Book review by Moritz Müller, Universität Passau, Germany.
March 7, 2023

Author: Jan Krajíček, Charles University, Prague
Book Title: Proof Complexity
Publisher: Cambridge University Press
Series: Encyclopedia of Mathematics and its Applications
Print publication year: 2019
ISBN: 9781108416849

The book presents the field of proof complexity in its full breadth and depth. It starts historically tracing proof complexity to foundational questions of mathematical logic, and ends with a question about its nature: "what are the intrinsic reasons that some formulas are hard to prove? Can the proof complexity of some formulas be traced to the computational complexity of associated computational tasks?" (p.477)

The central goal of proof complexity is to prove lower bounds to the size of proofs in various (propositional) proof systems. To date no superpolynomial lower bounds are known for standard textbook systems, called *Frege*, given by finitely many inference rules. However, already lower bounds for weak proof systems are well-motivated from a computer science perspective for their application to algorithm analysis. Systems around Resolution are related to SAT solvers, algebraic systems like Nullstellensatz or Polynomial Calculus to ideal membership algorithms, and semi-algebraic systems like Sherali-Adams or Sum-of-Squares to linear or semidefinite programming. While the combinatorially inclined research in this direction form the "rudiments from which proof complexity can grow" (p.473), it uses somewhat ad hoc methods tackling specific tautologies and proof systems. The book aims to presents "proof complexity as a whole entity rather than as a collection of various topics held together loosely by few notions. The frame that supports it is logic." (p.4)

The gem of proof complexity is a subexponential lower bound on the size of bounded-depth Frege proofs of tautologies expressing the pigeonhole principle. Being *bounded-depth* means that the proof operates with formulas of some fixed $\wedge/\vee$-alternation rank. This goes back to Ajtai 1988 and "opened completely new vistas, showing that proof complexity is part of a much larger picture and that it does not need to be just a finitary proof theory" (p.184). Ajtai gave a forcing-type construction of an expansion of a cut of a nonstandard model M of true arithmetic by a bijection between $n+1$ and n for some nonstandard n in such a way that induction for bounded formulas is preserved. This implies the proof lower bound due to the correspondence of bounded-depth Frege and arithmetics with bounded induction.

That a bounded arithmetic T *corresponds* to a proof system P means that (1) P has short proofs of propositional translations of universal consequences of T and (2) T proves the soundness of P. By (1), lower bounds on P-proofs imply independence from T, and this explains a central motivation from mathematical logic (p.37): understanding independence for universal arithmetical sentences. (2) implies that every T-provably sound proof system is *simulated* by P in the sense that its proofs can be efficiently translated to P-proofs. This implies that lower bounds on P imply the consistency of $\mathsf{NP} \neq \mathsf{coNP}$ with T, and thus

explains a central motivation from computer science (p.476): such a consistency counts towards the truth of the conjecture. Indeed, while bounded arithmetics are not foundational for the whole of mathematics, they are for computational complexity theory in that they formalize a large part of it.

The book has four parts. Part I (Basic Concepts) introduces the proof systems mentioned above and many more and develops their basic theory. Part II (Upper Bounds) is devoted to the correspondence and starts with Chapter 8 presenting the one for bounded-depth Frege with a clear model-theoretic argument. This is extended to systems with modular counting or threshold connectives, and also to weak systems around Resolution. Chapter 12 gives an elegant presentation of the correspondence of Cook's PV and Buss' S^1_2 with Extended Frege based on Herbrand's theorem. Beautiful applications in Chapter 11 are quasipolynomial upper bounds for weak pigeonhole principles in $R(\log)$, and subexponential bounded-depth simulations of Frege. A point stressed (p.204) is that natural theories should be based on prevailing reasoning principles identified in mathematical logic, like induction, collection, or choice principles.

Part III (Lower Bounds) starts with weak systems around Resolution. Aiming at general results and techniques, it treats the hardness of arbitrary infinity axioms and their relativizations, and a *proof complexity generator* $g : \{0,1\}^n \to \{0,1\}^m$ (with $m > n$): the hardness to prove that a given $y \in \{0,1\}^m$ is outside the range of g; here, g is given by an $m \times n$ matrix A over $\mathbb{F}_2$ with certain combinatorial expansion properties. Chapter 15 proves Ajtai's theorem on the propositional level via k-evaluations. Chapter 16 gives Polynomial Calculus degree lower lower bound for weak pigeonhole principles and sketches a Sum-of-Squares degree lower bound for the abovementioned generator. Chapters 17 and 18 cover *feasible interpolation*: given two disjoint NP problems, this property allows to efficiently construct separating circuits (or monotone ones, or formulas, or span programs, or what) from proofs of disjointness (per input length). Thus, this property reduces proof lower bounds to computational hardness (of the separation problem), and actually gives a win-win situation: its failure implies hardness of proof search.

Part IV (Beyond Bounds) is less detailed than the rest and surveys approaches to strong proof systems like Extended Frege. In particular, Chapter 19 presents the approach via proof complexity generators, Chapter 20 sketches two forcing perspectives, and Chapter 21 discusses finite consistency statements. The final Chapter 22 gives a structural overview of the whole field and ends with the question from the beginning of this review.