Basic analytic functions in VTC^0

Emil Jeřábek*

Institute of Mathematics, Czech Academy of Sciences

One of the basic themes in proof complexity is a loose correspondence between weak theories of arithmetic and computational complexity classes. If a theory T corresponds to a class C, it usually means that on the one hand, T can reason with C-concepts in the sense that it proves induction, comprehension, minimization, or similar schemata for formulas expressing predicates from C; on the other hand, provably total computable functions of T of suitable syntactic shape are C-functions. We may interpret this situation as a formalization of *feasible reasoning*. Here, we consider a natural concept X, and we ask what properties of X can be proved in an efficient manner while only using reasoning with concepts whose complexity does not exceed that of X itself; if C is a class that adequately describes the complexity of X, and T an arithmetical theory corresponding to C, we can approximate this form of feasible reasoning about X simply by provability in T. (This idea goes back to Parikh [9] and Cook [1].)

In this talk, we will be interested in feasible reasoning with the elementary integer arithmetic operations $+, \cdot, \leq$. Their computational complexity is captured by the class TC^0 (a small subclass of P): all the operations are computable in TC^0, and $\cdot$ is TC^0-complete under a suitable notion of reduction. Many other related functions are computable in TC^0 as well: iterated addition $\sum_{i<n} x_i$ and multiplication $\prod_{i<n} x_i$, division with remainder, the corresponding arithmetical operations in $\mathbb{Q}$, $\mathbb{Q}(i)$, number fields, or polynomial rings, and approximations of analytic functions such as log or sin defined by sufficiently nice power series. Here, the TC^0-computability of $\prod_{i<n} x_i$ and other above-mentioned functions that depend on it is a difficult result with a long history, finally settled by Hesse, Allender, and Barrington [2].

The theory of bounded arithmetic corresponding to TC^0 is the theory Δ^b_1-*CR* of Johannsen and Pollett [7], or equivalently (up to $RSUV$-isomorphism), the two-sorted theory VTC^0 introduced by Nguyen and Cook [8].

*Supported by grant 19-05497S of GA ČR. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840.

This talk will showcase several exhibits of provability in VTC^0, based on [3, 4, 5, 6]:

- VTC^0 can do iterated multiplication by formalizing a variant of the algorithm from [2].
- VTC^0 proves induction for open formulas (*IOpen*), and even for translations of Σ^b_0 formulas of Buss, using a formalization of TC^0 root approximation algorithms for constant-degree polynomials.
- VTC^0 can formalize basic properties of approximations of elementary analytic functions (exp, log, trigonometric functions); in a more convenient setup, these functions can be defined on topological completions of models of VTC^0.

References

[1] Stephen A. Cook, *Feasibly constructive proofs and the propositional calculus*, in: Proceedings of the 7th Annual ACM Symposium on Theory of Computing, 1975, pp. 83–97.

[2] 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.

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

[4] ———, *Iterated multiplication in* VTC^0, Archive for Mathematical Logic (2022), published online, `https://doi.org/10.1007/s00153-021-00810-6`.

[5] ———, *Basic analytic functions in* VTC^0, 2022, in preparation.

[6] ———, *Models of* VTC^0 *as exponential integer parts*, 2022, envisaged.

[7] Jan Johannsen and Chris Pollett, *On the* Δ^b_1*-bit-comprehension rule*, in: Logic Colloquium '98, Proceedings (S. R. Buss, P. Hájek, and P. Pudlák, eds.), ASL, 2000, pp. 262–280.

[8] 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.

[9] Rohit Parikh, *Existence and feasibility in arithmetic*, Journal of Symbolic Logic 36 (1971), no. 3, pp. 494–508.