Elementary analytic functions in VTC^0

Emil Jeřábek

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

Czech Gathering of Logicians
June 2022, Prague

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

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

2. Iterated multiplication and division

3. Induction in VTC^0

4. 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
- [J'15] Open induction in $\langle +, \cdot, < \rangle$ (*IOpen*),
  (translation of) Σ^b_0-minimization in Buss's language
- [J' ??] Elementary analytic functions:
  exp, log, sin, arcsin, sinh, arsinh, . . .

Iterated multiplication and division

History

[BCH'86]

- $\prod_{i<n} X_i$, $\lfloor Y/X \rfloor$, X^n are $\mathbf{TC}^0$-reducible to each other
- they are in **P**-uniform $\mathbf{TC}^0$
- compute the product in Chinese remainder representation:

$$\mathrm{CRR}_{\vec{m}}(X) = \langle X \bmod m_i : i < k \rangle$$

  where $\vec{m} = \langle m_i : i < k \rangle$ small primes
- (NB: predates definition of $\mathbf{TC}^0$)

Improved CRR reconstruction procedures $\implies$

- [CDL'01]: logspace-uniform $\mathbf{TC}^0$ (hence **L**)
- [HAB'02]: dlogtime-uniform $\mathbf{TC}^0$

Formalization in VTC^0

Raised as a problem by Atserias [Ats'03,NC'06]

Obstacles:

- complex structure with interdependent parts
- analysis elementary, but chicken-and-egg problems: uses iterated products and divisions all over the place

Results [J'22]:

- VTC^0 proves $IMUL$ and DIV
- $I\Delta_0 + WPHP(\Delta_0)$ has a well-behaved Δ_0 definition of $a^r \bmod m$

Induction in VTC^0

1. $\mathbf{TC}^0$ and VTC^0
2. Iterated multiplication and division
3. **Induction in VTC^0**
4. Elementary analytic functions

Open induction

Question: Can VTC^0 prove some amount of induction for binary numbers?

The weakest nontrivial fragment of induction: *IOpen*

- induction for quantifier-free formulas in language $\langle +, \cdot, < \rangle$
- [Shep'64] $\mathfrak{M} \vDash \mathit{IOpen} \iff$ $\mathfrak{M}$ is an integer part of a real-closed field

VTC^0-provable $\forall\exists\Sigma_0^B$ statements witnessed by $\mathbf{TC}^0$ functions $\Longrightarrow$ the following are equivalent:

- $VTC^0 \vdash \mathit{IOpen}$
- for every constant d, VTC^0 can formalize a $\mathbf{TC}^0$ root approximation algorithm for degree-d polynomials

Results [J'15]

VTC^0 does prove $IOpen$:

- Largange inversion formula $\implies$ approximation of roots of polynomials with "small" constant coefficient
- model-theoretic argument using Shepherdson's criterion
  - $\mathfrak{M} \rightsquigarrow$ DOR $\mathbf{Z}^{\mathfrak{M}} \rightsquigarrow$ fraction field $\mathbf{Q}^{\mathfrak{M}} \rightsquigarrow$ completion $\mathbf{R}^{\mathfrak{M}}$
  - $\mathfrak{M} \vDash DIV \implies \mathbf{Z}^{\mathfrak{M}}$ integer part of $\mathbf{Q}^{\mathfrak{M}}$ and $\mathbf{R}^{\mathfrak{M}}$
  - LIF $\implies \mathbf{R}^{\mathfrak{M}}$ henselian $\implies \mathbf{R}^{\mathfrak{M}}$ real-closed

Extend the argument using ideas of [Man'91]:

- VTC^0 proves induction and minimization for translations of Σ^b_0 formulas in Buss's language

Elementary analytic functions

1. TC^0 and VTC^0
2. Iterated multiplication and division
3. Induction in VTC^0
4. **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

Recall: $\mathfrak{M} \vDash VTC^0 \leadsto$ DOR $\mathbf{Z}^{\mathfrak{M}} \leadsto$ fraction field $\mathbf{Q}^{\mathfrak{M}}$
$\leadsto$ completion $\mathbf{R}^{\mathfrak{M}} \leadsto \mathbf{C}^{\mathfrak{M}} = \mathbf{R}^{\mathfrak{M}}(i)$

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

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

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

Outline of the construction

- Define exp: $\mathbf{C}^{\mathfrak{M}}_{\mathbf{L}} \to \mathbf{C}^{\mathfrak{M}}$ using $\sum_n \frac{z^n}{n!}$
  show $\exp(z_0 + z_1) = \exp z_0 \exp z_1$
- Define log on a nbh of 1 using $-\sum_n \frac{(1-z)^n}{n}$
  show $\log(z_0 z_1) = \log z_0 + \log z_1$ for z_j close enough to 1
- Extend log
  - to $\mathbf{R}^{\mathfrak{M}}_{>0}$ using $2^n \colon \mathbf{L}^{\mathfrak{M}} \to \mathbf{Z}^{\mathfrak{M}}$
  - to an angular sector by combining the two
  - to $\mathbf{C}^{\mathfrak{M}}_{\neq 0}$ using $8 \log \sqrt[8]{z}$
- $\log\exp(z_0 + z_1) = \log\exp z_0 + \log\exp z_1$ when $|\mathrm{Im}\, z_j|$ small
  $\implies$ $\log\exp z = z$ when $|\mathrm{Im}\, z|$ small
  $\implies$ $\exp\log z = z$ using injectivity of log
- exp is $2\pi i$-periodic for $\pi := \mathrm{Im}\log(-1)$
  $\implies$ extend exp to $\mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i\mathbf{R}^{\mathfrak{M}}$

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 $\mathfrak{M}$
- trigonometric, inverse trigonometric, hyperbolic, inverse hyperbolic functions

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 $\mathbf{R}^{\mathfrak{M}}$!)

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

References (cont'd)

- 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 (2022), `https://doi.org/10.1007/s00153-021-00810-6`
- E. Jeřábek: Elementary analytic functions in VTC^0, in preparation
- 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. Shepherdson: A nonstandard model for a free variable fragment of number theory, Bull. Acad. Polon. Sci. 12 (1964), 79–86