Circuit Complexity aspects of solving equations in finite algebraic structures

Piotr Kawałek[1]
Maria Curie-Sklodowska University in Lublin

For a fixed algebra $\mathbf{A}$, equation satisfiability problem over $\mathbf{A}$ asks whether the given equation $p(\overline{x}) = q(\overline{x})$ has a solution, for a pair of polynomials $p(\overline{x}), q(\overline{x})$ of $\mathbf{A}$. When we consider systems of equations over $\mathbf{A}$ (instead of single equation), the problem is famously equivalent to some finite CSP. However, by restricting number of equations to one, we end up with a problem that can become tractable in polynomial-time (while it was NP-complete beforehand). We discuss recent progress towards characterzing algebras with equation satisfiability problem being in P. We describe problems that, under reasonable assumptions, are NP-intermediate. We also discuss a version of the problem in which $p(\overline{x}), q(\overline{x})$ are represented by multi-valued circuits over $\mathbf{A}$.

In the study, we relate the presented results to some classical results in Circuit Complexity Thoery. We show that providing algorithms for the satisfiability problem over $\mathbf{A}$ is, in fact, strongly related to proving lower bounds for some non-uniform circuit families.

[1]Joint work with Paweł Idziak, Jacek Krzaczkowski, Armin Weiß