Towards theories for positive polynomial time and montone proofs with extension

Anupam Das*

University of Copenhagen
anupam.das@di.ku.dk

Monotone computation

Informally, we consider a computation 'monotone' if it does not use the 'negation' operation. The most well-known example of this phenomenon is the case of Boolean circuits without negation, i.e. over the basis $\{\bot, \top, \vee, \wedge\}$, often called *monotone circuits*, which are fundamental objects of study in circuit complexity.

The subject of *uniform* monotone computation is much less studied. To this end Grigni and Sipser initiated a line of work in [11,10], while Lautemann, Schwentick and Stewart proposed several definitions of the 'positive' polynomial-time predicates which they showed coincide [14,15]. In recent work, [9], we proposed a function algebra characterising the *positive polynomial-time functions* by 'uniformising' Cobham's characterisation of the (non-monotone) polynomial-time functions [4].

Monotone proofs

Working in the setting of the (propositional) sequent calculus, we call a proof *monotone* if the $\neg$ symbol does not occur in it. Namely the system *MLK* is defined just as Gentzen's *LK* but over the basis $\{\bot, \top, \vee, \wedge\}$. In their seminal work [1], Atserias, Galesi and Pudlàk showed that tree-like *MLK* quasipolynomially simulates *LK* over monotone implications. Their proof relies on a formalisation of certain counting arguments and boils down to the existence of monotone formulae for the *threshold* functions whose basic properties have small proofs in *MLK*. This result was recently improved to a polynomial simulation thanks to a combination of rather technical results by various authors, [1,12,2].

One motivation for the present work-in-progress is to explore whether the aforementioned results might be simplified or reformulated via a *logical* approach. Apart from offering a complementary understanding of these results, such research might also shed some light on how to extend the polynomial simulation to tree-like *MLK* or even weaker systems in 'deep inference', whose proof complexity status remain open, cf. [7].

* While conducting this research, the author was supported by a Marie Skłodowska-Curie fellowship, ERC project 753431.

Towards theories for monotone feasible reasoning

In this work-in-progress, we propose to complete the proof complexity theoretic account of *monotone proofs with extension*, by proposing arithmetic theories that formally link them to the positive polynomial time functions. Monotone proofs with extension were proposed by Jeřábek in [13], who showed that they polynomially simulate extended Frege over monotone implications, thanks to natural monotone $\mathbf{AC}^1$-definitions of threshold functions.

Building on [9], we consider a version of Cook's PV (cf. [5]) adapted for monotone polynomial-time. On top of this we build logical theory in such a way that only monotone functions remain definable. The key issue herein, for witnessing arguments, is the case of right-contraction:

$$\frac{\Gamma \Rightarrow \Delta, A, A}{\Gamma \Rightarrow \Delta, A}$$

Such steps translate to *conditionals* at the level of computation, which are inherently non-monotone. To avoid this issue we consider a minimal variant of *intuitionistic logic*, recovering metalogical reasoning while retaining monotonicity of definable functions. We propose a theory mPV_1 such that:

1. The provably total monotone functions of mPV_1 are precisely the positive polynomial-time functions, in the sense of [9].
2. Provable equations of mPV_1 translate to polynomial-size monotone proofs with extension, in the sense of [13].
3. mPV_1 proves a *reflection principle* for monotone proofs with extension.

This work is thematically similar to a previous work, [8], where intuitionistic second-order theories for monotone systems were proposed using the Paris-Wilkie translation. Here we rather consider systems with extension via Cook's translation, in a 'ground-up' approach. As well as additionally giving an associated witnessing result, we manage to avoid the quasipolynomial blowup that occurs in [8] and aim to recover a 'monotone' version of Buss' theory S^1_2 for polynomial-time [3]. With such a theory, it would be interesting to see if logical methods, e.g. as developed in [6], might offer alternative monotone simulations of non-monotone proofs.

References

1. A. Atserias, N. Galesi, and P. Pudlák. Monotone simulations of non-monotone proofs. *J. Comput. Syst. Sci.*, 65(4):626–638, 2002.
2. S. Buss, V. Kabanets, A. Kolokolova, and M. Koucký. Expander construction in VNC^1. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:144, 2016.
3. S. R. Buss. *Bounded arithmetic*, volume 1 of *Studies in Proof Theory*. Bibliopolis, Naples, 1986.

4. A. Cobham. The intrinsic computational difficulty of functions. In *Proc. of the International Congress for Logic, Methodology, and the Philosophy of Science*, pages 24–30. Amsterdam, 1965.
5. S. A. Cook. Feasibly constructive proofs and the propositional calculus (preliminary version). In *Proceedings of the 7th Annual ACM Symposium on Theory of Computing, May 5-7, 1975, Albuquerque, New Mexico, USA*, pages 83–97, 1975.
6. S. A. Cook and A. Urquhart. Functional interpretations of feasibly constructive arithmetic. *Ann. Pure Appl. Logic*, 63(2):103–200, 1993.
7. A. Das. *The Complexity of Propositional Proofs in Deep Inference*. PhD thesis, University of Bath, 2014.
8. A. Das. From positive and intuitionistic bounded arithmetic to monotone proof complexity. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016*, pages 126–135, 2016.
9. A. Das and I. Oitavem. A recursion-theoretic characterisation of the positive polynomial-time functions, 2018. Submitted. `http://www.anupamdas.com/wp/pos-fp/`.
10. M. Grigni. *Structure in monotone complexity*. PhD thesis, 1991.
11. M. Grigni and M. Sipser. Monotone complexity. In *London Mathematical Society Symposium on Boolean Function Complexity*, New York, NY, USA, 1992. Cambridge University Press.
12. E. Jeřábek. A sorting network in bounded arithmetic. *Annals of Pure and Applied Logic*, 162(4):341–355, 2011.
13. E. Jerábek. Proofs with monotone cuts. *Math. Log. Q.*, 58(3):177–187, 2012.
14. C. Lautemann, T. Schwentick, and I. A. Stewart. On positive P. In *IEEE Conference on Computational Complexity '96*, 1996.
15. C. Lautemann, T. Schwentick, and I. A. Stewart. Positive versions of polynomial time. *Inf. Comput.*, 147(2):145–170, 1998.