I am interested in Mathematical Logic and Complexity Theory. In particular, in Proof Complexity.

Specifying further, in my research I focus on proof complexity of circuit lower bounds. This research area was initiated by Razborov [23] who formulated the natural proofs barrier as an unprovability of circuit lower bounds in theories of bounded arithmetic. Such unprovability results correspond to lower bounds on lengths of proofs in propositional proof systems which in turn constitute Cook’s program to the separation of NP and coNP. Unfortunately, Razborov’s unprovability result as well as other existing proof complexity lower bounds work only for very weak proof systems. A generalization of Razborov’s approach led to the notion of proof complexity generators [1,11,24] which were introduced in a hope to obtain lower bounds against strong proof systems like Frege - standard textbook systems for propositional logic.

**Razborov’s conjecture.** Razborov [24] conjectured that any suitable NW-generator forms a good proof complexity generator in the sense that the tautologies stating the existence of elements outside its range require superpolynomial-size proofs in Frege systems assuming $P/poly$ is hard on average for $NC^1$. Some specific NW-generators were, in fact, proven to be hard for weak proof systems like Resolution [1]. In [17] I showed that Razborov’s conjecture holds for all proof systems with the so called feasible interpolation property, including e.g. Resolution and Cutting Planes. This also implied a conditional hardness of circuit lower bounds in such systems. Unfortunately, the feasible interpolation property is unlikely to hold in strong proof systems like Frege [4,13].

**Feasible provability of $P \neq NP$.** In order to approach stronger systems I later focused on a first-order version of the problem independently motivated by the question whether $P \neq NP$ holds in a strict feasibly constructive sense. In [19] I showed that theories weaker than Cook’s theory $PV$, which formalizes p-time reasoning [7], cannot prove $SAT \notin P/poly$ under standard hardness assumptions. This was obtained by showing a conditional impossibility of witnessing $P/poly$ lower bounds by weaker computational models. Unfortunately, this strategy cannot show the unprovability of $SAT \notin P/poly$ in $PV$ because standard hardness assumptions imply that $SAT \notin P/poly$ can be witnessed by a p-time algorithm. Such witnessing algorithms yield feasible/succinct propositional formulas encoding circuit lower bounds. These were proposed in [18] as possibly better candidate hard tautologies than formulas from Razborov’s conjecture.

**QBF Frege system.** An intuitionistic bounded arithmetic $S^1_2$, developed by Buss, Cook and Urquhart [5,8], captures the notion of feasibly constructive mathematics more closely than Cook’s $PV$. In [3] we showed that a QBF extension of Frege system, introduced by Beyersdorff, Bonacina and Chew [2], presents a QBF equivalent of intuitionistic $S^1_2$. In fact, it possesses even more constructive properties and can be seen as a formalization of ultrafinitism.

**Feasible Complexity Theory.** Complementing lower bounds, in [20] I aimed at supporting the thesis that a lot of Complexity Theory is derivable in feasible fragments of arithmetic. I formalized the PCP theorem in the theory $PV$. Further, with Müller [14], we proved $AC^0, AC^0[p]$ and monotone circuit lower bounds in a slight extension of $PV$, a theory $APC^1$ formalizing probabilistic p-time reasoning [10].

In [14] we thus formally strengthened constructivity of the existing circuit lower bounds. While already Razborov [22] showed the provability of $AC^0, AC^0[p]$ and monotone circuit

---

1This result is based on a theorem of Krajíček [12] giving a model-theoretic evidence for Razborov’s conjecture and remains the strongest unprovability result concerning $P \neq NP$ in first-order theories. However, it does not yield propositional lower bounds. In propositional setting the strongest lower bound on the hardness of $SAT \notin P/poly$ is due to Razborov [24].
lower bounds in $PV$, we showed the provability of their succinct formulation - in which one is not given the whole truth-table of a hard function but only its polynomially big part or its defining formula. In fact, we gave a succinct version of natural proofs against $AC^0[p]$ with proofs in a propositional proof system known as $WF$. This result was also motivated by an observation [14,21] pointing out that the ability to prove succinct circuit lower bounds implies the ability to learn properties of Boolean functions$^2$.

**Hardness magnification.** The mentioned proposal from [18] suggests to investigate succinct formulas expressing $SAT \notin P/poly$ which are exponentially harder than the truth-table formulas expressing $SAT \notin P/poly$. In [14] I expanded this approach by observing that if the truth-table formulas encoding a polynomial circuit lower bound require superlinear size proofs in $AC^0$-Frege systems, then succinct formulas encoding the same polynomial circuit lower bound require $(NC^1)$-Frege proofs of superpolynomial size [14, implicit in Proposition 4.14]. Since $AC^0$-Frege lower bounds are known this suggests a way for attacking Frege lower bounds.

Proposition 4.14 [14] inspired Oliveira and Santhanam [15] to develop an analogous strategy in circuit complexity, termed *hardness magnification*. They showed that if an average case version of the minimum circuit size problem MCSP is hard for superlinear-size circuits, then $P \neq NP$. Strikingly, their strategy overcomes the natural proofs barrier of Razborov and Rudich [25]. In [16] I proved that if a worst-case version of the minimum circuit size problem MCSP is hard for circuits of superlinear size, then $P \neq NP$. Further, by a lower bound of Hirahara-Santhanam [9], the same version of MCSP is hard for formulas of subquadratic size. Since the gap between magnification theorems and known lower bounds is generally relatively small, this raises the hope that closing it is within our reach.

References


$^2$This observation is very direct, in fact, essentially trivial, as opposed to the sophisticated theorem of Carmosino, Impagliazzo, Kabanets and Kolokolova [6] which established a canonical connection between lower bounds and learning algorithms.


