2)$

Construction of exp

Mostly straightforward:

- define $\exp\colon \mathbf{Q}^{\mathfrak{M}}_{\mathbf{L}}(i) \to \mathbf{C}^{\mathfrak{M}}$ as $\lim_{n\to\infty} \sum_{j<n} \frac{z^j}{j!}$
- extend to $\mathbf{C}^{\mathfrak{M}}_{\mathbf{L}}$ using (local) uniform continuity
- show $\exp(z_0 + z_1) = \exp z_0 \exp z_1$ in the usual way

But we can finish only after proving $\exp \log z = z$:

- $\pi := \operatorname{Im} \log(-1)$ satisfies $\exp(2\pi i) = 1$
  $\implies$ exp $2\pi i$-periodic
  $\implies$ extend exp to $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i\mathbf{R}^{\mathfrak{M}}$
- can further extend it to $\{z \in \mathbf{C}^{\mathfrak{M}} : \exists n \in \mathbf{L}^{\mathfrak{M}}\ \operatorname{Re} z \le n\}$ by putting $\exp z = 0$ when $\operatorname{Re} z < -\mathbf{L}^{\mathfrak{M}}$

Construction of $\log$

A lot of work:

- define $\log$ for $|z-1| <^* 1$ using $\lim_{n\to\infty} -\sum_{0<j\le n} \frac{(1-z)^j}{j}$
- show $\log(z_0z_1) = \log z_0 + \log z_1$ for z_j close to 1 by messy calculation
- extend $\log$ to $\mathbf{R}^{\mathfrak{M}}_{>0}$ using $2^n\colon \mathbf{L}^{\mathfrak{M}} \to \mathbf{Z}^{\mathfrak{M}}$
- extend $\log$ to an angular sector by combining the two
- develop $\sqrt{z}$
- extend $\log$ to $\mathbf{C}^{\mathfrak{M}}_{\ne 0}$ using $8\log\sqrt[8]{z}$
- $\log(z_0z_1) = \log z_0 + \log z_1$ when $\operatorname{Re} z_j > 0$
- $\log\exp(z_0+z_1) = \log\exp z_0 + \log\exp z_1$ when $|\operatorname{Im} z_j| < 1$
  $\Longrightarrow$ $\log\exp z = z$ when $|\operatorname{Im} z| < 1$
  $\Longrightarrow$ $\exp\log z = z$ using injectivity of log

Applications

Define

- $z^w = \exp(w \log z)$, $\sqrt[n]{z} = z^{1/n}$
- $\prod_{j<n} z_j$ for a sequence of $z_j \in \mathbf{Q}^{\mathfrak{M}}(i)$ coded in $\mathfrak{M}$
  - wlog $z_j \in \mathbf{Z}^{\mathfrak{M}}[i] \implies$ result also in $\mathbf{Z}^{\mathfrak{M}}[i]$
  - round appx. of $\exp(\sum_{j<n}$ appx. of $\log z_j)$
- trigonometric, inverse trigonometric, hyperbolic, inverse hyperbolic functions
- Q: Can VTC^0 prove π is irrational?

Model-theoretic consequence:

- Every countable model of VTC^0 is an exponential integer part of a real-closed exponential field (even though exp is not total on $\mathbf{R}^{\mathfrak{M}}$!)

Exponential integer parts

$\langle R, +, \cdot, < \rangle$ ordered field, $D \subseteq R$ subring:

- R real-closed: $R \equiv \mathbb{R}$ (odd-degree poly have roots, $\forall x > 0\, \exists \sqrt{x}$)
- $\langle R, \exp \rangle$ exponential field if $\exp \colon \langle R, +, < \rangle \simeq \langle R_{>0}, \cdot, < \rangle$
- D integer part (IP): discrete, $\forall x \in R\, \exists u \in D\, |x - u| < 1$
- [Res'93] exponential IP: $D_{>0}$ closed under exp
  ($\exp(1) = 2$, $\exp(n) > n$)

NB: $\exp \restriction D_{>0}$ may be different from the usual 2^n function

Motivation:

- [Shep'64] $\mathfrak{M} \vDash \mathit{IOpen} \iff \mathfrak{M}$ is an IP of a RCF
- What models are EIP of RCEF? Do they satisfy some nontrivial consequences of totality of exponentiation?

Models of VTC^0 as EIP

$\mathfrak{M} \models VTC^0 \implies$ IP of RCF $\mathbf{R}^{\mathfrak{M}}$

Catch: our exp or 2^x is $\langle \mathbf{R}^{\mathfrak{M}}_{\mathbf{L}}, +, < \rangle \simeq \langle \mathbf{R}^{\mathfrak{M}}_{>0}, \cdot, < \rangle$

Solution:

- $\langle \mathbf{Q}^{\mathfrak{M}}, \mathbf{Z}^{\mathfrak{M}}, \mathbf{L}^{\mathfrak{M}}, +, < \rangle$ is recursively saturated
  - quantifier elimination for $\mathrm{Th}(\mathbf{Q}^{\mathfrak{M}}, \mathbf{Z}^{\mathfrak{M}}, \mathbf{L}^{\mathfrak{M}}, +, <)$
- $\mathfrak{M}$ countable $\implies \langle \mathbf{Q}^{\mathfrak{M}}, \mathbf{N}^{\mathfrak{M}}, +, < \rangle \simeq \langle \mathbf{Q}^{\mathfrak{M}}_{\mathbf{L}}, \mathbf{L}^{\mathfrak{M}}, +, < \rangle$
- continuous extension $\langle \mathbf{R}^{\mathfrak{M}}, \mathbf{N}^{\mathfrak{M}}, +, < \rangle \simeq \langle \mathbf{R}^{\mathfrak{M}}_{\mathbf{L}}, \mathbf{L}^{\mathfrak{M}}, +, < \rangle$
- compose with $2^x \Rightarrow \langle \mathbf{R}^{\mathfrak{M}}, \mathbf{N}^{\mathfrak{M}}, +, < \rangle \simeq \langle \mathbf{R}^{\mathfrak{M}}_{>0}, P_2^{\mathfrak{M}}, \cdot, < \rangle$
  $P_2^{\mathfrak{M}} = \{x \in \mathbf{N}^{\mathfrak{M}} : x \text{ is a power of } 2\}$

References

- A. Atserias: Improved bounds on the Weak Pigeonhole Principle and infinitely many primes from weaker axioms, Theoret. Comput. Sci. 295 (2003), 27–39
- P. Beame, S. Cook, H. Hoover: Log depth circuits for division and related problems, SIAM J. Comp. 15 (1986), 994–1003
- A. Chiu, G. Davida, B. Litow: Division in logspace-uniform $\mathbf{NC}^1$, RAIRO – Theoret. Inf. Appl. 35 (2001), 259–275
- S. Cook, P. Nguyen: Logical foundations of proof complexity, Cambridge Univ. Press, 2010
- 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

References (cont'd)

- E. Jeřábek: Iterated multiplication in VTC^0, Arch. Math. Logic (2022), https://doi.org/10.1007/s00153-021-00810-6
- E. Jeřábek: Elementary analytic functions in VTC^0, 2022, 55pp., arXiv:2206.12164 [cs.CC]
- E. Jeřábek: Models of VTC^0 as exponential integer parts, ?
- S.-G. Mantzivis: Circuits in bounded arithmetic part I, Ann. Math. Artif. Intel. 6 (1991), 127–156
- P. Nguyen, S. Cook: Theories for TC^0 and other small complexity classes, Log. Methods Comput. Sci. 2 (2006), art. 3
- 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