Mathematics in VTC^0

Emil Jeřábek

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

Journées sur les Arithmétiques Faibles 44

Institute of Mathematics, Prague, September 2025

Outline

1. **$\mathbf{TC}^0$ and VTC^0**
2. **Sums**
3. **Products**
4. **Polynomial roots**
5. **Analytic functions**

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

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?

Correspondence to propositional proof systems P: (not in this talk)

- P operates with "C-formulas"
- universal theorems of T uniformly translate to short P-proofs

This talk: $C = \mathbf{TC}^0$, $T = \mathrm{VTC}^0$ ($P = \mathbf{TC}^0$-Frege)

Some small complexity classes

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

- $\mathbf{AC}^0$: DLOGTIME-uniform constant-depth poly-size formulas with unbounded fan-in $\wedge, \vee, \neg$ gates
  $=$ **FO**-definable
  $=$ log time, $O(1)$ alternations on an alternating TM
- $\mathbf{AC}^0[m]$: $+$ MOD_m gates (constant m)
- $\mathbf{TC}^0$: $+$ Majority or threshold gates
- $\mathbf{NC}^1$: uniform poly-size formulas $=$ alternating log time
- $\mathbf{L}$: logarithmic space on a deterministic TM
- $\mathbf{NL}$: logarithmic space on a nondeterministic TM
- $\mathbf{P}$: polynomial time on a deterministic TM

The class $\mathbf{TC}^0$

$\mathbf{TC}^0$ = DLOGTIME-uniform $O(1)$-depth $n^{O(1)}$-size
unbounded fan-in formulas 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

$\mathbf{TC}^0$-functions ($\mathbf{FTC^0}$): $\mathbf{TC}^0$ bit-graph, polynomially bounded

= Constable's $\mathcal{K}$: closure of $+, -, \times, /$ under superposition
and polynomially bounded $\sum, \prod$ [HAB'02]
= closure of $+, -, \times, /, \#, \wedge$ under superposition [Vol'07]

The power of $\mathbf{TC}^0$

For integers given in binary:

- $+$, $-$, $\leq$ 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 $\prod_{i<n} X_i$ [BCH'86,CDL'01,HAB'02]
- the corresponding operations on $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\alpha)$, ...
- arithmetic on polynomials: $\sum$, $\prod$, composition, interpolation
- approximate functions given by nice power series:
  - sin, arctan, (bounded) exp, log, $\sqrt[k]{X}$, ...
- sorting, tree contraction/balancing, ...

Why TC^0?

Very weak/efficient . . .

- no sequential computation

. . . yet surprisingly powerful !

- computation with polynomials, power series, etc. (previous slide)
- no unconditional separation from polynomial hierarchy

Relevance for arithmetic:

The complexity class of basic integer arithmetic operations

One-sorted bounded arithmetic

- language $0, 1, +, \cdot, \le, \lfloor x/2 \rfloor, |x|, \#$
- Σ^b_0 formulas: sharply bounded q'fiers $\exists x \le |t|$, $\forall x \le |t|$
- $\hat\Sigma^b_i$ formulas: i alternating blocks of bounded quantifiers (first block $\exists$) followed by a Σ^b_0 formula
- $T^i_2 = \mathrm{BASIC} + \hat\Sigma^b_i\text{-IND}$, $S^i_2 = \mathrm{BASIC} + \hat\Sigma^b_i\text{-LIND}$
- $T_2 = \bigcup_i T^i_2 = \bigcup_i S^i_2 \cong I\Delta_0 + \Omega_1$

Johannsen and Pollett's theories for $\mathbf{TC}^0$:

- language with $\dot-$, $\lfloor x/2^y \rfloor$
- Δ^b_1-CR: open LIND, Δ^b_1 bit-comprehension rule [JP'00]
- C^0_2: $+ \mathrm{BB}\Sigma^b_0$ [JP'98]
- $C^0_2[div]$: language incl. $\lfloor x/y \rfloor$ [Joh'99]

Two-sorted bounded arithmetic

- unary (auxiliary) integers with $0, 1, +, \cdot, \leq$
- finite sets = binary integers = binary strings
  $x \in X$, $|X| = \sup\{x + 1 : x \in X\}$
- bounded quantifiers: $\exists x \leq t$, $\forall x \leq t$, $\exists X \leq t$, $\forall X \leq t$
  where $X \leq t$ is short for $|X| \leq t$
- Σ^B_0 formulas: bounded FO, no SO quantifiers
- Σ^B_i formulas: i alternating blocks of bounded quantifiers (first block $\exists$) followed by a Σ^B_0 formula
- $\mathrm{V}^i = \text{2-BASIC} + \Sigma^B_i\text{-COMP}$ (implies Σ^B_i-IND)

Theory VTC^0 corresponding to $\mathbf{TC}^0$: [NC'06,CN'10]

- V^0 + every set X has a counting function
  $\{\langle i, \mathrm{card}(X \cap [0, i))\rangle : i \leq |X|\}$

RSUV translation

two-sorted arithmetic	one-sorted arithmetic
sets	numbers
numbers	logarithmic numbers
bounded SO quantifiers	bounded quantifiers
bounded FO quantifiers	sharply bounded quantifiers
Σ^B_i	$\hat{\Sigma}^b_i$
V^i	S^i_2
TV^i	T^i_2
VTC^0	Δ^b_1-CR
$\mathrm{VTC}^0 + \Sigma^B_0$-AC	C^0_2
($\mathrm{VTC}^0 + \mathrm{IMUL} + \Sigma^B_0$-AC	$\mathrm{C}^0_2[div]$)

$$(i \geq 1)$$

The power of VTC^0

Correspondence of VTC^0 to $\mathbf{TC}^0$:

- provably total computable ($\exists\Sigma^B_0$) functions $=$ $\mathbf{TC}^0$ functions
- proves $\mathbf{TC}^0$ induction, comprehension, minimization, ...

More formally [CN'10]:

- VTC^0 has a universal extension $\overline{\mathrm{VTC}^0}$ in a language $\mathcal{L}_{\overline{\mathrm{VTC}^0}}$
  - $\mathcal{L}_{\mathrm{V}^0}$, $\mathrm{card}(X)$, bounded comprehension and minimization functions for $\Sigma^B_0(\mathcal{L}_{\overline{\mathrm{VTC}^0}})$ formulas
- $\mathcal{L}_{\overline{\mathrm{VTC}^0}}$-func. Δ^B_1-bit-definable in VTC^0 $\implies$ conservative
- $\mathcal{L}_{\overline{\mathrm{VTC}^0}}$-functions in $\mathbb{N} = \mathbf{TC}^0$-functions
- witnessing/Herbrand theorem: $\forall\exists\Sigma^B_0(\mathcal{L}_{\overline{\mathrm{VTC}^0}})$ theorems of $\overline{\mathrm{VTC}^0}$ witnessed by $\mathcal{L}_{\overline{\mathrm{VTC}^0}}$ functions

Sums

Binary $\leq, +, -$

$\leq, +, -$ are in **AC^0** $\implies$ Σ_0^B-definable:

$$X < Y \iff \exists i \in Y \, (i \notin X \land \forall j \in X \, (i < j \to j \in Y))$$

$$X \leq Y \iff \forall i \in X \, (\forall j \in Y \, (i < j \to j \in X) \to i \in Y)$$

$$X + Y = \{i : i \in X \oplus i \in Y \oplus \mathrm{carry}(X, Y, i)\}$$

$$\mathrm{carry}(X, Y, i) \iff \exists j < i \, (j \in X \land j \in Y \land \forall k < i \, (j < k \to k \in Y \lor k \in Y))$$

Straightforward formalization $\implies$

Proposition: V^0 proves that binary natural numbers with $+, \leq$ form the nonnegative part of a discretely ordered abelian group

Introduce binary integers (e.g., using a sign bit)

Coding of sequences

Unary pairing function: e.g., $\langle x, y\rangle := (x+y)^2 + x$

Sequences of binary numbers:
$\langle X_i : i < n\rangle$ coded by $\{\langle i, u\rangle : u \in X_i\}$

I.O.W.: the *i*th element of the sequence coded by X is
$X^{[i]} := \{u : \langle i, u\rangle \in X\}$

Sequences of unary numbers:
$\langle x_i : i < n\rangle$ coded by $\{\langle i, u\rangle : u < x_i\}$

$X^{(i)} := \left|X^{[i]}\right|$

Many other possibilities
[CN'10]: $(X)^i := \min\left(X^{[i]} \cup \{|X|\}\right)$

Iterated addition

Goal: $\mathbf{TC}^0$-function $\quad n, X = \langle X_i : i < n \rangle \longmapsto \sum_{i<n} X_i \quad$ s.t.

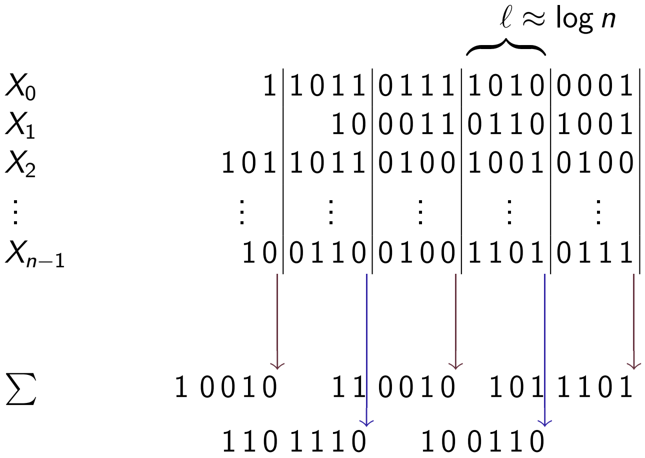
$$\mathrm{VTC}^0 \vdash \quad \sum_{i<0} X_i = 0, \quad \sum_{i<n+1} X_i = \sum_{i<n} X_i + X_n$$

Easy cases:

0–1 sequences $\langle x_i : i < n \rangle$:
represent by $X = \{i < n : x_i = 1\} \implies \sum_{i<n} x_i := \mathrm{card}(X)$

Unary sequences $\langle x_i : i < n \rangle$:
represent by $X = \{\langle i, n \rangle : n < x_i\} \implies \sum_{i<n} x_i := \mathrm{card}(X)$

$\sum$ of binary numbers



Straightforward to formalize in VTC^0 [CN'10]

Products

Binary multiplication

Schoolbook multiplication reduces to iterated addition:

$$Y = \sum_{i \in Y} 2^i \implies X \cdot Y := \sum_{i \in Y} 2^i X$$

$$\text{where } 2^i X = \{i + j : j \in X\}$$

Proposition:

VTC^0 proves that binary natural numbers with $0, 1, +, \cdot, \leq$ form the nonnegative part of a discretely ordered ring (PA^-)

Division and iterated multiplication

[BCH'86,CDL'01,HAB'02] Integer division with remainder and iterated multiplication are $\mathbf{TC}^0$-computable

Question: Can VTC^0 prove the existence of $\lfloor X/Y \rfloor$ and $\prod_{i<n} X_i$ satisfying the defining axioms

$$Y > 0 \to Y \cdot \lfloor X/Y \rfloor \le X < Y \cdot \big(\lfloor X/Y \rfloor + 1 \big) \qquad \text{(DIV)}$$

$$\prod_{i<0} X_i = 1, \qquad \prod_{i<n+1} X_i = \prod_{i<n} X_i \cdot X_n \ ? \qquad \text{(IMUL)}$$

NB: Reducible to each other

$$n \ge |X|,\ m = |Y| \implies \lfloor X/Y \rfloor = \lfloor 2^{-mn} Z X \rfloor \text{ where}$$

$$Z := \sum_{i<n} (2^m - Y)^i 2^{m(n-1-i)} = \frac{2^{mn} - (2^m - Y)^n}{Y} \approx \frac{2^{mn}}{Y}$$

Structure of the [HAB'02] algorithm

(1) $\prod_{u<t} X_u$ is in $\mathbf{TC}^0[\mathrm{pow}]$

- pick a sufficiently long list of small primes $\vec{m}$
- convert each X_u to Chinese remainder representation $\mathsf{CRR}_{\vec{m}}(X_u) = \langle X_u \bmod m_i : i < k\rangle$
- multiply the residues modulo each m_i
- hard part: reconstruct the result from $\mathsf{CRR}_{\vec{m}}$ to binary

(2) $\prod_{u<t} X_u$ is in $\mathbf{AC}^0$ if $\sum_{u<t} |X_u| = (\log n)^{O(1)}$

- scale **(1)** down

(3) pow is in $\mathbf{AC}^0$

- express exponents in $\mathsf{CRR}_{\vec{d}}$

pow: $a^r \bmod m$ $\qquad$ (a, r unary, m unary prime)

Structure of the [HAB'02] algorithm

(0) imul is in $\mathbf{TC}^0[\mathrm{pow}]$

- sum of discrete logarithms modulo m

(1) $\prod_{u<t} X_u$ is in $\mathbf{TC}^0[\mathrm{imul}]$

- pick a sufficiently long list of small primes $\vec{m}$
- convert each X_u to $\mathrm{CRR}_{\vec{m}}$
- multiply the residues modulo each m_i
- hard part: reconstruct the result from $\mathrm{CRR}_{\vec{m}}$ to binary

(2) $\prod_{u<t} X_u$ is in $\mathbf{AC}^0$ if $\sum_{u<t} |X_u| = (\log n)^{O(1)}$

- scale **(1)** down

(3) pow is in $\mathbf{AC}^0$

- express exponents in $\mathrm{CRR}_{\vec{d}}$

imul: $\prod_{i<n} a_i \bmod m$ $\quad$ (n, a_i unary, m unary prime)

Obstacles to formalization

Complex structure with interdependent parts

Which came first: the chicken or the egg?

- $\mathrm{CRR}_{\vec{m}}$ reconstruction:
  - analysis heavily uses iterated products and divisions: $\prod_{i<k} m_i, \dots$
  - need $\mathrm{CRR}_{\vec{m}}$ reconstruction to define iterated products and divisions in the first place
- computation of pow:
  - analysis of the pow algorithm heavily uses pow
  - relies on Fermat's little theorem
- cyclicity of $(\mathbb{Z}/p\mathbb{Z})^\times$:
  - needed to compute imul in $\mathbf{TC}^0[\mathrm{pow}]$
  - notoriously difficult in bounded arithmetic
  - provable in $\mathrm{VTC}^0 + \mathrm{IMUL}$, but what good is that?

Formalization of IMUL and DIV

Theorem [J'22]
VTC^0 proves IMUL, and consequently DIV

$\mathrm{C}^0_2[div] \equiv \mathrm{C}^0_2$

Side effect:

Theorem [J'22]
$\exists\ \Delta_0$ definition of $a^r \bmod m$ s.t. $I\Delta_0 + \mathrm{WPHP}(\Delta_0)$ proves

$$a^0 \equiv 1 \pmod{m}, \qquad a^{r+1} \equiv a^r a \pmod{m}$$

Outline of the argument

- preparatory results
  - $\mathsf{VTC}^0 \vdash$ there are enough primes
  - $\mathsf{VTC}^0(\mathrm{pow})$ can do division $\lfloor X/m \rfloor$ by small primes

(1) $\mathsf{VTC}^0(\mathrm{imul}) \vdash \mathsf{IMUL}$
  - hard part: CRR reconstruction
  - teach $\mathsf{VTC}^0(\mathrm{imul})$ to compute in CRR from scratch

(2) $\mathsf{V}^0 \vdash \mathsf{IMUL}\big[|w|^c\big]$
  - the polylogarithmic cut in V^0 is a model of VNL

(3) $\mathsf{V}^0 + \mathsf{WPHP} \vdash$ totality of pow
  - reorganize the [HAB'02] algorithm to avoid circularity

- can't do **(0)** directly!
  - structure theorem for finite abelian groups (partially)
  - each turn around the vicious circle
    $\mathsf{IMUL} \to$ cyclicity $\to \mathrm{imul} \to \mathsf{IMUL}$ makes progress
    $\Longrightarrow$ proof by induction

Polynomial roots

Open induction

So far: VTC^0 proves $\mathbb{Z}$ forms a discretely ordered ring (DOR) with Euclidean division

Question: Can VTC^0 prove nontrivial instances of induction over binary integers?

Simplest case:
Does VTC^0 prove (the RSUV translation of) open induction?

$\mathrm{IOpen} = \mathrm{PA}^- +$ induction for open (= quantifier-free) formulas

IOpen algebraized

Theorem [Shep'64]: For any DOR D, TFAE:

- $D \vDash$ IOpen
- D is an integer part of a real-closed field (RCF)
- $f \in D[X]$, $u < v \in D$, $f(u) \leq 0 < f(v)$
  $\implies \exists x \in D$ s.t. $u \leq x < v$ and $f(x) \leq 0 < f(x+1)$

Corollary: TFAE:

- VTC^0 proves IOpen
- VTC^0 can formalize $\mathbf{TC}^0$ root approximation algorithms (real or complex) for constant-degree polynomials

NB: Such $\mathbf{TC}^0$ algorithms exist [J'12] but heavily rely on complex analysis $\implies$ not suitable for direct formalization

- we'll use a mixed model-theoretic argument instead

Reals over models of VTC^0

$$\mathfrak{M} \vDash \mathrm{VTC}^0 \rightsquigarrow \text{DOR } \mathbf{Z}^{\mathfrak{M}}$$
$$\rightsquigarrow \text{fraction field } \mathbf{Q}^{\mathfrak{M}}$$
$$\rightsquigarrow \text{completion } \mathbf{R}^{\mathfrak{M}}$$
$$\rightsquigarrow \text{complex numbers } \mathbf{C}^{\mathfrak{M}} = \mathbf{R}^{\mathfrak{M}}(i)$$

Equivalent descriptions of $\mathbf{R}^{\mathfrak{M}}$ as a completion of $\mathbf{Q}^{\mathfrak{M}}$:

- topological completion (uniform space/topological field)
- ordered field (Scott) completion (Dedekind-like cuts)
- valued field completion (natural valuation induced by $\leq$)

Fact: K valued field with value group Γ and residue field $k \implies$

K is RCF $\iff$ Γ is divisible & k is RCF & K is henselian

Open induction in VTC^0

Theorem [J'15]: VTC^0 proves the RSUV translation of IOpen
Δ^b_1-CR and C^0_2 prove IOpen

- direct proof of a form of the Lagrange inversion formula
  - polynomials can be locally inverted by power series
  - $\implies$ compute roots of polynomials with small constant coefficient
- model-theoretic argument using valued fields
  - $\mathfrak{M} \vDash \mathrm{VTC}^0 \vdash \mathrm{DIV} \implies \mathbf{Z}^{\mathfrak{M}}$ integer part of $\mathbf{Q}^{\mathfrak{M}}$ and $\mathbf{R}^{\mathfrak{M}}$
  - $\mathbf{R}^{\mathfrak{M}}$ is henselian by the first part (LIF)
    value group divisible (easy)
    residue field is $\mathbb{R}$ if $\mathfrak{M}$ is ω-saturated (wlog)
  - $\implies$ $\mathbf{R}^{\mathfrak{M}}$ is RCF, $\mathfrak{M} \vDash$ IOpen by Shepherdson's criterion

In fact: $\mathfrak{M} \vDash \mathrm{VTC}^0 \implies \mathbf{R}^{\mathfrak{M}}$ is RCF and $\mathbf{C}^{\mathfrak{M}}$ is ACF
regardless of saturation

Sharply bounded minimization

Formalization a structural description of Σ^b_0 formulas [Man'91]
$\Longrightarrow$ considerable generalization:

Theorem [J'15]

- VTC^0 proves the RSUV-translations of Σ^b_0-IND ($= \mathrm{T}^0_2$) and Σ^b_0-MIN
- Δ^b_1-CR and C^0_2 prove Σ^b_0-IND, Σ^b_0-MIN

NB: this is for Buss's original language

- also works with $\dot{-}$, $2^{\min\{x,|y|\}}$, $\lfloor x/||y||\rfloor$, $\lfloor x/2^{||y||}\rfloor$ included
- with $\lfloor x/2^y\rfloor$, T^0_2 becomes PV_1 and Σ^b_0-MIN becomes T^1_2
  $\Longrightarrow$ likely much stronger than VTC^0

Analytic functions

TC^0 analytic functions

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

Question: Can VTC^0 prove their basic properties?

For a start: elementary analytic functions ($\mathbb{R}$ or $\mathbb{C}$)

- exp, log
- trigonometric, inverse trig., hyperbolic, inverse hyp.

(all definable in terms of complex exp and log)

Working with rational approximations only is quite tiresome

Recall: $\mathfrak{M} \vDash \mathrm{VTC}^0 \rightsquigarrow \mathbf{Z}^{\mathfrak{M}} \rightsquigarrow \mathbf{Q}^{\mathfrak{M}} \rightsquigarrow \mathbf{R}^{\mathfrak{M}} \rightsquigarrow \mathbf{C}^{\mathfrak{M}}$

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

Results on exp and log

[J'23a] We can define $\pi \in \mathbf{R}^{\mathfrak{M}}$, $\exp\colon \mathbf{R}^{\mathfrak{M}}_{\mathbf{L}} + i\mathbf{R}^{\mathfrak{M}} \to \mathbf{C}^{\mathfrak{M}}_{\neq 0}$,

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

- $\exp(z_0 + z_1) = \exp z_0 \exp z_1$
- $\exp$ 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: $\exp z = 1 + z + O(z^2)$, $\log(1 + z) = z + O(z^2)$

Notation: unary integers embed in binary as $\mathbf{L}^{\mathfrak{M}} \subseteq \mathbf{Z}^{\mathfrak{M}}$

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

Outline of the construction

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

Applications

[J'23a] 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

[J'23b] 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 $\mathbf{R}^{\mathfrak{M}}$!)

Limitations

The construction of $\mathbf{R}^{\mathfrak{M}}$, $\mathbf{C}^{\mathfrak{M}}$ is external to the theory

- cannot directly speak of reals, analytic functions, . . .
  $\Longrightarrow$ only expressible using rational approximations
  - also needed in induction arguments, . . .
- cannot quantify over reals, analytic functions, . . .
  $\Longrightarrow$ no general theory of analytic functions

Need a more robust set-up:

- version of VTC^0 where infinite sets, sequences, functions are bona fide objects
- develop basic complex analysis

NB: Theories for real analysis [F'94,FF'08,F'09,FFF'17]
— too strong in several respects

VTC^0 with infinite sets

VTC^0: 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'86] 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 $a = \lim_n 2^{-n}A[n]$
  $\implies$ 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: $\{a_n\}_{n\in\mathbf{L}} \mapsto \{\sum_{n<N} a_n\}_{N\in\mathbf{L}}, \{\prod_{n<N} a_n\}_{N\in\mathbf{L}}$
- $f(z) = \sum_n a_n z^n$ converges for $|z| <^* r$ if $a_n = O(r^{-n})$
  $x <^* y \iff x \le y(1 - m^{-1})$ for some $m \in \mathbf{L}$
- adapting [J'15,J'23a]: constant-degree polynomial roots, elementary analytic functions (exp, log, ...)

Operations on power series:

- derivatives and primitive functions $f^{(n)}(z)$, $n \in \mathbf{Z_L}$
- shift: $f(z) = \sum_n a_n(z-u)^n \mapsto f(z) \equiv \sum_n b_n(z-v)^n$
- $\sum_{n<N} f_n$, $\prod_{n<N} f_n$, $f(g(z))$
  - polynomials: evaluate at $\{e^{2\pi ij/m}\}_{j<m}$, interpolate (DFT)
  - power series: apply to partial sums

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 $\displaystyle\int_\gamma f(z)\,dz := \sum_{j<\tilde{\ell}} \big(F_{k_j}(\tilde{z}_j) - F_{k_j}(\tilde{z}_{j+1})\big)$ 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
- maximum modulus principle
- ...

Potential applications:

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

References (1/4)

- S. R. Buss: Bounded arithmetic, Bibliopolis, Naples, 1986
- 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
- R. Constable: Type two computational complexity, STOC, 1973, 108–121
- 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

References (2/4)

- F. Ferreira, G. Ferreira: The Riemann integral in weak systems of analysis, J. Univ. Computer Sci. 14 (2008), 908–937
- G. Ferreira: The counting hierarchy in binary notation, Portugaliae Mathematica 66 (2009), 81–94
- A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, G. Turán: Threshold circuits of bounded depth, J. Comp. System Sci. 46 (1993), 129–154
- 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: Root finding with threshold circuits, Theoret. Computer Sci. 462 (2012), 59–69
- 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

References (3/4)

- E. Jeřábek: Elementary analytic functions in VTC^0, Ann. Pure Appl. Logic 174 (2023), 103269
- E. Jeřábek: Models of VTC^0 as exponential integer parts, Math. Logic Quarterly 69 (2023), 244–260
- J. Johannsen, C. Pollett: On proofs about threshold circuits and counting hierarchies (extended abstract), LICS, 1998, 444–452
- J. Johannsen: Weak bounded arithmetic, the Diffie-Hellman problem, and Constable's class K, LICS, 1999, 268–274
- J. Johannsen, C. Pollett: On the Δ_1^b-bit-comprehension rule, Logic Colloquium '98 (Proceedings), ASL, 2000, 262–280
- S.-G. Mantzivis: Circuits in bounded arithmetic part I, Ann. Math. Artif. Intel. 6 (1991), 127–156
- P. Nguyen, S. Cook: Theories for $\mathbf{TC}^0$ and other small complexity classes, Log. Methods Comput. Sci. 2 (2006), art. 3

References (4/4)

- 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
- S. Volkov: An exponential expansion of the Skolem-elementary functions, and bounded superpositions of simple arithmetic functions, Mathematical Problems of Cybernetics vol. 16, 2007, 163–190 (Russian)
- S. Volkov: Generating some classes of recursive functions by superpositions of simple arithmetic functions, Dokl. Math. 76 (2007), 566–567
- D. Zambella: End extensions of models of linearly bounded arithmetic, Ann. Pure Appl. Logic 88 (1997), 263–277