Root finding in TC^0 and open induction

Emil Jeřábek

jerabek@math.cas.cz
http://math.cas.cz/~jerabek/

Institute of Mathematics of the Academy of Sciences, Prague

Overview

Correspondence of theories of arithmetic T and complexity classes C:

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

Feasible reasoning:

- Given a natural concept $P \in C$, what can we prove about P using only concepts from C?
- That is: what T proves about P?

Our P: elementary integer arithmetic operations $+, \cdot, \leq$

Small complexity classes

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

All circuit classes are assumed uniform.

- $\mathbf{AC}^0$: constant-depth poly-size unbounded fan-in circuits with $\wedge, \vee, \neg$ gates
  = $\mathbf{FO}$ = log time, $O(1)$ alternations on an alternating TM
- $\mathbf{ACC}^0$: + MOD_m gates, constant m
- $\mathbf{TC}^0$: + majority gates
- $\mathbf{NC}^1$: log-depth bounded fan-in circuits
  = poly-size formulas = alternating log time
- $\mathbf{L}$: log space on a deterministic TM

Complexity of arithmetic operations

For integers given in binary:

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

$\mathbf{TC}^0 = \mathbf{DLOGTIME}$-uniform $O(1)$-depth $n^{O(1)}$-size threshold circuits

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

$= \mathbf{FOM}$ (first-order logic with majority quantifiers)

The power of TC^0

TC^0 can do:

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

$\Rightarrow$ the right class for basic arithmetic operations

The theory VTC^0

The most common theory corresponding to $\mathbf{TC}^0$ is VTC^0:

- Zambella-style two-sorted bounded arithmetic
  - unary (auxiliary) integers $x, y, \dots$ with $0, 1, +, \cdot, \leq$
  - finite sets $X, Y, \dots$ = binary integers = binary strings
  - $x \in X$, $|X| = \sup\{x + 1 : x \in X\}$
- Noteworthy axioms:
  - Σ^B_0-comprehension ($\Sigma^B_0 =$ bounded, w/o SO q'fiers)
  - every set has a counting function
- Σ^1_1-definable functions are exactly $\mathbf{FTC}^0$
- Has induction, minimization, ... for $\mathbf{TC}^0$-predicates

Arithmetic in VTC^0

VTC^0

- can define $+, \cdot, \leq$ on binary integers
- proves integers form a discretely ordered ring (DOR)

Basic question:
What other properties of $+, \cdot, \leq$ are provable in VTC^0?

More formally:
Let I be the interpretation of DOR in VTC^0 by binary integers. What is the first-order theory

$$\{\varphi \in \mathrm{Form}_{+,\cdot,\leq} : VTC^0 \vdash \varphi^I\}$$

$VTC^0 + IMUL$

Annoying trouble: Unknown if VTC^0 can formalize the [HAB'02] algorithms for iterated multiplication and division

$$VTC^0 \overset{?}{\vdash} \forall X \forall Y > 0\, \exists Q \exists R < Y\, (X = Y \cdot Q + R)$$

$\Rightarrow$ Consider iterated multiplication as an additional axiom:

$(IMUL)$ $\forall X, n\, \exists Y\, \forall i \leq j < n\, \big(Y^{[\langle i,i\rangle]} = 1 \wedge Y^{[\langle i,j+1\rangle]} = Y^{[\langle i,j\rangle]} . X^{[j]}\big)$

Think $Y^{[\langle i,j\rangle]} = \prod_{k=i}^{j-1} X^{[k]}$

Note: $VTC^0 + IMUL$ also corresponds to $\mathbf{TC}^0$

Open induction

The weakest arithmetic theory with a nontrivial fragment of the induction schema:

$IOpen = DOR +$ induction for open formulas φ in $\langle +, \cdot, \leq \rangle$

$$\varphi(0) \wedge \forall x\,(\varphi(x) \to \varphi(x+1)) \to \forall x \geq 0\,\varphi(x)$$

[Shep'64]

Main question: Does VTC^0 or $VTC^0 + IMUL$ prove $IOpen$ for binary integers?

N.B.: $IOpen$ is $\forall\exists$. Its universal fragment is included in the theory of $\mathbb{Z}$-rings ($DOR + \exists\lfloor x/n \rfloor$ for any standard $n > 0$), provable in VTC^0

$\Rightarrow$ we mainly care about witnesses to $\exists$ in axioms of $IOpen$

$IOpen$ algebraized

For a DOR M, the following are equivalent [Shep'64]:

- $M \vDash IOpen$
- M is an integer part of its real closure $R = \mathrm{rcl}(M)$
  - $R =$ the maximal ordered field algebraic over M
  - $\forall \alpha \in R \, \exists x \in M \, (x \leq \alpha < x + 1)$
- If $u < v \in M$ and $f \in M[x]$ is such that $f(u) \leq 0 < f(v)$, there is $u \leq x < v$ in M such that $f(x) \leq 0 < f(x+1)$

One can also reformulate these conditions in terms of the algebraic closure $\mathrm{acl}(M) = R(i)$

Open induction and root finding

Algebraic characterization of $IOpen$ and Σ^1_1-witnessing theorem for VTC^0 yield

Lemma: The following are equivalent.

- VTC^0 proves $IOpen$
- For any constant $d > 0$, there is a $\mathbf{TC}^0$ algorithm for approximation of (real or complex) roots of degree d polynomials (over $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{Q}(i)$) whose correctness is provable in VTC^0

The same holds also for $VTC^0 + IMUL$ and extensions by true universal axioms

TC^0 root finding

Root-finding algorithms

Goal: Given a polynomial f over $\mathbb{Q}(i)$ and t, compute t-bit approximations to complex roots of f

- Iterative approaches
  - Find an initial approximation, and refine it iteratively
  - Newton, Laguerre, Brent, Durand–Kerner, ...
  - Eigenvalue algorithms: QR
- Divide and conquer
  - Find a contour splitting the set of roots, approximate coefficients of $f_1 f_2 = f$ by numerical integration
- Root finding is in $\mathbf{NC}$

New result

Theorem [J.]: For any constant d, there is a $\mathbf{TC}^0$ root-finding algorithm for degree-d polynomials

Corollary:

$$VTC^0 + \mathrm{Th}_{\forall\Sigma_0^B}(\mathbb{N}) \vdash IOpen$$

The algorithm uses tools from complex analysis:

Polynomials are locally invertible, the inverse is a holomorphic function $\Rightarrow$ locally expressible by a power series

Our algorithm in a nutshell

Given a constant-degree f, we do in TC^0:

- (Preprocessing: $\square$-free)
- Compute recursively roots of f'
- Use them to identify a poly-size set of sample points. For each sample point a, do in parallel:
  - Let g be a power series inverting f with centre $b = f(a)$
  - Output a partial sum of $g(0)$
- (Postprocessing: remove repeated roots)

Mathematical requirements

To make the algorithm work, we need:

- TC^0-computability of the coefficients of g
- Bounds on the coefficients and on the radius of g's image
  - Polynomially many terms of the series are sufficient for the desired accuracy
  - A particular root α is $g(0)$ if the sample point a is sufficiently close to α
    $\Rightarrow$ can devise a poly-size set of sample points

Lagrange inversion formula

Notation: $g(w) = \sum_n c_n (w-b)^n \;\Rightarrow\; [(w-b)^n]g(w) := c_n$

Lagrange inversion formula: If $f(0) = 0 \neq f'(0)$ and g is the inverse of f in a neighbourhood of 0 such that $g(0) = 0$, then $[w^n]g(w) = \frac{1}{n}[z^{-1}](f(z))^{-n}$.

An explicit version of LIF: If WLOG $f'(0) = [z]f(z) = 1$, then

$$[w^n]g(w) = \sum_{\sum_i (i-1)m_i = n-1} C_{m_2,\dots,m_d} \prod_{i=2}^{d} (-[z^i]f(z))^{m_i}$$

$$C_{m_2,\dots,m_d} = \frac{\left(\sum_{i=2}^{d} i m_i\right)!}{\left(\sum_{i=2}^{d}(i-1)m_i + 1\right)! \prod_{i=2}^{d} m_i!}$$

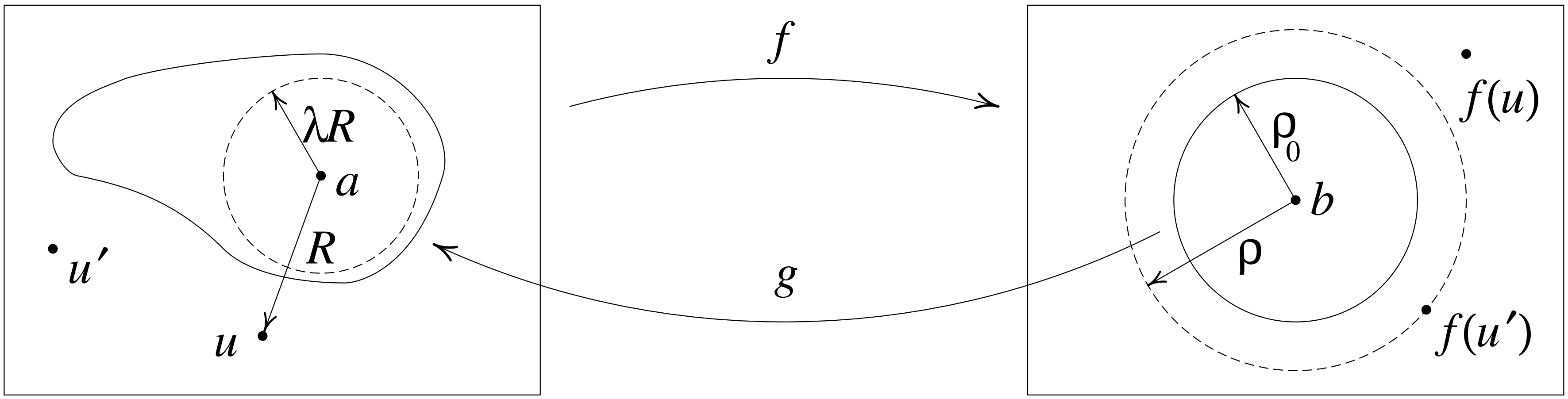
TC^0-computable, given n in unary and coef's of f in binary

Bounds

For any d there are constants μ, ν, λ such that:

If $f \in \mathbb{C}[z]$ has degree d, $f(a) = b$, g is f^{-1} around b s.t. $g(b) = a$, and $R > 0$ distance from a to the nearest root u of f':

- g has radius of convergence $\rho \geq \rho_0 = \nu R\,|f'(a)|$
- $g[B(b, \rho_0)] \supseteq B(a, \lambda R)$
- $|[(w-b)^n]g(w)| \leq \mu R/(n\rho_0^n)$



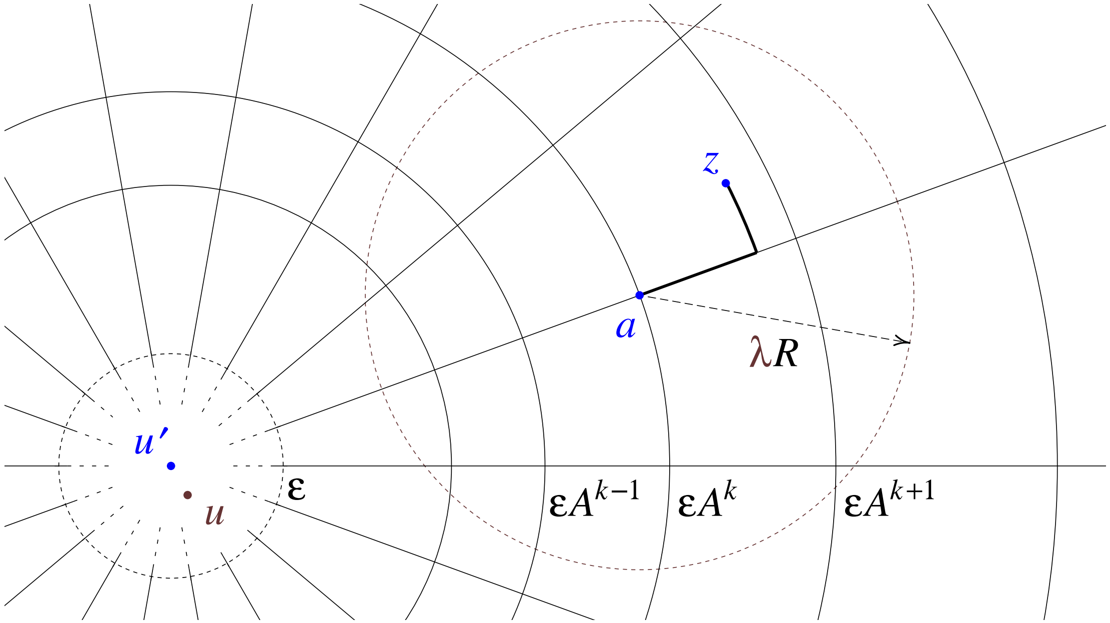
Sample points

For each root u of f' approximated by u', we take intersections of

- Circles around u' with geometrically increasing radius
- $O(1)$ lines through u'

Then: $\forall z \, \exists$ sample point a s.t. $|z-a| < \lambda|a-u|$

$\Rightarrow$ if g inverts f around $b = f(a)$ and $f(z) = 0$, then $g(0) = z$



Formalization in $VTC^0 + IMUL$?

Root finding and open induction

$\mathbf{TC}^0$ constant-degree root-finding algorithms imply

$$VTC^0 + \mathrm{Th}_{\forall\Sigma^B_0}(\mathbb{N}) \vdash IOpen$$

To bring it down to $VTC^0 \pm IMUL$, need to formalize the soundness of the algorithm in the theory

Main issues

The proof of soundness relies on

- Lagrange inversion formula
- Bounds on coefficients of the inverse series and its image

The original proof heavily uses complex-analytic tools (Cauchy integral formula, . . .) not available in bounded arithmetic

Lagrange inversion formula, revisited

Let $f(z) = \sum_{k=1}^{d} a_k z^k$, $a_1 = 1$, and consider $g(w) = \sum_{n=1}^{\infty} b_n w^n$,

$$b_n = \sum_{\sum_i (i-1)m_i = n-1} C_{m_2,\dots,m_d} \prod_{i=2}^{d} (-a_i)^{m_i}$$

$$C_{m_2,\dots,m_d} = \frac{\left(\sum_{i=2}^{d} i m_i\right)!}{\left(\sum_{i=2}^{d}(i-1)m_i + 1\right)! \prod_{i=2}^{d} m_i!}$$

LIF: $f(g(w)) = w$ as formal power series

LIF, continued

Corollary of LIF: If $|b_n| \le cr^{-n}$ and $g_N(w) := \sum_{n=1}^{N} b_n w^n$, then

$$|f(g_N(w)) - w| \le c' N^d \left(\frac{|w|}{r}\right)^N$$

for each $N > 1$ and $|w| \le r$

LIF, restated

Coefficients of $f(g(w))$: multivariate polynomials in $a_2, \dots, a_d$
Comparing their coefficients $\Rightarrow$ LIF amounts to the identity

$$C_m = \sum_{k=2}^{d} \sum_{m^1+\dots+m^k=m-\delta^k} C_{m^1} \cdots C_{m^k} \qquad (m \neq \vec{0})$$

Here, m denotes the sequence $\langle m_2, \dots, m_d \rangle$, similarly for $m^i = \langle m^i_2, \dots, m^i_d \rangle$

Addition coordinate-wise

$\delta^k = \langle \delta^k_2, \dots, \delta^k_d \rangle$ is Kronecker's delta

Combinatorial interpretation of LIF

$C_m = \#$ of unary terms with m_j occurrences of a single j-ary connective for each $j = 2, \dots, d$
$= \#$ of ordered rooted trees with m_j nodes of in-degree $j = 2, \dots, d$ and no other inner nodes

LIF $\approx$ a term is a variable or $f(t_1, \dots, t_k)$, where f is k-ary and t_j are terms

$\Rightarrow$ an easy bijective proof of LIF

But: based on counting of exponentially many objects
$\Rightarrow$ useless in VTC^0

Need something more down-to-earth

Inductive proof of LIF

By induction on $m_2 + \cdots + m_d$, we can prove simultaneously

$$C_m = \sum_{k=2}^{d} \sum_{m^1+\cdots+m^k = m-\delta^k} C_{m^1} \cdots C_{m^k} \qquad (m \neq \vec{0})$$

$$\Bigl(\sum_i i m_i + 1\Bigr) C_m = \sum_{m'+m''=m} \Bigl(\sum_i (i-1) m'_i + 1\Bigr) C_{m'} C_{m''}$$

$$\sum_{m^1+\cdots+m^k=m} C_{m^1} \cdots C_{m^k} = \frac{\bigl(\sum_i i m_i + k - 1\bigr)!\, k}{\bigl(\sum_i (i-1) m_i + k\bigr)! \prod_i m_i!} \qquad (k = 1, \dots, d)$$

by direct manipulations of sums and products

Theorem: $VTC^0 + IMUL$ proves LIF

Corollaries for root finding

Crude bound on coef's: $C_m \le d^{\sum_j j m_j}$ ($\because$ multinomial thm)

Suffices to finish two special cases:

- $\sqrt[d]{x}$ ($\because$ can first scale argument to be arbitrarily close to 1)
  Theorem: For any constant $d > 0$,
  $VTC^0 + IMUL \vdash \forall X \, \exists Y \, (Y^d \le X < (Y+1)^d)$
- Standard f ($\because$ local compactness of standard $\mathbb{R}$)
  Theorem (roughly): Every algebraic number α with a minimal polynomial f is computable by a TC^0 algorithm such that $VTC^0 + IMUL \vdash f(\alpha) = 0$

Open problem

Does $VTC^0 + IMUL$ prove $IOpen$?

Need: prove in $VTC^0 + IMUL$ a lower bound on the radius of image of $g = f^{-1}$ as a constant fraction of the distance R to the nearest root of f'.

(The crude bound gives $\Omega(1/\|f\|_\infty)$, independent of R.)

Thank you for attention!

References

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*, CUP, 2010.

W. Hesse, E. Allender, D. Mix 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*, arXiv:1112.3925 [cs.DS], 2011.

V. Pan, *Solving a polynomial equation: Some history and recent progress*, SIAM Review 39 (1997), 187–220.

W. Press, S. Teukolsky, W. Vetterling, B. Flannery, *Numerical recipes: The art of scientific computing*, 3rd ed., CUP, 2007.

J. Shepherdson, *A nonstandard model for a free variable fragment of number theory*, Bull. Acad. Polon. Sci. 12 (1964), 79–86.