Iterated multiplication in VTC^0

Emil Jeřábek

August 30, 2021

The complexity class[1] TC^0 is a small subclass of P (polynomial time) which has fundamental significance in that it describes the complexity of *elementary arithmetic operations*. In detail, the integer operations $+$, $\cdot$, and the relation $<$, are all TC^0-computable; while $+$ (and $-$) and $<$ are already in the subclass $\mathrm{AC}^0 \subsetneq \mathrm{TC}^0$, the operations $\cdot$ (and $/$) are *complete* for TC^0 under AC^0 Turing reductions, thus TC^0 is the smallest class with reasonable closure properties that includes them.

The basic arithmetical theory corresponding to TC^0 is the Zambella-style two-sorted bounded arithmetic VTC^0, defined by Nguyen and Cook [10], or equivalently (modulo $RSUV$-isomorphism) the Buss-style one-sorted theory Δ^b_1-CR, introduced earlier by Johannsen and Pollett [9]. (In [8], they also defined a simpler theory C^0_2, which is a $\forall\exists\Sigma^b_1$-conservative extension of Δ^b_1-CR.) We may interpret provability in VTC^0 (or Δ^b_1-CR) as a formalization of *feasible reasoning* about the elementary arithmetic operations $+$, $\cdot$, and $<$: what properties of these operations can be proved using only concepts whose complexity does not exceed that of $+$, $\cdot$, $<$ themselves?

Apart from the elementary integer operations, TC^0 includes iterated addition $\sum_{i<n} X_i$ and iterated multiplication $\prod_{i<n} X_i$; the corresponding operations in $\mathbb{Q}$, $\mathbb{Q}(i)$, or other number fields, as well as polynomial rings and other related structures; and using iterated addition and multiplication, it can compute approximations of real-valued or complex-valued analytic functions given by sufficiently nice power series, such as $\sqrt[k]{X}$, exp (on not-too-large arguments), log, trigonometric and inverse trigonometric functions, etc.

While TC^0-computability of $+$, $-$, $<$, and $\sum_{i<n} X_i$ follows easily from the definition, TC^0-computability of $\prod_{i<n} X_i$ and $/$ (as well as the more fancy functions just mentioned that depend on these) is a difficult result with a long history: first, Beame, Cook, and Hoover [2] proved (in present terminology)

[1] Originally, TC^0 was introduced as a nonuniform circuit class by Hajnal et al. [4], but here we always mean the DLOGTIME-uniform version of the class, which is known to give a robust notion of "fully uniform" TC^0 with several equivalent definitions across various computation models (cf. [1]). Likewise for AC^0. For simplicity, we will conflate the language class TC^0 with the corresponding function class FTC^0.

that / and $\prod_{i<n} X_i$ (and X^n with n given in unary) are TC^0 Turing-reducible to each other, and that they are all computable in P-*uniform* TC^0; a decade later, Chiu, Davida, and Litow [3] proved that / and $\prod_{i<n} X_i$ are in L-uniform TC^0, and in particular, in L itself; finally, Hesse, Allender, and Barrington [5] proved the optimal result that both functions are in fully uniform TC^0.

On the arithmetical side, Jeřábek [6] considered the extension of VTC^0 by an axiom *IMUL* postulating the totality of iterated multiplication, and showed that it is unexpectedly powerful: apart from integer division, it can formalize a certain form of root approximation algorithms for constant-degree polynomials, which implies that it includes the theory of quantifier-free induction *IOpen* for binary numbers. More generally, $VTC^0 + IMUL$ proves the *RSUV* translation of induction and minimization for Σ^b_0 formulas in Buss's language.

This leaves us with the basic question whether VTC^0 proves *IMUL*, i.e., whether the soundness of the algorithm from [5] can be proved in VTC^0. (This problem was first explicitly posed in [10], where it is attributed to A. Atserias.)

The iterated multiplication algorithm from [5] is not really just a single algorithm—the argument has a complex structure with several interdependent parts. But what truly makes its formalization challenging is that the analysis of the algorithms suffers from multiple "chicken or egg" problems (which came first, the chicken or the egg?):

- The proof of soundness of the main Chinese remainder reconstruction procedure heavily relies on $\prod_{i<n} X_i$ and /: e.g., it refers to the product of primes from the CRR basis. However, in VTC^0, we need the soundness of CRR reconstruction to define such iterated products in the first place.

- The analysis of the modular powering algorithm refers to various modular powers, and even relies on Fermat's little theorem. However, the latter cannot be stated, let alone proved, without having a means to define modular powering in the first place.

- The reduction of $\prod_i a_i \bmod p$ (p prime) to modular powering relies on cyclicity of the groups of units $(\mathbb{Z}/p\mathbb{Z})^\times$, which is notoriously difficult to prove in bounded arithmetic. (What makes this a chicken-or-egg problem is that the cyclicity of $(\mathbb{Z}/p\mathbb{Z})^\times$ is in fact provable in $VTC^0 + IMUL$.)

In this talk, we outline how to overcome these difficulties, leading to a proof of *IMUL* in VTC^0. Besides the fundamental significance of the fact that the basic TC^0 theory can formalize the soundness of TC^0 algorithms for the elementary operation / as well as $\prod_{i<n} X_i$, we obtain as a consequence that the results of [6] apply to VTC^0: i.e., VTC^0 proves (the *RSUV* translations of) induction and minimization for Σ^b_0 formulas, and similarly for Δ^b_1-*CR* and C^0_2.

We also obtain a side result of independent interest: there is a Δ_0 definition of modular powering $a^r \bmod m$ whose defining recurrence is provable in the theory $I\Delta_0 + WPHP(\Delta_0)$.

The talk is based on the paper [7].

References

[1] David A. Mix Barrington, Neil Immerman, and Howard Straubing, *On uniformity within NC^1*, Journal of Computer and System Sciences 41 (1990), no. 3, pp. 274–306.

[2] Paul W. Beame, Stephen A. Cook, and H. James Hoover, *Log depth circuits for division and related problems*, SIAM Journal on Computing 15 (1986), no. 4, pp. 994–1003.

[3] Andrew Y. Chiu, George I. Davida, and Bruce E. Litow, *Division in logspace-uniform NC^1*, RAIRO – Theoretical Informatics and Applications 35 (2001), no. 3, pp. 259–275.

[4] András Hajnal, Wolfgang Maass, Pavel Pudlák, Mário Szegedy, and György Turán, *Threshold circuits of bounded depth*, Journal of Computer and System Sciences 46 (1993), no. 2, pp. 129–154.

[5] William Hesse, Eric Allender, and David A. Mix Barrington, *Uniform constant-depth threshold circuits for division and iterated multiplication*, Journal of Computer and System Sciences 65 (2002), no. 4, pp. 695–716.

[6] Emil Jeřábek, *Open induction in a bounded arithmetic for* TC^0, Archive for Mathematical Logic 54 (2015), no. 3–4, pp. 359–394.

[7] ———, *Iterated multiplication in VTC^0*, arXiv:2011.03095 [cs.LO], 2020, `https://arxiv.org/abs/2011.03095`.

[8] Jan Johannsen and Chris Pollett, *On proofs about threshold circuits and counting hierarchies* (*extended abstract*), in: Proceedings of the 13th Annual IEEE Symposium on Logic in Computer Science, 1998, pp. 444–452.

[9] ———, *On the Δ_1^b-bit-comprehension rule*, in: Logic Colloquium '98: Proceedings of the 1998 ASL European Summer Meeting held in Prague, Czech Republic (S. R. Buss, P. Hájek, and P. Pudlák, eds.), ASL, 2000, pp. 262–280.

[10] Phuong Nguyen and Stephen A. Cook, *Theories for TC^0 and other small complexity classes*, Logical Methods in Computer Science 2 (2006), no. 1, article no. 3, 39 pp.