STEPHEN COOK and PHUONG NGUYEN. ***Logical foundations of proof complexity.*** Perspectives in Logic. Cambridge University Press, New York, 2010, 15 + 479 pp.

It is no secret that computational complexity theory has its origins deeply rooted in mathematical logic. By this we mean not only that the original definitions and early results were inspired by concepts from classical computability theory, but also that some of the most influential results in the area have a deep logical meaning. For example, one of the important early results in the area, the Cook–Levin Theorem, states that the satisfiability problem for propositional logic is **NP**-complete or, dually, that the problem of detecting propositional tautologies is **co-NP**-complete. One immediate consequence of this is that, unless **NP** = **co-NP**, the standard textbook proof systems for propositional logic are not *polynomially bounded*: although they are complete in the sense that all tautologies have proofs, they are not efficiently so in the sense that not all tautologies have short (i.e., polynomial-size) proofs. Perhaps surprisingly, this straight consequence of the hypothesis that **NP** $\neq$ **co-NP** is not known to hold unconditionally except for some weak proof systems. This takes us to an active field of research called propositional proof complexity, one of whose aims is to classify the relative strength of the existing propositional proof systems, with the goal of understanding and exploiting this sort of incompleteness phenomenon at the level of the propositional logic.

The subject of ***Logical foundations of proof complexity*** revolves precisely around the theme of propositional proof complexity. It does so by developing a general framework by which a given complexity class $\mathcal{C}$ gets associated both a propositional proof system $\mathcal{P}$ and a corresponding weak theory of arithmetic $\mathcal{T}$. The definable functions in $\mathcal{T}$ are precisely those computable in $\mathcal{C}$. The bounded theorems of $\mathcal{T}$ translate into tautologies with polynomial-size proofs in $\mathcal{P}$. And a sort of converse to this last statement holds too since the theory $\mathcal{T}$ proves the soundness of $\mathcal{P}$. Thus, in the language of the previous paragraph, the proof system $\mathcal{P}$ is not only complete, but efficiently so, with respect to the propositional translations of bounded theorems in $\mathcal{T}$.

At this point an example will help and will also illustrate one of the constructions in the book. Let **PH** be the class of languages in the polynomial-time hierarchy. In logic terms, these are the sets of binary strings that are described by a bounded first-order formula in a two-sorted language, with one sort for natural numbers and one sort for binary strings indexed by these numbers, equipped with the basic arithmetic language 0, 1, $+$, $\times$ and $\leq$ on numbers, the length function $|\cdot|$ on strings, and the bit indicator relationship $\in$ between indices and strings.

The propositional proof system associated to **PH** is called **G**. This is an extension of the standard propositional sequent calculus to deal with quantified Boolean formulas. To be precise, **G** adds the following two rules to the usual propositional rules for the sequent calculus:

$$\frac{A(p), \Gamma \longrightarrow \Delta}{(\exists x)(A(x)), \Gamma \longrightarrow \Delta} \qquad \frac{\Gamma \longrightarrow \Delta, A(B)}{\Gamma \longrightarrow \Delta, (\exists x)(A(x))},$$

where in the first rule p is a free variable that does not appear in the lower sequent, and in the second $A(B)$ is the result of replacing each free occurrence of x in A by B.

The weak theory of arithmetic associated to **PH** is called $\mathbf{V}^\infty$. This is a two-sorted theory in the first-order language described above, with basic axioms for 0, 1, $+$, $\times$, $\leq$, $|\cdot|$, and $\in$, and the comprehension axiom for each bounded first-order formula. More precisely, if $\phi(x)$ is a bounded first-order formula, perhaps with additional free variables, the comprehension axiom for ϕ states that, for every length y, the binary string of length y that has ones precisely at the positions $z < y$ for which $\phi(z)$ holds, exists. In symbols:

$$(\exists X, |X| \leq y)(\forall z < y)(z \in X \leftrightarrow \phi(z)).$$

Alternatively, in this case one may replace the comprehension axiom scheme by the axiom scheme of induction for bounded formulas and obtain the same theory.

One of the main points of the book is that this intimate *ménage a trois* between a complexity class, its associated propositional proof system, and its associated weak theory of arithmetic can be arranged naturally and in a uniform way across all the spectrum of classical complexity classes in the neighborhood of **P**. The example we gave corresponds precisely to the upper end of this spectrum **PH**, but the book actually starts the development of the theory at the bottom end of the spectrum $\mathbf{AC}^0$. The studied complexity classes include:

$$\mathbf{AC}^0 \subseteq \mathbf{AC}^0(2) \subseteq \mathbf{ACC} \subseteq \mathbf{TC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2 \subseteq \mathbf{P} \subseteq \mathbf{PH}.$$

The declared motivation for developing this theory is to set up the background to start a program that the authors call "bounded reverse mathematics", in analogy with the ongoing program of reverse mathematics put forward by Harvey Friedman and others. In bounded reverse mathematics one would look for the weakest theory of bounded arithmetic in which the most important theorems that are relevant to computer science can be proved. The book includes several such examples from the recent literature in this area, such as feasible proofs of the Cayley–Hamilton Theorem of linear algebra, or a graphical version of the Jordan Curve Theorem.

The treatment of bounded arithmetic in the book is somewhat unusual in that it takes the two-sorted language with one sort for numbers and one sort for strings as the preferred language for the theory. This setup has its origins in Buss' celebrated thesis ***Bounded arithmetic***, Bibliopolis, 1986, for complexity classes beyond **PH**, and following Zambella *Notes on polynomially bounded arithmetic*, ***The Journal of Symbolic Logic***, vol. 61 (1996), no. 3, pp. 942–966, the authors adapt the method to **PH** and below. Of course one could say that the difference is merely cosmetic and that no real gain is obtained by considering two-sorted theories instead of one-sorted theories as in Peano arithmetic, but the point that the authors make is that their treatment makes the subject both closer and more accessible to mainstream computational complexity theory, where the string plays an important role as the basic representation device for inputs to Turing machines and, more importantly, to Boolean circuits. Indeed the outcome of the theory is an elegant setup with a clean language that, for example, avoids the introduction of *smash functions* and *rounded halving* from Buss' theories S^i_2 and T^i_2. One nice consequence of this is that the formulas that describe the languages in the standard complexity classes become syntactically quite close to those used in the capturing results of descriptive complexity theory *à la* Immerman in ***Descriptive complexity***, Springer, 1999. As a matter of fact, the subject of the book can almost be thought as developing the proof theory that is missing from the descriptive complexity approach to understanding complexity classes through logic.

Before we close this review, a comparison to Krajíček's book ***Bounded arithmetic, propositional logic and computational complexity***, Cambridge University Press, 1995, is in order. Both books cover the topics of bounded arithmetic and propositional proof complexity through the lens of computational complexity. However, one of the declared goals of Cook and Nguyen's monograph, which is to prepare the ground for developing the program of bounded reverse mathematics, is barely touched in Krajíček's book, and in the reverse direction, one of the main focuses in Krajíček's book, which is to prove independence results for bounded arithmetic theories and super-polynomial lower bounds for concrete propositional proof systems, is barely covered in Cook and Nguyen's monograph. In this respect, the two books complement each other quite well. A piece of useful information for the student of the subject is that one consequence of this difference in focus is that the book under review makes a more accessible text for learning the basic theory from the start, yet at a good pace.

Albert Atserias

Universitat Politècnica de Catalunya, Barcelona, Spain. atserias@lsi.upc.edu.

Entry for the Table of Contents: