Iterated multiplication in VTC^0

Emil Jeřábek

jerabek@math.cas.cz

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

Institute of Mathematics, Czech Academy of Sciences, Prague

Journées sur les Arithmétiques Faibles 40
October 2021, Athens

Outline

1. **$\mathbf{TC}^0$, VTC^0, and $IMUL$**
2. **Hesse–Allender–Barrington algorithm**
3. **Working with CRR**
4. **Polylogarithmic cut**
5. **Modular exponentiation**
6. **The grand scheme**

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

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 $+, \cdot, \leq$

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

$\mathbf{TC}^0$ 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 $\mathbb{Q}$, $\mathbb{Q}(i)$
- 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

Buss-style bounded arithmetic

One-sorted theories of bounded arithmetic:

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

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

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

Zambella-style bounded arithmetic

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
- $V^i = 2\text{-}BASIC + \Sigma^B_i\text{-}COMP$ (implies $\Sigma^B_i\text{-}IND$)

The theory VTC^0

The two-sorted theory corresponding to $\mathbf{TC}^0$ is VTC^0:

- $V^0 +$ every set has a counting function
- provably total computable (i.e., $\exists\Sigma^B_0$-definable) functions are exactly the $\mathbf{TC}^0$-functions
- has induction, comprehension, minimization, ... for $\mathbf{TC}^0$-predicates

Binary arithmetic in VTC^0:

- can define $+, \cdot, \leq$ on binary integers
- proves integers form a discretely ordered ring
- iterated multiplication challenging $\implies$ axiom $IMUL$:

$$\forall X, n\, \exists Y\, \forall i \leq j < n\, (Y_{i,i} = 1 \wedge Y_{i,j+1} = Y_{i,j} \cdot X_j)$$

(think $Y_{i,j} = \prod_{k=i}^{j-1} X_k$)

RSUV isomorphism

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	$\Delta^b_1\text{-}CR$
$VTC^0 + \Sigma^B_0\text{-}AC$	C^0_2
$VTC^0 + IMUL + \Sigma^B_0\text{-}AC$	$C^0_2[div]$

$$(i \geq 1)$$

Arithmetic in $VTC^0 + IMUL$ / $C^0_2[div]$

Besides division, $VTC^0 + IMUL$ / $C^0_2[div]$ can do:

- root approximation for constant-degree polynomials
- $\Longrightarrow$ ($RSUV$-translation of) open induction ($IOpen$)

Even better (using ideas of [Man'91]):

Theorem [J'15]

- $VTC^0 + IMUL$ proves the $RSUV$-translations of Σ^b_0-IND (T^0_2) and Σ^b_0-MIN
- $C^0_2[div]$ proves Σ^b_0-IND, Σ^b_0-MIN

What remains

Question

Does VTC^0 prove $IMUL$?

Iterated multiplication is $\mathbf{TC}^0$-computable:

Question

Can VTC^0 formalize the algorithms from [HAB'02]?

Hesse–Allender–Barrington algorithm

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 $\mathbf{P}$-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 $\Longrightarrow$

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

Structure of the algorithm

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

- pick sufficiently long list of primes $\vec{m}$
- convert each X_u to $\mathrm{CRR}_{\vec{m}}$
- multiply the residues modulo each m_i
- 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 $\mathrm{CRR}_{\vec{d}}$

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

Structure of the algorithm

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

- sum discrete logarithms modulo m

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

- pick sufficiently long list of primes $\vec{m}$
- convert each X_u to $\mathrm{CRR}_{\vec{m}}$
- multiply the residues modulo each m_i
- 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: $\prod_{i<n} a_i \bmod m$ (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 $VTC^0 + IMUL$, but what good is that?

Results [J'20]

Theorem

$VTC^0 \vdash IMUL$

Corollary

- $VTC^0 \vdash RSUV$-translation of Σ^b_0-MIN
- $C^0_2 \equiv C^0_2[div]$, proves Σ^b_0-MIN

Theorem

$\exists\ \Delta_0$ definition of $a^r \bmod m$ s.t. $I\Delta_0 + WPHP(\Delta_0) \vdash$

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

Overview of the formalization

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

(1) $VTC^0(\mathrm{imul}) \vdash \mathit{IMUL}$

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

(2) $V^0 \vdash \mathit{IMUL}\big[|w|^c\big]$

  - the polylogarithmic cut in V^0 is a model of VNL

(3) $V^0 + \mathit{WPHP} \vdash$ 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
    $\mathit{IMUL} \to$ cyclicity $\to \mathrm{imul} \to \mathit{IMUL}$ makes progress
    $\Longrightarrow$ proof by induction

Working with CRR

Goal: CRR reconstruction

Theorem

$\exists$ $\mathbf{TC}^0(\mathrm{imul})$-function Rec s.t. $VTC^0(\mathrm{imul})$ proves:

$\vec{m}$ distinct primes, $|X| < \sum_i \big(|m_i| - 1\big)$
$\implies \mathrm{Rec}\big(\vec{m}; \mathrm{CRR}_{\vec{m}}(X)\big) = X$

Corollary

$VTC^0(\mathrm{imul}) \vdash IMUL$

Proof: $\vec{m}$ large enough $\implies Y_j := \mathrm{Rec}\big(\vec{m}; \prod_{i<j} \mathrm{CRR}_{\vec{m}}(X_i)\big)$

By induction on j, show $|Y_j| \le \sum_{i<j} |X_i|$ and $Y_{j+1} = X_j Y_j$

Basic tool

Notation: $[\vec{m}] = \prod_{i<k} m_i$, $[\vec{m}]_{\neq j} = \prod_{i\neq j} m_i$

CRR rank equation

$X < [\vec{m}]$, $\vec{x} = \mathrm{CRR}_{\vec{m}}(X) \implies$

$$\sum_{i<k} \frac{x_i h_i}{m_i} = r(\vec{x}) + \frac{X}{[\vec{m}]}$$

where $h_i = [\vec{m}]_{\neq i}^{-1} \bmod m_i$

- rank $r(\vec{x})$: small integer
- holds in $\mathbb{Q} \implies$ approximation $\xi(\vec{m};\vec{x})$ of $X/[\vec{m}]$
- holds in $\mathbb{Z}/a\mathbb{Z} \implies$ base extension $e(\vec{m};\vec{x};a) = X \bmod a$

Rank and friends formalized

In $VTC^0(\mathrm{imul})$: for large enough n, consider

$$
\begin{aligned}
S_n(\vec{m};\vec{x}) &= \sum_{i<k} \left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil \\
r_n(\vec{m};\vec{x}) &= \lfloor 2^{-n} S_n(\vec{m};\vec{x}) \rfloor \\
\xi_n(\vec{m};\vec{x}) &= 2^{-n}\big(S_n(\vec{m};\vec{x}) \bmod 2^n\big) \\
e_n(\vec{m};\vec{x};a) &= \sum_{i<k} x_i h_i [\vec{m}]_{\neq i} - r_n(\vec{m};\vec{x})[\vec{m}] \mod a
\end{aligned}
$$

The laborious part:

- prove lots of properties of r_n, ξ_n, e_n from first principles
- use them to analyze the reconstruction procedure

Polylogarithmic cut

The polylogarithmic cut

$$\mathcal{M} = \langle M_1, M_2, \in, |\cdot|, 0, 1, +, \cdot, < \rangle \vDash V^0$$
$$\implies \mathcal{M}_{\mathrm{pl}} = \langle M_{\mathrm{pl},1}, M_{\mathrm{pl},2}, \dots \rangle \text{ where}$$

$$M_{\mathrm{pl},1} = \{x \in M_1 : \exists c \in \omega \, \mathcal{M} \vDash \exists w \, x \le |w|^c\}$$
$$M_{\mathrm{pl},2} = \{X \in M_2 : |X| \in M_{\mathrm{pl},1}\}$$

Using the idea of Nepomnjaščij's theorem:

- [Zam'97] (implicitly) $\mathcal{M} \vDash V^0 \implies \mathcal{M}_{\mathrm{pl}} \vDash VL$
- [Mül'13] $\mathcal{M} \vDash V^0 \implies \mathcal{M}_{\mathrm{pl}} \vDash VNC^1$
- similar formalization in [Ats'03]

Lemma

$$\mathcal{M} \vDash V^0 \implies \mathcal{M}_{\mathrm{pl}} \vDash VNL$$

Polylogarithmic products

Lemma

$VTC^0(\mathrm{imul}) \subseteq VL$

Corollary

For any constant c, V^0 can do:

- $\prod_{i<n} X_i$ if $\sum_i |X_i| \le |w|^c$
- $\lfloor Y/X \rfloor$ if $|X|, |Y| \le |w|^c$
- $\prod_{i<n} a_i \bmod m$ if $n \le |w|^c$

Modular exponentiation

The [HAB'02] algorithm

To compute a^r for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, $n = \varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$:

- fix sequence $\vec{d}$ of primes s.t. $d_i = O(\log n)$, $d_i \nmid n$
  $d = \prod_i d_i$: $n < d < n^{O(1)}$
- $x \mapsto x^{d_i}$ an automorphism $\implies$ $\mathbf{AC}^0$ inverse $x \mapsto x^{1/d_i}$
- given r, find $u_i = O(\log n)$, $u = O\big((\log n)^2\big)$ s.t.

$$r \equiv u + \sum_i u_i \left\lfloor \frac{n}{d_i} \right\rfloor \pmod{n}$$

- using $a^n = 1$, compute $a_i = a^{\lfloor n/d_i \rfloor} = a^{-(n \bmod d_i)/d_i}$,
  $a^r = a^u \prod_i a_i^{u_i}$

Analysis requires: modular exponentiation (chicken or egg?), Fermat's little theorem

Drop $a^{\lfloor n/d_i \rfloor}$, just use a^{1/d_i} directly

To compute a^r for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, $n = \varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$:

- fix sequence $\vec{d}$ of primes s.t. $d_i = O(\log n)$, $d_i \nmid n$
  $d = \prod_i d_i$: $n < d < n^{O(1)}$
- $x \mapsto x^{d_i}$ an automorphism $\implies$ $\mathbf{AC}^0$ inverse $x \mapsto x^{1/d_i}$
- given $s < 2d$, find $u_i, u = O(\log n)$ s.t.

$$\frac{s}{d} = u + \sum_i \frac{u_i}{d_i} \qquad (\mathrm{CRR}_{\vec{d}} \text{ rank equation})$$

- compute $a^{s/d} := a^u \prod_i (a^{1/d_i})^{u_i}$
- *WPHP* $\implies$ $a^{s/d}$ is t-periodic for some $t \le 2n$
  $\implies$ extend the definition of $a^{s/d}$ to all s by $a^{(s \bmod t)/d}$
- put $a^r = a^{(rd)/d}$

Modular exponentiation formalized

Theorem

$V^0 + WPHP \subseteq VTC^0$ proves the totality of pow

Also extends to non-prime m

Using conservativity, can do it in $I\Delta_0 + WPHP(\Delta_0)$:

Theorem

$\exists$ Δ_0 definition of $a^r \bmod m$ s.t. $I\Delta_0 + WPHP(\Delta_0) \vdash$

$$\begin{aligned} a^0 &\equiv 1 \pmod{m}, \\ a^{r+1} &\equiv a^r a \pmod{m} \end{aligned}$$

The grand scheme

Cyclic generators

Still missing: $VTC^0 \overset{?}{\vdash} m \text{ prime} \to (\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic

$\implies VTC^0 = VTC^0(\mathrm{pow}) = VTC^0(\mathrm{imul})$

Lemma

The following are equivalent over VTC^0:

- *IMUL*
- m prime $\to (\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic
- m, p primes, $a \not\equiv 1 \equiv a^p \equiv b^p \pmod m$
  $\to \exists r < p \; b \equiv a^r \pmod m$

Can we escape this vicious circle?

VTC^0 **proves** $IMUL$

Fine-tune the parameters:

- $IMUL[x]$, $\mathrm{imul}[x]$, $Cyc[z, x]$

VTC^0 proves $IMUL$

Fine-tune the parameters:

- $IMUL[x]$, $\mathrm{imul}[x]$, $Cyc[z,x]$

$$\exists \prod_{i<n} X_i \text{ whenever } \sum_i |X_i| \le x$$

VTC^0 proves $IMUL$

Fine-tune the parameters:

- $IMUL[x]$, $\mathrm{imul}[x]$, $Cyc[z,x]$

$$\exists \prod_{i<n} a_i \bmod m \text{ whenever } m \le x \text{ prime}$$

VTC^0 proves $IMUL$

Fine-tune the parameters:

- $IMUL[x]$, $\mathrm{imul}[x]$, $Cyc[z,x]$ ($Cyc \in \Sigma^B_0$)

$$m \le z \text{ and } p < x \text{ primes, } a \not\equiv 1 \equiv a^p \equiv b^p \pmod m$$
$$\implies \exists r < p \; b \equiv a^r \pmod m$$

VTC^0 proves $IMUL$

Fine-tune the parameters:

- $IMUL[x]$, $\mathrm{imul}[x]$, $Cyc[z,x]$ ($Cyc \in \Sigma^B_0$)
- VTC^0 proves

$$\begin{aligned} \mathrm{imul}[x^3] &\to IMUL[x] \\ IMUL\big[x^2|z|\big] &\to Cyc[z,x] \\ Cyc[z,x] &\to \mathrm{imul}\big[\min\{z, x^c|z|^c\}\big] \end{aligned}$$

(new idea: structure theorem for finite abelian groups)

$$\therefore (x+1)^6|z|^3 \le z \wedge Cyc[z,x] \to Cyc[z,x+1]$$

- finish the proof by induction on x

Summary

- VTC^0 proves $IMUL$
- VTC^0 proves $RSUV$-translation of Σ^b_0-MIN
- $C^0_2 \equiv C^0_2[div]$, proves Σ^b_0-MIN
- $I\Delta_0 + WPHP(\Delta_0)$ has a well-behaved Δ_0 definition of $a^r \bmod m$

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
- E. Jeřábek: Open induction in a bounded arithmetic for $\mathbf{TC}^0$, Arch. Math. Logic 54 (2015), 359–394

References (cont'd)

- E. Jeřábek: Iterated multiplication in VTC^0, arXiv:2011.03095
- 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^b_1-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
- S. Müller: Polylogarithmic cuts in models of $\mathbf{V}^0$, Logical Methods in Comp. Sci. 9 (2013), no. 1
- D. Zambella: End extensions of models of linearly bounded arithmetic, Ann. Pure Appl. Logic 88 (1997), 263–277