On the parameterized complexity of Δ_0 truth

Moritz Müller, University of Passau

Joint work with Yijia Chen and Keita Yokoyama

The classical problem to decide the truth of Δ_0-formulas is

> Δ_0-TRUTH
> *Instance:* $n \in \mathbb{N}$ in unary and a Δ_0-formula $\varphi(x)$.
> *Problem:* $\mathbb{N} \models \varphi(n)$?

Informally speaking, we are interested in instances where $n >> |\varphi|$ where $|\varphi|$ is the length of (a reasonable binary encoding of) φ. This is a natural focus. Classical work of Paris and Dimitracopolous took n to be nonstandard and related the complexity of truth definitions for Δ_0-formulas to the complexity-theoretic hypotheses that the linear time hierarchy LINH or the polynomial time hierarchy PH do not collapse.

We formally realize this focus as it is usually done in parameterized complexity and consider $|\varphi|$ as a parameter:

> p-Δ_0-TRUTH
> *Instance:* $n \in \mathbb{N}$ in unary and a Δ_0-formula $\varphi(x)$.
> *Parameter:* $k := |\varphi|$.
> *Problem:* $\mathbb{N} \models \varphi(n)$?

The straightforward algorithm decides p-Δ_0-TRUTH in space $f(k) \cdot \log n$ for some computable function f. Can it be decided in space $f(k) + O(\log n)$? Wilkie verified this for the subproblem of quantifier free input formulas. Can nondeterministic space $f(k) + O(\log n)$ be attained? Can it be decided in time $f(k) \cdot n^{O(1)}$, i.e., is it in FPT? Maybe with nondeterminism, i.e., is it in para-NP? At present all these questions are wide open.

We show that such *upper bounds* imply *lower bounds* in classical complexity theory. Notably,

Theorem 1. *If* p-Δ_0-TRUTH $\in$ para-NP, *then* NE $\not\subseteq$ LINH.

The proof has two ingredients. The first is an analysis of the parameterized halting problem

p-HALT	
Instance:	$n \in \mathbb{N}$ in unary and a nondeterministic Turing machine $\mathbb{M}$.
Parameter:	$|\mathbb{M}|$, the size of $\mathbb{M}$.
Problem:	Does $\mathbb{M}$ accept the empty input in at most n steps?

The work of Chen and Flum reveiled some surprising connections between the parameterized complexity of this problem and central questions of descriptive complexity as well as proof complexity.

The second ingredient is an unconditional lower bound:

Theorem 2. p-Δ_0-TRUTH $\notin$ para-AC^0.

Here, para-AC^0 is the parameterized version of (dlogtime-uniform) AC^0. The proof is based on diagonalization or, more specifically, the undefinability of truth. Furthermore, it relies on the classical result of descriptive complexity that, roughly speaking, equates AC^0 and first-order logic with built-in arithmetic.

As a corollary we get some information about the long standing open problem whether $I\Delta_0$ proves the MRDP theorem. Namely,

Theorem 3. *If $I\Delta_0$ proves MRDP for small numbers, then* $\mathsf{NE} \not\subseteq \mathsf{LINH}$.

That $I\Delta_0$ *proves* MRDP *for small numbers* means that the equivalence of a given Δ_0-formula $\varphi(\bar{x})$ to some Diophantine formula is proved in $I\Delta_0$ for all $\bar{x}$ of logarithmic order. Model-theoretically, the equivalence holds in any $I\Delta_0$-model for all $\bar{x}$ from the initial segment of numbers x such that 2^x exists, while proof-theoretically, we allow an $I\Delta_0$-proof to use exponentiation, but only once. Such limited use of exponentiation is well studied in bounded arithmetic.