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

Motivation

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 $P \in C$, what can we prove about P using only concepts from C?
- That is: what does T prove about P?

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

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)

Weak subclass of polynomial time

$\mathbf{TC}^0$ 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, ...

$\Rightarrow$ $\mathbf{TC}^0$ 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 VTC^0 include Shepherdson's theory $IOpen = DOR +$ quantifier-free induction in $L = \langle +, \cdot, \leq \rangle$?

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

$VTC^0 + IMUL$

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

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

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

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

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

Note: $VTC^0 + IMUL$ corresponds to $\mathbf{TC}^0$, just like VTC^0

$VTC^0 + IMUL \vdash DIV$

We need $IMUL$ rather than DIV for technical reasons

$IOpen$ algebraized

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

- $D \vDash IOpen$
- D is an integer part of a real-closed field $R \supseteq D$:

$$\forall \alpha \in R\, \exists x \in D\, (x \le \alpha < x + 1)$$

- If $u < v \in D$ and $f \in D[x]$ is such that $f(u) \le 0 < f(v)$, there is $u \le x < v$ in D such that $f(x) \le 0 < f(x + 1)$

Open induction and root finding

Corollary: The following are equivalent:

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

Good news: $\mathbf{TC}^0$ root approximation algorithms exist for any constant d [J'12]

Bad news: The argument heavily relies on complex analysis $\Rightarrow$ not suitable for $VTC^0 + IMUL$

Proof overview

We show $VTC^0 + IMUL \vdash IOpen$ using a mixed strategy:

(1) 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

(2) Model-theoretic argument employing valued fields

- the fraction field F of a DOR D carries a natural valuation induced by $\leq$
- $D \vDash DIV \Rightarrow D$ is an integer part of the completion $\hat{F}$
- D comes from $M \vDash VTC^0 + IMUL$
  $\Rightarrow \hat{F}$ is henselian due to (1)
  $\Rightarrow \hat{F}$ is a real-closed field if M is ω-saturated

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_j 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 elementary induction on $\vec{m} = \langle m_2, \dots, m_d \rangle$, show the identity

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

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

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

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

$$|z_N| \le \frac{|a_0|}{1 - 4a|a_0|}$$

$$|z_N - z_M| \le \frac{|a_0|}{1 - 4a|a_0|}\bigl(4a|a_0|\bigr)^{N-1}$$

$$|h(z_N)| \le |a_0| N^d \bigl(4a|a_0|\bigr)^N$$

for any unary $N \le M$.

Valued fields

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

- value group Γ: totally ordered abelian group
- $v(x) = \infty \Leftrightarrow x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x+y) \geq \min\{v(x), v(y)\}$
- valuation ring $O = \{x \in K : v(x) \geq 0\}$
- maximal ideal $I = \{x \in K : v(x) > 0\} = O \smallsetminus O^*$
- residue field $k = O/I$

v is defined by the valuation ring up to equivalence:
$\Gamma \simeq K^*/O^*$, $v\colon K^* \to K^*/O^*$ quotient map

Valuation on ordered fields

$\langle K, \leq \rangle$ ordered field $\Rightarrow$ 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 $\Rightarrow k \subseteq \mathbb{R}$
- the completion $\hat{K}$ of $\langle K, v \rangle$ is the largest ordered field extension of K in which K is dense

Open induction and valued fields

$M \vDash VTC^0 + IMUL$ induces DOR D, let F be its fraction field

Using $D \vDash DIV$, we have:

$$\begin{aligned} D \vDash IOpen &\Leftrightarrow D \text{ integer part of a RCF} \\ &\Leftrightarrow F \text{ dense subfield of a RCF} \\ &\Leftrightarrow \hat{F} \text{ is a RCF} \end{aligned}$$

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

(1) value group $\Gamma = K^*/O^*$ is divisible

(2) residue field $k = O/I$ is a RCF

(3) O is henselian

Checking the conditions

In our case:

(1) Γ is divisible—easy

(2) We can assume M ω-saturated, then $k = \mathbb{R}$ RCF

(3) We need: any $h(x) = \sum_{j \le d} a_j x^j \in O[x]$ such that $a_1 = 1$, $a_0 \in I$, has a root in O. This follows from Theorem 2.

We obtain
Theorem 3: $VTC^0 + IMUL \vdash IOpen$

What about VTC^0?

Question: Does VTC^0 prove $IOpen$?

Theorem 3 and [JP'98] imply that TFAE:

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

$\Rightarrow$ 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.