Feasibly constructive proofs of succinct weak circuit lower bounds

Moritz Müller Ján Pich

Kurt Gödel Research Center for Mathematical Logic
University of Vienna
{moritz.mueller,jan.pich}@univie.ac.at

Abstract

It comes as no surprise when a complexity theorist, being concerned with the algorithmic hardness of computational tasks, starts wondering whether the notorious conjectures in the field are in some sense 'hard' to prove. Can one show first that existing proofs of partial results are 'simple' in some sense and second that such 'simple' reasoning is insufficient to settle the conjecture under consideration?

It is unclear whether there exists a good general notion of simplicity of proofs, already Hilbert asked for it in his 24th problem [14]. From a complexity theoretic perspective, however, one would naturally like to grade the complexity of proofs by the computational complexity of the concepts and constructions appearing in it. This is the viewpoint of "Bounded Reverse Mathematics" taken in the monograph [5, p.xiv] on proof complexity. In particular, the bounded arithmetic theory PV_1, going back to Cook [4], can be viewed as being restricted to polynomial time computable concepts and constructions. In Cook's own words, "if one believes that all feasibly constructive arguments can be formalized in PV_1, then it is worthwhile seeing which parts of mathematics can be so formalized." [4, p.96] As it turns out, a large part of contemporary complexity theory can be carried out in PV_1 or slight extensions of it.

An example of particular interest is the apparently difficult task to prove circuit lower bounds for explicit functions. We consider three seminal results in the area:

(a) The Switching Lemma and a size lower bound for bounded depth circuits computing the parity function [1, 6, 7].

(b) Razborov and Smolensky's method of approximations by low degree polynomials and a size lower bound for bounded depth circuits containing modulo p counting gates computing the modulo q counting function [11, 13].

(c) Razborov's method of approximations and a size lower bound for monotone circuits deciding the clique problem [10].

We refer to [3] or [2] for surveys. We give proofs of (a)-(c) that are in a certain sense feasibly constructive.

0.1 Circuit lower bounds in PV_1

We continue Razborov's search for the "right fragment capturing the kind of techniques existing in Boolean complexity at present" [12, p.344]. He argued "that V^1_1 is exactly the required theory. By this I mean in particular that it proves all lower bounds mentioned above *and, moreover, these formal proofs are obtained in a very natural and straightforward way*[1]." [12, p.376] V^1_1 is a second-order variant of PV_1.[2] Proofs of (a)-(c) formalize in V^1_1 and partly even below: (a) in a theory corresponding to NC via a now famous new proof of Håstad's Switching Lemma [7], and (c) in a theory corresponding to circuits of a certain sublinear depth (see [12] for precise statements).

We want to talk about circuit lower bounds for computational problems like the satisfiability problem SAT, and therefore blurr the distinction between an explicit function $\mathsf{Q} : \{0,1\}^* \to \{0,1\}$ and the computational problem $\{x \mid \mathsf{Q}(x) = 1\}$.

It is not straightforward to formalize a size s circuit lower bound

$$\textit{For every circuit } C \textit{ of size } s \textit{ there exists } y \in \{0,1\}^n \textit{ such that } C(y) \neq \mathsf{Q}(y). \qquad (1)$$

in bounded arithmetic which lacks exponentiation. Razborov treats circuits as sets and inputs as numbers. In his words, this captures "the common practice in the area which tends to treat Boolean inputs and functions separately, as two different kinds of objects".[12, p.375] We stick to the first-order setting, and PV_1 instead V^1_1. There Razborov's formalization assumes 2^{2^n} exists which allows to code C by a number even for s exponential in n. Note that the whole $\mathtt{t}$ruth $\mathtt{t}$able of Q on $\{0,1\}^n$ is coded by a number. Denote[3] this formula by $\mathsf{LB}_{\mathsf{tt}}[\mathsf{Q}]$.

In Krajíček's words, this formalization "differs from the one usually accepted in bounded arithmetic [...] in which all combinatorial objects (inputs, circuits,...) are coded at the same level (by sets in the case of V^1_1) while (Boolean) functions are identified with definable classes". An according *succinct* formalization, assumes only that 2^n exists. It allows only to consider polynomial size bounds $s \leqslant n^k$ for some constant $k \in \mathbb{N}$. Denote

[1] Emphasis added by the authors. Additionally to our (a)-(c), Razborov refers to lower bounds for monotone formulas.

[2] More precisely, the *RSUV*-isomorphism (see e.g. [9, Theorem 5.5.13]) translates V^1_1 into S^1_2 which is Σ^b_1-conservative over PV_1.

[3] All notions and notations are defined later.

such a formula by $\mathsf{LB}[\mathsf{Q}]$. More precisely, we have a formula $\mathsf{LB}[\mathsf{C},\mathsf{Q}](C,s,n,N)$ expressing a size s lower bounds for circuits C from the class C; it uses an auxiliary variable N and supposes $n=|N|$.

The assumption that 2^n is the length of some number, intuitively means that the whole truth-table of Q on $\{0,1\}^n$ is considered a feasible object. The succinct LB-formalization assumes only that n is the length of some number. Intuitively, this means that only the size $\leqslant n^k$ of the circuit is considered feasible. For size bound $s=n^k$, the theory PV_1 is in some sense exponentially stronger w.r.t. $\mathsf{LB}_{\mathsf{tt}}[\mathsf{Q}]$ than it is w.r.t. $\mathsf{LB}[\mathsf{Q}]$. We now ask again for the right fragment to capture circuit lower bounds, this time in the succinct LB-formalization. This is the topic of the present paper.

0.2 Succinct circuit lower bounds in APC_1

As a candidate we put forward Jeřábek's theory APC_1 of approximate counting [8] which is a slight extension of PV_1 by the (*dual* or) *surjective* weak pigeonhole principle for polynomial time functions. While PV_1 formalizes polynomial time reasoning, APC_1 formalizes probabilistic polynomial time reasoning. Recalling Razborov's quote, we aim at formalizations as close as possible to the original arguments. Some changes are, however, needed.

For (a) we formalize in APC_1 an argument close to Furst, Saxe and Sipser's [6] based on probabilistic reasoning with random restrictions. Probabilities are estimated using Jeřábek's notion of approximate counting, and doing so requires the construction of feasible surjections witnessing these estimations. That APC_1 proves the succinct formalization of (a) has already been shown by Krajíček [9, Theorem 15.2.3] formalizing Razborov's abovementioned alternative proof of Håstad's Switching Lemma. His proof is different and of independent interest.

Letting AC^0_d denote the set of circuits of depth $\leqslant d$, and PARITY denote the set of numbers whose binary expansion contains an odd number of ones, the formal statement reads as follows:

Theorem 0.1. *Let $d,k\in\mathbb{N}$. There is $n_0\in\mathbb{N}$ such that the theory APC_1 proves*

$$n_0\leqslant n\to \mathsf{LB}[\mathsf{AC}^0_d,\mathsf{PARITY}](C,n^k,n,N).$$

Razborov and Smolensky's method for (b) typically requires to consider exponentially large objects such as the ring of n-variate polynomials over some finite field. In order to simulate the argument in APC_1 we compromise slightly on our aspired succinctness and assume a fixed quasi-polynomial function of n to be a length (formally expressed by "$\in$ *Log*" below). As a consolation prize, this scaled down n allows to formulate and prove a lower bound for $s=n^{\log n}$ instead just n^k. Secondly, polynomials approximating formulas are not constructed directly but instead we construct succinct descriptions of them by arithmetical circuits.

Letting $\mathsf{AC}^0_d[p]$ denote the set of circuits of depth $\leqslant d$ with MOD_p-gates, and MOD_q denote the set of numbers whose binary expansion contains a number of ones divisible by q, the formal statement reads as follows:

Theorem 0.2. *Let $d \in \mathbb{N}$ and $p \neq q$ be primes. There is $n_0 \in \mathbb{N}$ such that the theory* APC_1 *proves*

$$n_0 \leqslant 2^{\log^{9d} n} \in Log \to \mathsf{LB}[\mathsf{AC}^0_d[p], \mathsf{MOD}_q](C, n^{\log n}, n, N).$$

The proof [3] of the monotone circuit lower bound (c) is formalizable in APC_1 without essential change. However, here (and also in the proof of Theorem 0.2), we actually need to reason not directly in APC_1 but in a suitably conservative extensions.

Letting MC denote the set of all monotone circuits, and k-CLIQUE the set of (numbers coding) graphs with a clique of size k, the formal statement reads as follows:

Theorem 0.3. *Let $d, k \in \mathbb{N}$. There is $n_0 \in \mathbb{N}$ and a rational $0 < \epsilon < 1$ such that the theory* APC_1 *proves*

$$n_0 \leqslant n \to \mathsf{LB}[\mathsf{MC}, k\text{-}\mathsf{CLIQUE}](C, n^{\epsilon\sqrt{k}}, n, N).$$

Actually, we prove a more general statement allowing for non-constant k.

We remark that a proof of $\mathsf{LB}[\mathsf{C}, \mathsf{Q}]$ in APC_1 gives a probabilistic polynomial time algorithm that witnesses errors of small C-circuits trying to decide Q.

References

[1] Ajtai, M.; Σ^1_1 *formulae on finite structures*, Annals of Pure and Applied Logic, 24 (1): 1-48, 1983.

[2] Arora S., Barak B.; *Computational Complexity: A Modern Approach*, Cambridge University Press, 2009.

[3] Boppana R.B., Sipser M.; *The complexity of finite functions*, van Leeuwen J. (ed.), Handbook of theoretical computer science (vol. A), pp. 758-804, Elsevier, 1990.

[4] Cook S.A.; *Feasibly constructive proofs and the propositional calculus*, Proceedings of the 7th Annual ACM Symposium on Theory of Computing (STOC), ACM Press, pp. 83-97, 1975.

[5] Cook S.A., Nguyen P.; *Logical Foundations of Proof Complexity*, Cambridge University Press, 2010.

[6] Furst M., Saxe J. B., Sipser M.; *Parity, circuits, and the polynnomial-time hierarchy*; Mathematical systems Theory, 17: 13-27, 1984.

[7] Håstad J.; *Computational limitations for small depth circuits*, PhD thesis, M.I.T. press, 1986.

[8] Jeřábek E.; *Approximate counting in bounded arithmetic*, Journal of Symbolic Logic, 72: 959-993, 2007.

[9] Krajíček J.; *Bounded arithmetic, propositional logic, and complexity theory*, Cambridge University Press, 1995.

[10] Razborov A.A.; *Lower bounds on the monotone complexity of some Boolean functions*, Doklady Akademii Nauk SSSR, 281 (4), pp. 798-801 (in Russian), 1985.

[11] Razborov A.A.; *Lower bounds on the size of bounded depth networks over a complete basis with logical addition* (in Russian), Matematicheskie Zametki, 41(4): 598-607, 1987.

[12] Razborov A.A.; *Bounded arithmetic and lower bounds in Boolean complexity*, Feasible Mathematics II, pp. 344-386, 1995.

[13] Smolensky R.; *Algebraic methods in the theory of lower bounds for Boolean circuit complexity*, Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC), pp. 77-82, 1987.

[14] Thiele R.; *Hilbert's twenty-fourth problem.* American Mathematical Monthly, January 2003.