Research Statement

Ján Pich

October 2021

I am interested in mathematical logic and complexity theory. In particular, in proof complexity of circuit lower bounds.

Background. Proving lower bounds on size of circuits computing explicit boolean functions is one of the most fundamental problems in the theory of computation, underlying questions such as the P versus NP problem. *Circuit lower bounds* have been, however, notoriously difficult to prove. This led to the development of a theory of formal barrier results. A prominent attempt to understand the complexity of circuit lower bounds was made with the discovery of the natural proofs barrier of Razborov and Rudich [30], which ruled out many potential proof methods. The possibility that circuit lower bounds could present even the limits of logical reasoning was investigated by Razborov [28], who used natural proofs to derive the unprovability of circuit lower bounds in certain theories of bounded arithmetic. Such unprovability results correspond to lower bounds on lengths of proofs in propositional proof systems, which in turn represent the Cook-Reckhow program towards the separation of NP and coNP - proving that there is no propositional proof system with p-size proofs of all tautologies is equivalent to $\mathsf{NP} \neq \mathsf{coNP}$. Unfortunately, Razborov's unprovability result as well as other existing *proof complexity lower bounds* work only for very weak theories resp. proof systems.

I. Feasible complexity theory

Razborov's conjecture. Razborov's investigation of proof complexity of circuit lower bounds formed a part of the motivation for the development of a theory of proof complexity generators [1, 13, 29], which was introduced in a hope to obtain lower bounds against strong proof systems like Frege - standard textbook systems for propositional logic. Razborov [29] conjectured that any suitable Nisan-Wigderson (NW) generator forms a good proof complexity generator in the sense that tautologies stating the existence of elements outside its range require superpolynomial-size proofs in Frege systems assuming $\mathsf{P/poly}$ is hard on average for NC^1. Some specific NW-generators were, in fact, proven to be hard for weak proof systems like Resolution, cf. [1]. In [20] 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, cf. [15, 4].

Feasible provability of $\mathbf{P \neq NP}$. In order to approach stronger systems I later focused on a first-order version of the problem independently motivated by the question whether $\mathsf{P} \neq \mathsf{NP}$ holds in a strict feasibly constructive sense. In [22] I showed that theories weaker than Cook's theory PV_1, which formalizes p-time reasoning [8], cannot prove $\mathsf{SAT} \notin \mathsf{P/poly}$ under standard hardness assumptions[1]. This was obtained by showing a conditional impossibility of witnessing $\mathsf{P/poly}$ lower bounds by weaker computational models. Unfortunately, this strategy cannot show the unprovability of $\mathsf{SAT} \notin \mathsf{P/poly}$ in PV_1 because standard hardness assumptions imply that $\mathsf{SAT} \notin \mathsf{P/poly}$ can be witnessed by a p-time algorithm. On the positive side, such witnessing algorithms yield feasible/succinct propositional formulas encoding circuit lower bounds. These were proposed in [21] as possibly better candidate hard tautologies than formulas from Razborov's conjecture.

[1] This result is based on a theorem of Krajíček [14] giving a model-theoretic evidence for Razborov's conjecture and remains the strongest unprovability result concerning $\mathsf{P} \neq \mathsf{NP}$ in first-order theories. However, it does not yield propositional lower bounds. In propositional setting the strongest lower bound on the hardness of $\mathsf{SAT} \notin \mathsf{P/poly}$ is due to Razborov [29].

Formalizations of complexity theory. Complementing lower bounds, in [23] 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_1. Further, with Müller [16], we proved $\mathsf{AC}^0, \mathsf{AC}^0[p]$ and monotone circuit lower bounds in a slight extension of PV_1, a theory APC_1 formalizing probabilistic p-time reasoning [11]. In [16] we thus formally strengthened constructivity of the existing circuit lower bounds. While already Razborov [27] showed the provability of $\mathsf{AC}^0, \mathsf{AC}^0[p]$ and monotone circuit lower bounds in PV_1, 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 $\mathsf{AC}^0[p]$ with proofs in a propositional proof system known as WF.

QBF Frege system. An intuitionistic bounded arithmetic S^1_2, developed by Buss, Cook and Urquhart [5, 9], captures the notion of feasibly constructive mathematics more closely than Cook's PV_1. 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 posseses even more constructive properties and can be seen as a formalization of *ultrafinitism.*

II. Hardness magnification

Hardness magnification frontiers. The above-mentioned proposal from [21] suggests to investigate succinct formulas expressing $\mathsf{SAT} \notin \mathsf{P/poly}$ which are exponentially harder than the truth-table formulas expressing $\mathsf{SAT} \notin \mathsf{P/poly}$. In [16] 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 [16, 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 [16] inspired Oliveira and Santhanam [18] 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 $\mathsf{P} \neq \mathsf{NP}$. Strikingly, their strategy seemed to overcome the natural proofs barrier of Razborov and Rudich. In [19] I proved that even if a worst-case version of the minimum circuit size problem MCSP is hard for circuits of superlinear size, then $\mathsf{P} \neq \mathsf{NP}$. Further, by a lower bound of Hirahara-Santhanam [10], the same version of MCSP is hard for formulas of subquadratic size. Since the gap between magnification theorems and known lower bounds is (from several perspectives) seemingly negligible, this raised the hope that closing it was within our reach.

Beyond natural proofs & the locality barrier. In [7] we formally supported the intuition that hardness magnification overcomes the natural proofs barrier: we proved that hardness magnification is in certain cases inherently nonnaturalizable. On the other hand, in [7] we identified a new *locality barrier* which explains why direct adaptations of the existing lower bounds do not yield strong complexity separations via hardness magnification.

III. Learning algorithms from circuit lower bounds

Learning algorithms from witnessing. Formalizations from [16] were partially motivated by an observation [24, 16] pointing out that the ability to prove succinct circuit lower bounds implies the ability to learn properties of boolean functions. In [25] I developed this connection further and showed that efficient algorithms witnessing errors of p-size circuits (analogous to the witnessing of circuit lower bounds in bounded arithmetic) are equivalent to the existence of efficient learning algorithms for $\mathsf{P/poly}$. This extended the natural proofs barrier and provided a new characterization of learning algorithms. A similar theorem was previously proved by Carmosino, Impagliazzo, Kabanets and Kolokolova [6], who established an equivalence between learning algorithms and lower bounds defined in terms of natural proofs. Moreover, in [25]

I gave an alternative proof of a surprising theorem of Oliveira and Santhanam [17] showing that learning algorithms can be sped up in a generic way. The learning speedup can be also interpreted as a hardness magnification theorem avoiding the locality barrier.

Learning algorithms versus automatability. One of the central notions in proof complexity is the concept of proof-search algorithms formalized by the notion of automatability: a proof system P is automatable if there is an algorithm finding P-proofs of each tautology ϕ in p-time w.r.t. the shortest P-proof of ϕ. Extending the work of Razborov [28], Krajíček [12] and Carmosino et al. [6], in [26] we showed that for every sufficiently strong, well-behaved proof system P such as WF or set theory ZFC (interpreted as a proof system for proving tautologies), if P proves efficiently some sufficiently strong circuit lower bound, then efficient P-provability of efficient learnability of $\mathsf{P/poly}$ is equivalent to efficient P-provability of automatability of P on tautologies encoding circuit lower bounds. This shows that in the context of metamathematics it is possible to establish a conditional equivalence between central concepts of complexity theory which we do not know to establish otherwise.

References

[1] Alekhnovich M., Ben-Sasson E., Razborov A.A., Wigderson A.; *Pseudorandom generators in propositional proof complexity*; SIAM Journal on Computing, 34(1):67-88, 2004.

[2] Beyersdorff O., Bonacina I., Chew. L.; *Lower bounds: From circuits to QBF proof systems*; ITCS, 2016.

[3] Beyersdorff O., Pich J.; *Understanding Gentzen and Frege systems for QBF*; LICS, 2016.

[4] Bonet M.L., Domingo C., Gavalda R., Maciel A., Pitassi T.; *Non-automatizability of bounded-depth Frege proofs*; Computational Complexity, 13:47-68, 2004.

[5] Buss S.R.; *The polynomial hierarchy and intuitionistic bounded arithmetic*; In Proc. Structure in Complexity Theory Conference, 77-103, 1986.

[6] Carmosino M., Impagliazzo R., Kabanets V., Kolokolova A.; *Learning algorithms from natural proofs*; CCC, 2016.

[7] Chen L., Hirahara S., Oliveira I.C., Pich J., Rajgopal N., Santhanam R.; *Beyond natural proofs: hardness magnification and locality*; ITCS, 2020.

[8] Cook S.A.; *Feasibly constructive proofs and the propositional calculus*; STOC, 1975.

[9] Cook S.A., Urquhart A.; *Functional interpretations of feasibly constructive arithmetic*; Annals Pure and Applied Logic, 63(2):103-200, 1993.

[10] Hirahara S., Santhanam R.; *On the average-case complexity of MCSP and its variants*; CCC, 2017.

[11] Jeřábek E., *Approximate counting in bounded arithmetic*; Journal of Symbolic Logic, 72(3), 2007.

[12] Krajíček J.; *Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic*; Journal of Symbolic Logic, 66(2):457-486, 1997.

[13] Krajíček J.; *On the weak pigeonhole principle*; Fundamenta Mathematicae, 170(1-3):123-140, 2001.

[14] Krajíček J.; *On the proof complexity of the Nisan-Wigderson generator based on a hard NP∩coNP function*; Journal of Mathematical Logic, 11(1):11-27, 2011.

[15] Krajíček J., Pudlák P.; *Some consequences of cryptographical conjectures for S_2^1 and EF*; Information and Computation, 140(1):82-94, 1998.

[16] Müller M., Pich J.; *Feasibly constructive proofs of succinct weak circuit lower bounds*; Annals of Pure and Applied Logic, 2019.

[17] Oliveira I.C., Santhanam R.; *Conspiracies between learning algorithms, circuit lower bounds, and pseudorandomness*; CCC, 2017.

[18] Oliveira I.C., Santhanam R.; *Hardness magnification for natural problems*; FOCS, 2018.

[19] Oliveira I.C., Pich. J., Santhanam R.; *Hardness magnification near state-of-the-art lower bounds*; CCC, 2019.

[20] Pich J.; *Nisan-Wigderson generators in proof systems with forms of interpolation*; Mathematical Logic Quarterly, 57(4), 2011.

[21] Pich J.; *Complexity Theory in Feasible Mathematics*; PhD thesis, Charles University in Prague, 2014.

[22] Pich J.; *Circuit lower bounds in bounded arithmetics*; Annals of Pure and Applied Logic, 166(1), 2015.

[23] Pich J.; *Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic*; Logical Methods in Computer Science, 11(2), 2015.

[24] Pich J.; *Mathesis Universalis*; Literis 2016.

[25] Pich J.; *Learning algorithms from circuit lower bounds*; preprint, 2020.

[26] Pich J., Santhanam R.; *Learning algorithms versus automatability of Frege systems*; preprint, 2021.

[27] Razborov A.A.; *Bounded Arithmetic and Lower Bounds in Boolean Complexity*; Feasible Mathematics II, pp. 344-386, 1995.

[28] Razborov A.A; *Unprovability of Lower Bounds on the Circuit Size in Certain Fragments of Bounded Arithmetic*; Izvestiya of the Russian Academy of Science, 59:201-224, 1995.

[29] Razborov A.A; *Pseudorandom Generators Hard for k-DNF Resolution and Polynomial Calculus*; Annals of Mathematics, 181(2):415-472, 2015.

[30] Razborov A.A, Rudich S.; *Natural Proofs*; Journal of Computer and System Sciences, 55(1):24-35, 1997.