Iterated multiplication in VTC^0

Emil Jeřábek

jerabek@math.cas.cz

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

Institute of Mathematics, Czech Academy of Sciences, Prague

Logic seminar, Institute of Mathematics, 26 October 2020

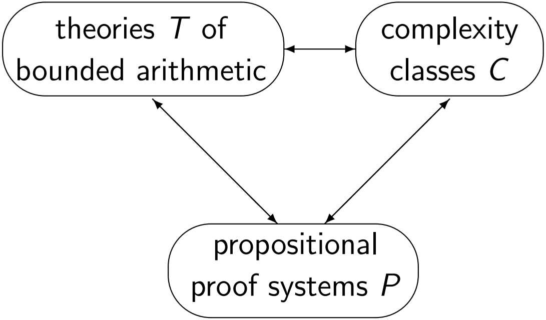
Outline

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

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

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 $+, \cdot, \leq$

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

Zambella-style bounded arithmetic

Two-sorted 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
- Σ^1_1 formulas: $\exists X\, \theta(X, \dots)$, $\theta \in \Sigma^B_0$
- $V^i = 2\text{-}BASIC + \Sigma^B_i\text{-}COMP$ (implies $\Sigma^B_i\text{-}IND$)

The theory VTC^0

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

- V^0 + every set has a counting function
- provably total computable (i.e., Σ^1_1-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

Basic question

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

The iterated multiplication axiom

Iterated multiplication algorithm [HAB'02] challenging to formalize $\implies$ divide and conquer: make it an axiom!

IMUL

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

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

Basic questions

- What properties of $+, \cdot, \le$ are provable in $VTC^0 + IMUL$?
- Does VTC^0 prove $IMUL$?

Arithmetic in $VTC^0 + IMUL$

Theorem [J'15]

$VTC^0 + IMUL$ can do:

- Division: $\forall X\,\forall Y > 0\,\exists Q\,\exists R < Y\,(X = Y \cdot Q + R)$
- Root approximation: $p(X) = \sum_{i\le d} A_i X^i$, d constant

$$X < Y \wedge p(X) \le 0 < p(Y) \to$$
$$\exists Z\,\big(X \le Z < Y \wedge p(Z) \le 0 < p(Z+1)\big)$$

- Open induction (*IOpen*): second-order induction

$$\varphi(0) \wedge \forall X\,\big(\varphi(X) \to \varphi(X+1)\big) \to \forall X\,\varphi(X)$$

for quantifier-free $\langle +, \cdot, \le \rangle$-formulas $\varphi(X, \vec{Y})$

Buss-style bounded arithmetic

One-sorted theories of bounded arithmetic:

- (binary) integers, language $\langle 0, 1, +, \cdot, \leq, \lfloor x/2 \rfloor, |x|, \# \rangle$
- Σ_0^b formulas: sharply bounded q'fiers $\exists x \leq |t|$, $\forall x \leq |t|$
- $\hat{\Sigma}_i^b$ formulas: i alternating blocks of bounded quantifiers (first block $\exists$) followed by a Σ_0^b formula
- $T_2^i = BASIC + \hat{\Sigma}_i^b\text{-}IND$, $S_2^i = BASIC + \hat{\Sigma}_i^b\text{-}PIND$

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

- language with $\dot{-}$, $\lfloor x/2^y \rfloor$
- all theories include open $LIND$
- C_2^0: $BB\Sigma_0^b$ [JP'98]
- $C_2^0[div]$: language incl. $\lfloor x/y \rfloor$ [Joh'99]
- $\Delta_1^b\text{-}CR$: Δ_1^b bit-comprehension rule [JP'00]

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

$(i \geq 1)$

Sharply bounded minimization

The result above, more precisely:

- $VTC^0 + IMUL$ proves the $RSUV$-translation of $IOpen$
- $\implies C^0_2[div]$ proves $IOpen$

Structural description of Σ^b_0 formulas [Man'91]
$\implies$ generalization:

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 $IMUL$?

NB: Using results of [Joh'99], the following are equivalent:

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

Iterated multiplication and division are $\mathbf{TC}^0$-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 **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 $\mathbf{TC}^0$)

Improved CRR reconstruction procedures $\implies$

- [CDL'01]: logspace-uniform $\mathbf{TC}^0$ (hence **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: $a^r \bmod m$ (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

Theorem

$VTC^0 \vdash IMUL$

Corollary

- $VTC^0 \vdash RSUV$-translation of Σ_0^b-MIN
- $C_2^0 \equiv C_2^0[div]$, proves Σ_0^b-MIN

Theorem

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

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

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

Minutiae

Primes

CRR requires a steady supply of primes

Consider contribution of various prime factors to $\binom{2n}{n}$:

Theorem (Chebyshev 1848)

$$\sum_{p \le x} \log p = \Theta(x).$$

Stragithforward formalization:

Lemma

$$VTC^0 \vdash \sum_{p \le x|x|^{17}} (|p| - 1) \ge x \text{ for } x \text{ large enough}$$

Division by small primes

Need $X \bmod m$ to define CRR and to manipulate it

Lemma

$VTC^0(\mathrm{pow}) \vdash m \text{ prime} \to \forall X\, \exists Q\, \exists r < m\, X = mQ + r$

$$\left\lfloor \frac{2^n}{m} \right\rfloor = \sum_{i<n} 2^i \left((2^{n-i} \bmod m) \bmod 2 \right)$$

Working with CRR

Goal: CRR reconstruction

Theorem

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

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

Corollary

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

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

By induction on j, show $|Y_j| \leq \sum_{i<j} |X_i|$ 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

$$S_n(\vec{m};\vec{x}) = \sum_{i<k} \left\lceil \frac{2^n x_i h_i}{m_i} \right\rceil$$

$$r_n(\vec{m};\vec{x}) = \lfloor 2^{-n} S_n(\vec{m};\vec{x}) \rfloor$$

$$\xi_n(\vec{m};\vec{x}) = 2^{-n}\big(S_n(\vec{m};\vec{x}) \bmod 2^n\big)$$

$$e_n(\vec{m};\vec{x};a) = \sum_{i<k} x_i h_i [\vec{m}]_{\neq i} - r_n(\vec{m};\vec{x})[\vec{m}] \mod a$$

The laborious part:
prove lots of properties of r_n, ξ_n, e_n from first principles

Computing with CRR: example (I)

$\vec{x} = \mathrm{CRR}_{\vec{m}}(X)$, $\vec{y} = \mathrm{CRR}_{\vec{m}}(Y) \implies$
$\vec{x} + \vec{y} \pmod{\vec{m}}$ represents $(X + Y) \bmod [\vec{m}]$

Formalize without reference to X, Y:

Lemma

$VTC^0(\mathrm{imul})$ proves: $n \geq |k|$, $\vec{z} = (\vec{x} + \vec{y}) \bmod \vec{m}$
$\implies \exists c \in \{-1, 0, 1\}$ s.t.

$$r_n(\vec{m}; \vec{z}) = r_n(\vec{m}; \vec{x}) + r_n(\vec{m}; \vec{y}) + c - \sum_{x_i + y_i \geq m_i} h_i$$

$$\xi_n(\vec{m}; \vec{z}) = \xi_n(\vec{m}; \vec{x}) + \xi_n(\vec{m}; \vec{y}) - c \pm 2^{-n} k$$

$$e_n(\vec{m}; \vec{z}; a) \equiv e_n(\vec{m}; \vec{x}; a) + e_n(\vec{m}; \vec{y}; a) - c[\vec{m}] \pmod{a}$$

Computing with CRR: example (II)

r_n and e_n are discrete quantities
$\implies$ approximation better be exact for large enough n

Lemma

$VTC^0(\mathrm{imul})$ proves: $n' \geq n \geq |k| + 2 + \sum_{i<k} |m_i| \implies$

$$r_n(\vec{m}; \vec{x}) = r_{n'}(\vec{m}; \vec{x})$$
$$e_n(\vec{m}; \vec{x}; \vec{a}) = e_{n'}(\vec{m}; \vec{x}; \vec{a})$$
$$\xi_n(\vec{m}; \vec{x}) = \xi_{n'}(\vec{m}; \vec{x}) \pm 2^{-n} k$$

The reconstruction procedure

Given $\vec{m}$, $\vec{x}$:

Fix large enough s, prime sequences $\vec{a}_u$, $u < s$, and put

$$\vec{w}_t = \Big(2^{-t} \prod_{u<t} (1 + [\vec{a}_u])\Big) e(\vec{m}; \vec{x}; \vec{m}, \vec{a}_{<t}) \mod \vec{m}, \vec{a}_{<t}$$

$$\vec{y}_t = [\vec{a}_{<t}]^{-1} \big(\vec{w}_t \restriction \vec{m} - e(\vec{a}_{<t}; \vec{w}_t \restriction \vec{a}_{<t}; \vec{m})\big) \mod \vec{m}$$

$$b_t \in \{-1, 0, 1, 2\} \quad \text{s.t.} \quad \vec{y}_t - 2\vec{y}_{t+1} \equiv \mathrm{CRR}_{\vec{m}}(b_t)$$

Define $\mathrm{Rec}(\vec{m}; \vec{x}) = \sum_{t<s} 2^t b_t$

Analysis of CRR reconstruction

Let $\vec{x} = \mathrm{CRR}_{\vec{m}}(X)$

In the real world:

- $\vec{w}_t$ represents $X \prod_{u<t} \frac{1+[\vec{a}_u]}{2}$
- $\vec{y}_t$ represents $\left\lfloor X \prod_{u<t} \frac{1+[\vec{a}_u]}{2[\vec{a}_u]} \right\rfloor = \lfloor X 2^{-t} \rfloor$
- $b_t = \mathrm{bit}(X, t) \implies \mathrm{Rec}(\vec{m}; \vec{x}) = X$

In $VTC^0(\mathrm{imul})$:

- $\xi_n(\vec{m}; \vec{y}_t) \approx \xi_n(\vec{m}, \vec{a}_{<t}; \vec{w}_t) \approx 2^{-t} \xi_n(\vec{m}; \vec{x})$
- $\xi_n(\vec{m}; \vec{y}_t) \approx 2\xi_n(\vec{m}; \vec{y}_{t+1}) + b_t \xi_n(\vec{m}; \vec{1})$
- $\mathrm{Rec}(\vec{m}; \vec{x})\, \xi_n(\vec{m}; \vec{1}) \approx \xi_n(\vec{m}; \vec{x}) \approx X \xi_n(\vec{m}; \vec{1})$
  $\implies \mathrm{Rec}(\vec{m}; \vec{x}) = X$

Polylogarithmic cut

The polylogarithmic cut

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

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

Main idea of [HAB'02]

To compute a^r for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$:

- $n = \varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$
- fix a large enough prime sequence $\vec{d}$,
  $d_i = O(\log n)$, $d_i \nmid n$
- $x \mapsto x^{d_i}$ is an automorphism $\implies$ $\mathbf{AC}^0$ inverse $x \mapsto x^{1/d_i}$
- compute $a_i = a^{\lfloor n/d_i \rfloor} = a^{-(n \bmod d_i)/d_i}$ (using $a^n = 1$)
- write $r \equiv u + \sum_i u_i \lfloor n/d_i \rfloor \pmod{n}$,
  $u_i = O(\log n)$, $u = O\big((\log n)^2\big)$
- $a^r = a^u \prod_i a_i^{u_i}$ (using $a^n = 1$)

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

Simplify the algorithm

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

- $d = \prod_i d_i$: $n < d < n^{O(1)}$
- define $a^{x/d}$ for $x < 2d$ using the $\mathrm{CRR}_{\vec{d}}$ rank equation:

$$\frac{x}{d} = u + \sum_i \frac{u_i}{d_i} \implies a^{x/d} := a^u \prod_i (a^{1/d_i})^{u_i},$$

  where $u_i = x[\vec{d}]^{-1}_{\neq i} \bmod d_i = O(\log n)$, $u = O(\log n)$
- *WPHP* $\implies$ $a^{x/d}$ is t-periodic for some $t \leq 2n$
  $\implies$ extend the definition of $a^{x/d}$ to all x with $a^{(x \bmod t)/d}$
- 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

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

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

The grand scheme

Cyclic generators

Still missing: $VTC^0 \overset{?}{\vdash} m$ 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?

Fine-tune the parameters

$IMUL[w]$:

- $\exists \prod_{i<n} X_i$ whenever $\sum_i |X_i| \leq w$

$\mathrm{imul}[w]$:

- $\exists \prod_{i<n} a_i \bmod m$ whenever $m \leq w$ prime

$Cyc[z, w]$:

- $m \leq z$ and $p < w$ primes, $a \not\equiv 1 \equiv a^p \equiv b^p \pmod{m}$
  $\to \exists r < p\, b \equiv a^r \pmod{m}$

NB: $Cyc[z, w] \in \Sigma^B_0$

$\mathrm{imul} \to \mathit{IMUL} \to \mathit{Cyc}$

Lemma

VTC^0 proves $\mathrm{imul}[w^3] \to \mathit{IMUL}[w]$

By inspection of the proof of $VTC^0(\mathrm{imul}) \vdash \mathit{IMUL}$

Lemma

VTC^0 proves $\mathit{IMUL}\left[w^2|z|\right] \to \mathit{Cyc}[z, w]$

Given $a \not\equiv 1 \equiv a^p \equiv b^p \pmod{m}$, construct the polynomial

$$f(x) \equiv \prod_{i<p}(x - a^i) \pmod{m}$$

$$f(x) \equiv f(ax) \implies f(x) \equiv x^p - 1 \implies \prod_{i<p}(b - a^i) \equiv 0$$

$Cyc \to \mathrm{imul}$

Lemma

For any c, $VTC^0 \vdash Cyc[z,w] \to \mathrm{imul}\bigl[\min\{z, w^c|z|^c\}\bigr]$

Mimick the proof of the structure theorem for finite abelian groups

$m \le z$ prime, $Cyc[z,w] \implies (\mathbb{Z}/m\mathbb{Z})^\times$ is
a large cyclic group $\times$ p-prime components for $p \ge w$

$\implies$ has a generating set of size $O\bigl(|m|/|w|\bigr)$
$\implies$ bit-size $O\bigl(|m|^2/|w|\bigr) = O\bigl(|z|\bigr)$

Finish the argument

Theorem

VTC^0 proves $IMUL$

Proof: VTC^0 proves

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

$\Longrightarrow$ by induction on w:

$$w^6|z|^3 \le z \to Cyc[z,w]$$

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

- 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
- E. Jeřábek: Iterated multiplication in VTC^0, arXiv:2011.03095 [cs.LO]

References (cont'd)

- 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