Circuit satisfiability and solving equations

Paweł M. Idziak

Jagiellonian University, Poland

The talk is intended to present latest achievements in searching structural algebraic conditions a finite algebra $\mathbf{A}$ has to satisfy in order to have a low complexity algorithm that decides if an equation $\mathbf{s}(x_1,\ldots,x_n) = \mathbf{t}(x_1,\ldots,x_n)$, where $\mathbf{s},\mathbf{t}$ are polynomials over $\mathbf{A}$, has a solution in $\mathbf{A}$. In order to get such structural characterization (that is independent of the basic operations of $\mathbf{A}$) we translate this problem to circuit satisfiability $\textsc{Csat}(\mathbf{A})$ over the algebra $\mathbf{A}$.

In this new setting the paper [1] gives such conditions for a very broad class of algebras from congruence modular varieties. In particular it has been shown that if an algebra $\mathbf{A}$ fails to decompose nicely, i.e. into a direct product of a nilpotent algebra and an algebra that essentially is a subreduct of a distributive lattice then $\textsc{Csat}$ for $\mathbf{A}$ (or at least one of its quotients) is NP-complete. And, almost conversely, if $\mathbf{A}$ does decompose nicely (in the above sense), but with the additional assumption that the nilpotent factor is actually supernilpotent, then $\textsc{Csat}(\mathbf{A})$ is in fact in P. Subsequently, in [2] and [3], a polynomial time algorithm has been presented for 2-nilpotent algebras. However in general nilpotent but not supernilpotent algebras had not been put on any side of this borderline.

Very recently we started to fill this nilpotent/supernilpotent gap. The essential difference between this two concepts of nilpotency lies in fact that in supernilpotent algebras there is an absolute bound for the arity of expressible (by polynomials) conjunction. In nilpotent (but not supernilpotent) algebras conjunction-like polynomials of arbitrary arity n do always exist but the known ones are too long to be used to polynomially code NP-complete problems in $\textsc{Csat}$. We split nilpotent algebras into slices that will correspond to the measure how much a nilpotent algebra fails to be supernilpotent. This distance h is determined by the behavior of a multi-ary commutator operation on congruences of $\mathbf{A}$ which is used to define h-step supernilpotent algebras. On the other hand we show that it strictly corresponds to the longest chain of alternating primes hidden in the algebra. Then we show that, under the Exponential Time Hypothesis and Strong Exponential Size Hypothesis (saying that Boolean circuits need exponentially many modular counting gates to produce boolean conjunctions of any arity), satisfiability over these algebras have intermediate complexity between $\Omega(2^{c\log^{h-1} n})$ and $O(2^{c\log^{h} n})$, where $h \geqslant 3$ measures how much a nilpotent algebra fails to be supernilpotent.

Our examples are striking in view of the natural strong connections between circuits satisfiability and Constraint Satisfaction Problem for which the dichotomy had been shown by Bulatov and Zhuk.

idziak@tcs.uj.edu.pl

References

[1] P. M. Idziak and J. Krzaczkowski, Satisfiability in multi-valued circuits, *LICS '18: Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, 2018, pp. 550–558.

[2] P. M. Idziak, P. Kawałek, and J. Krzaczkowski, Expressive Power, Satisfiability and Equivalence of Circuits over Nilpotent Algebras, *43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018)*, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[3] P. Kawałek, M. Kompatscher, and J. Krzaczkowski, Circuit equivalence in 2-nilpotent algebras, preprint arXiv:1909.12256, (2019).