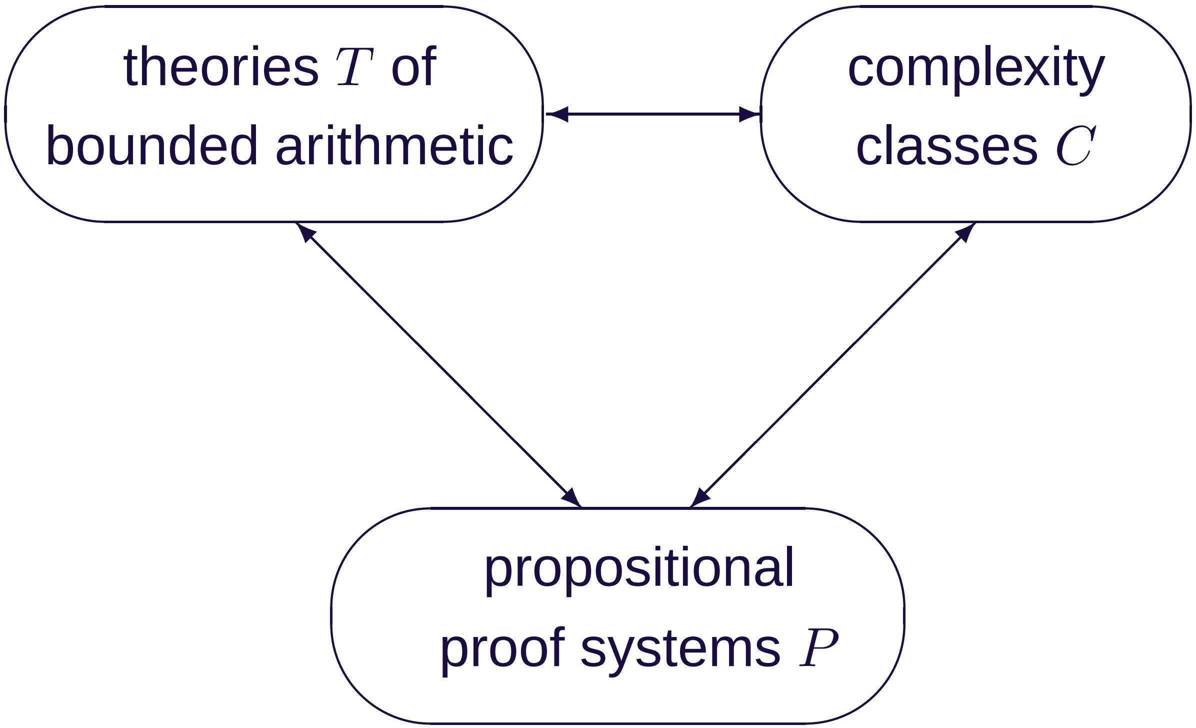
Open induction in a TC^0 arithmetic

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

Institute of Mathematics of the Academy of Sciences, Prague

Correspondence

The “big picture” in proof complexity:



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 do reasoning using C-predicates (comprehension, induction, ...)

Feasible reasoning:

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

This talk:
X = 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

The class TC^0

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

unbounded fan-in circuits with threshold gates

$= O(\log n)$ time, $O(1)$ thresholds

on a threshold Turing machine

$= \mathbf{FOM}$-definable on finite structures

representing strings

(first-order logic with majority quantifiers)

$\mathbf{TC}^0$ 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 Turing reductions)

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

- iterated addition $\sum_{i<n} x_i$
- integer division and iterated multiplication [HAB'02]
- the corresponding operations on $\mathbb{Q}$, $\mathbb{Q}(i)$
- 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

The most common theory corresponding to $\mathbf{TC}^0$ is 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 ($\Sigma^B_0 =$ 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

Binary 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 $+, \cdot, \leq$ for binary integers are provable in VTC^0?

In particular: Does it prove some nontrivial instances of induction?

$VTC^0 + IMUL$

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

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

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

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

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

Iterated multiplication and division

- $VTC^0 + IMUL$ corresponds to $\mathbf{TC}^0$, just like VTC^0
- $VTC^0 + IMUL \vdash DIV$
- We need $IMUL$ rather than DIV for technical reasons. A “reasonable theory”:
  - provably total computable functions closed under parallel repetition
  - closed under the Σ^B_0-choice rule

  $VTC^0 + IMUL$ is the smallest “reasonable theory” containing $VTC^0 + DIV$ (using [JP’98])
  - $VTC^0 \vdash DIV$ iff $VTC^0 \vdash IMUL$

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 prove $IOpen$ for binary integers?

Notes on $IOpen$

- $IOpen$ proves DIV
- $IOpen$ is $\forall\exists$-axiomatized
- Its universal fragment is included in the theory of $\mathbb{Z}$-rings
  - $DOR + \forall x\, \exists \lfloor x/n \rfloor$ for each standard $n > 0$ = DOR + Presburger arithmetic
  - provable in VTC^0

$\Longrightarrow$ we are mostly concerned about witnesses to $\exists$ in axioms of $IOpen$

Ordered fields

Ordered field = field with a compatible total order

Real-closed field = an OF R satisfying one of the following equivalent conditions:

- every positive $a \in R$ has a square root, and every $f \in R[x]$ of odd degree has a root
- R has no proper ordered algebraic extension
- $R(\sqrt{-1})$ is algebraically closed
- $R \equiv \mathbb{R}$

Every OF F has a unique real closure $\mathrm{rcl}(F)$
= real-closed algebraic ordered extension $R \supseteq F$

$IOpen$ algebraized

Integer part of an OF F = discretely ordered subring $D \subseteq F$ such that every $\alpha \in F$ is within distance 1 from a $z \in D$

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

- $D \vDash IOpen$
- $D \vDash LOpen$
- D is an integer part of a real-closed field $R \supseteq D$
- If $u < v \in D$ and $f \in D[x]$ is such that $f(u) \leq 0 < f(v)$, there is $u \leq z < v$ in D such that $f(z) \leq 0 < f(z+1)$

Witnessing for VTC^0

Witnessing theorem:
If $VTC^0 \pm IMUL \vdash \forall X \, \exists Y \, \varphi(X,Y)$, where φ is $\Sigma^1_1 (= \exists\Sigma^B_0)$
$\Longrightarrow$ $\exists$ a $\mathbf{TC}^0$ function F s.t. $VTC^0 \pm IMUL \vdash \forall X \, \varphi(X, F(X))$.

Corollary: The following are equivalent:

- $VTC^0 \pm IMUL$ proves $IOpen$
- For every constant $d > 0$, $VTC^0 \pm IMUL$ can formalize a $\mathbf{TC}^0$ (real or complex) root approximation algorithm for degree d polynomials

TC^0 root finding

Theorem [J'12]:

TC^0 root approximation algorithms exist for any constant d.

- works naturally for complex polynomials and roots
- make f square-free, get roots of f' by induction on d
- $f(a) = b \implies f$ has an inverse function g_a s.t. $g_a(b) = a$ in a nbh of b, given by a power series $g_a(w) = \sum_n c_n (w - b)^n$
- c_n TC^0-computable (Lagrange inversion formula)
- image of g_a includes a nbh of a with radius proportional to the distance from a to the nearest root of f'
  $\implies$ construct a poly-size set of sample points a s.t. all roots of f have the form $g_a(0)$

Formalization in $VTC^0 + IMUL$?

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

Bad news:
The argument heavily relies on complex analysis
(Cauchy integral formula, ...)
$\Longrightarrow$ unsuitable for formalization in bounded arithmetic

Nevertheless, we can prove

Main theorem: $VTC^0 + IMUL \vdash IOpen$

but we need a different strategy

Proof outline

- Direct proof of a form of the Lagrange inversion formula
  - polynomials can be locally inverted by power series
  - use this to compute roots of polynomials with small constant coefficient
- Model-theoretic argument using valued fields
  - the fraction field F of a DOR D carries a natural valuation induced by $\leq$
  - $D \vDash DIV \implies D$ is an integer part of the completion $\hat{F}$
  - D comes from $M \vDash VTC^0 + IMUL$
    $\implies \hat{F}$ is henselian by LIF
    $\implies \hat{F}$ is a real-closed field if M is ω-saturated
    $\implies D \vDash IOpen$ by Shepherdson's criterion

Lagrange inversion formula

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

$$b_n = \sum_{\sum_j (j-1)m_j = n-1} C_{m_2,\dots,m_d} \prod_{j=2}^{d} (-a_j)^{m_i}$$

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

($a_j, b_n, C_{\vec{m}}$ are binary rationals, $n, m_2, \dots, m_d$ unary integers)

Lagrange inversion formula (LIF):

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

LIF in $VTC^0 + IMUL$

Theorem 1: $VTC^0 + IMUL$ proves LIF for any constant d

Proof: By a convoluted but down-to-earth induction on $\vec{m} = \langle m_2, \dots, m_d \rangle$, show the identity

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

$VTC^0 + IMUL$ also proves a bound on the coefficients b_n:

Lemma: $|b_n| \le (4a)^{n-1}$, where $a = \max\{1, \sum_{j=2}^{d} |a_j|\}$

Aside: combinatorial interpretation of LIF

$C_{\vec{m}} = \#$ 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 $(*)$ $\iff$ a term is a variable or $c(t_1, \dots, t_k)$, where c is k-ary and t_j are terms

(counting of exponentially many objects
$\implies$ can't be used in $VTC^0 + IMUL$)

Root approximation with LIF

Theorem 2: $VTC^0 + IMUL$ proves for any constant d:
Let $h(z) = \sum_{j=0}^{d} a_j z^j$, $a_1 = 1$. Put $f(z) = h(z) - a_0$, and let g, b_n, a be as above.

If $|a_0| < 1/(4a)$, the partial sums $z_N = \sum_{n=1}^{N} b_n(-a_0)^n$ satisfy

$$|z_N| \le c := \frac{|a_0|}{1 - 4a|a_0|}, \qquad |z_N - z_M| \le c\big(4a|a_0|\big)^{N-1},$$

$$|h(z_N)| \le |a_0| N^d \big(4a|a_0|\big)^N.$$

That is, they converge fast to a (bounded) root of h.

Shepherdson's criterion revisited

For any DOR D with fraction field F, TFAE:

- $D \vDash IOpen$
- $D \vDash DIV$, and F is a dense subfield of a RCF R

(Assume $D \vDash DIV$ from now on.) Canonical choice of R:

- R = the least RCF extending F = its real closure $\mathrm{rcl}(F)$
- $D \vDash IOpen$ iff $F \subseteq \mathrm{rcl}(F)$ is dense

Try the other way round:

- R = the largest ordered extension of F where it is dense = its (Scott) completion $\hat{F}$
- $D \vDash IOpen$ iff $\hat{F}$ is a RCF

Completion of ordered fields

OF F is complete if it is not dense in any proper extension

Fact: (Scott/folklore)
Every OF F has a unique completion $\hat{F}$, i.e., a complete OF such that $F \subseteq \hat{F}$ is dense.

If $F \subseteq K$ is dense, then $K \subseteq \hat{F}$.

- $\hat{F}$ can be constructed using a kind of Dedekind cuts
- Alternative description: completion of valued fields
  - $\approx$ construction of $\mathbb{R}$ with Cauchy sequences
  - advantage: can apply general results from valuation theory

In models of arithmetic

Let D be a DOR coming from a model of arithmetic

Basic intuition:

- D = "integers" of the model
- fraction field F = "rationals" of the model
- completion $\hat{F}$ = "reals" of the model
  - virtual elements that can be arbitrarily closely approximated by "rationals"
  - not interpretable in D (too large)

Valued fields

Valuation $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$ on a field K:

- value group Γ: totally ordered abelian group
- $v(x) = \infty$ iff $x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min\{v(x), v(y)\}$

Induces additional data:

- valuation ring $O = \{x \in K : v(x) \geq 0\}$
- maximal ideal $I = \{x \in K : v(x) > 0\} = O \smallsetminus O^*$
- residue field $k = O/I$

Valuation rings

- Valuation rings in K = subrings $O \subseteq K$ s.t.
  $a \in O$ or $a^{-1} \in O$ for all $a \in K^*$
- Abstractly: valuation ring = integral domain O s.t.
  $a \mid b$ or $b \mid a$ for all $a, b \in O$
  $\implies$ such O is a valuation ring in its fraction field K
- Valuation is defined by the valuation ring up to equivalence: $\Gamma \simeq K^*/O^*$, $v\colon K^* \to K^*/O^*$ quotient map

Example 1

Let k be a field. The field $K = k((x))$ of formal Laurent series

$$a = \sum_{n=N}^{\infty} a_n x^n, \qquad N \in \mathbb{Z}, a_n \in k$$

carries a valuation

$$v(a) = \min\{n \in \mathbb{Z} : a_n \neq 0\}$$

- Valuation ring = $k[\![x]\!]$ (formal power series)
- Value group = $\mathbb{Z}$
- Residue field = k

Example 2

Let p be a prime. The field $K = \mathbb{Q}_p$ of p-adic numbers

$$\dots a_3 a_2 a_1 a_0 . a_{-1} \dots a_{-N}, \qquad a_n \in \{0, \dots, p-1\}$$

carries the p-adic valuation

$$v_p(a) = \min\{n \in \mathbb{Z} : a_n \neq 0\}$$

- Valuation ring = $\mathbb{Z}_p$ (p-adic integers)
- Value group = $\mathbb{Z}$
- Residue field = $\mathbb{F}_p$ (p-element field)

Also induces the p-adic valuation on $\mathbb{Q} \subseteq \mathbb{Q}_p$:
$v_p(p^e p_1^{e_1} \cdots p_k^{e_k}) = e$

Topology and completeness

Valuation induces a topology on the field:
basic (cl)open sets = ultrametric balls

$$B(a,\gamma) = \{u \in K : v(a-u) > \gamma\}, \qquad a \in K, \gamma \in \Gamma$$

$\langle K, v\rangle$ is complete if every transfinite Cauchy sequence converges

Theorem: Every valued field $\langle K, v\rangle$ has a unique completion, i.e., a complete extension $\langle \hat{K}, \hat{v}\rangle$ of $\langle K, v\rangle$ s.t. $K \subseteq \hat{K}$ is (topologically) dense

Examples: $\mathbb{Q}_p$ is the completion of $\langle \mathbb{Q}, v_p\rangle$
$k((x))$ is the completion of $k(x)$

Valuations on ordered fields

$\langle K, \leq \rangle$ ordered field $\implies$ natural valuation v with

$$O = \{x \in K : \exists n \in \mathbb{N}\, |x| \leq n\}$$
$$I = \{x \in K : \forall n \in \mathbb{N}\, |x| \leq 1/n\}$$

- residue field: archimedean OF $\implies k \subseteq \mathbb{R}$
- valued field completion $\hat{K}$ = ordered field completion
- More generally: valuations with convex valuation ring
  - residue field canonically ordered
  - valuation topology = interval topology

Need yet: how to recognize RCF?

Discrete valuation rings

Discrete valuation ring (DVR): valuation ring with $\Gamma = \mathbb{Z}$

- Examples: $k[\![x]\!]$, $\mathbb{Z}_p$
- Nice properties: noetherian, PID, . . .

Henselian valuations

Hensel's lemma:
O complete DVR, $f \in O[x]$, $v(f(a)) > 0$, $v(f'(a)) = 0$
$\implies f$ has a root $\alpha \in O$ with $v(\alpha - a) > 0$

Generally: valuation rings or valued fields satisfying Hensel's lemma are called henselian

- first-order property
- share nice model-theoretic properties of complete DVRs

Warning: Complete valuation rings are not henselian in general ($\Gamma = \mathbb{Z}$ makes a difference)

AKE principle

Theorem (Cohen):
Complete DVR of residue characteristic 0 are uniquely determined by the residue field (i.e., isomorphic to $k[\![x]\!]$).

Vast generalization to henselian VF:

Ax–Kochen–Ershov principle:
Two henselian valued fields of res.char. 0 (more generally: unramified) are elementarily equivalent iff their residue fields and value groups are elementarily equivalent.

Characterization of RCF

A (much easier) special case of AKE:

Theorem: K ordered field, O convex valuation ring of K
$\Longrightarrow$ K is a RCF iff

- henselian
- residue field k is a RCF
- value group Γ is divisible

Example

Puiseux series: $K = k\langle\langle x \rangle\rangle := \bigcup_m k((x^{1/m}))$

$$\sum_{n=N}^{\infty} a_n x^{n/m}, \qquad N \in \mathbb{Z}, a_n \in k, m \in \mathbb{N}^+$$

- value group $\mathbb{Q}$
- henselian ($\because$ each $k[[x^{1/m}]]$ is a complete DVR)

Corollary: k RCF $\implies$ $k\langle\langle x \rangle\rangle$ RCF

By the way: $k = \mathrm{rcl}(\mathbb{Q}) \implies k\langle\langle x \rangle\rangle$ has an integer part of Puiseux polynomials with integer constant coefficient $\implies$ $IOpen$ has a nonstandard recursive model [Shep'64]

Open induction and valued fields

Corollary: Let D DOR, $D \vDash DIV$, F fraction field with natural valuation, $\hat{F}$ its completion.

Then $D \vDash IOpen$ iff $\hat{F}$ henselian, residue field k RCF, value group Γ divisible.

Note: F and $\hat{F}$ have the same residue field and value group

Our case: $M \vDash VTC^0 + IMUL$ induces DOR $D \vDash DIV$

- Γ is divisible—easy
- if M is ω-saturated, then $k = \mathbb{R}$
- $\hat{F}$ henselian: follows from Theorem 2 (LIF)

This gives the Main theorem: $VTC^0 + IMUL \vdash IOpen$

What about VTC^0?

Question: Does VTC^0 prove $IOpen$?

The Main theorem and [JP'98] imply that TFAE:

- $VTC^0 \vdash IOpen$
- $VTC^0 \vdash IMUL$
- $VTC^0 \vdash DIV$

$\implies$ the problem is whether VTC^0 can formalize the division algorithm of [HAB'02]

Thank you for attention!

References

S. Cook, P. Nguyen, *Logical foundations of proof complexity*, CUP, 2010.

A. Engler, A. Prestel, *Valued fields*, Springer, 2005.

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*, Theoret. Comput. Sci. 462 (2012), 59–69.

J. Johannsen, C. Pollett, *On proofs about threshold circuits and counting hierarchies* (*extended abstract*), in: Proc. 13th LICS, 1998, 444–452.

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