JAN KRAJÍČEK. ***Forcing with Random Variables and Proof Complexity.*** London Mathematical Society Lecture Note Series, vol. 232. Cambridge University Press, 2011. xvi+247 pp.

Bounded arithmetic has many intimate connections with feasible computational complexity and questions related to the P versus NP problem. Indeed, the original definition of bounded arithmetic, in the form of $I\Delta_0$, by R. Parikh was motivated by connections with linear space computation. It was subsequently recognized that the Δ_0-definable sets are exactly the sets computable in the linear time hierarchy (a subclass of linear space, but not known to be a proper subclass). The early research by C. Dimatracopoulos, J. Paris, A. Wilkie, and others found many connections between bounded arithmetic and computational complexity. With the definition of the bounded arithmetic theories PV by S. Cook, and S^i_2 and T^i_2 by this reviewer, and many subsequent works, the connections between bounded arithmetic and computational complexity became central. In these theories, the core motivations were to characterize the provably total functions of logical theories in terms of computational complexity: the complexity classes considered are feasible, or near-feasible, such as log space, polynomial time, non-deterministic polynomial time, polynomial space, etc.

Bounded arithmetic is also closely connected to propositional proof complexity. There are two primary connections. First, J. Paris and A. Wilkie showed that certain proofs in bounded arithmetic can be translated into polynomial size, or quasipolynomial size, constant depth propositional proofs. A different kind of correspondence between PV (and S^1_2) and extended Frege proof systems was found by S. Cook. Extended Frege proofs are the usual "textbook style" proof systems based on modus ponens with proof length measured in terms of number of inferences. Under both translations, propositional proofs turn out to be non-uniform versions of proofs in theories of bounded arithmetic. This is analogous to the way that Boolean circuits are essentially non-uniform versions of algorithms. This has been a useful analogy in some ways, as concepts and tools from complexity theory have been used to establish lower bounds in proof complexity. In other ways, however, it has been a frustrating analogy, as there has been less success in establishing lower bounds on proof complexity than in proving lower bounds on circuit complexity. A particularly important and tantalizing problem of this type is to prove a super-polynomial lower bound on the lengths of proofs of constant depth Frege systems for a Boolean language enlarged with unbounded fanin parity gates or, more generally, gates for modular counting mod p. There is hope that this might be achievable as there are lower bounds, due to R. Smolensky and A. Razborov, on the expressive power of formulas in these proof systems for fixed primes p.

It has been a long-standing goal to use model-theoretic techniques for theories of arithmetic to prove lower bounds in computational complexity or proof complexity. Influential early work includes M. Ajtai's work giving lower bounds on the complexity of constant depth formulas for counting: this, along with the work of Furst-Saxe-Sipser was later improved by Yao-Håstad style switching lemmas. Ajtai's work suggested that forcing methods might allow lower bounds to be proved by model-theoretic methods. Another intriguing early work giving model-theoretic constructions of models of arithmetic was the restricted ultraproduct construction of nonstandard models of arithmetic by S. Kochen and S. Kripke; however, this never found application to bounded arithmetic.

The goal of the book under review is to develop model-theoretic methods to attack problems in proof complexity and in bounded arithmetic. One of the main goals was to establish lower bounds for constant depth Frege proofs with parity gates or gates for modular counting mod p. Although this remains an open problem, the book describes

a new set of tools for creating models of bounded arithmetic with forcing, and contains many new techniques that are not available elsewhere in the literature.

The first five chapters of the book introduce a forcing method for constructing Boolean-valued models of arithmetic. (Five chapters may sound like a lot, but the chapters are quite short, and five chapters takes one only up to page 46.) The forcing construction starts with an $\aleph_1$-saturated model $\mathcal{M}$ of true arithmetic, and a set $\Omega \in \mathcal{M}$, and selects a set F of functions $f : \Omega \mapsto |\mathcal{M}|$. This forms the first-order universe of a structure; measure-theoretic considerations, using Loeb's measure, give a Boolean valuation for sentences over this structure. After the basic definitions and theorems, there are some striking results on how quantifiers can be witnessed (approximately) with elements of F. The fifth chapter concludes by extending these definitions to second order structures.

The next four short chapters develop models of arithmetic created from functions f which are computable with small decision trees (these functions are called "rudimentary"), establish induction and comprehension principles, and discuss a general framework for quantifier elimination. The subsequent three chapters develop a "tree model" that corresponds to models built from functions that are computable with a special type of Boolean decision trees. This incorporates a novel and ingenious construction: the functions are computed by decision trees which are stratified into k levels for some natural number k, plus have small rudimentary decision trees at the bottom level. (Krajíček does not use the terminology "stratified", however.) This is a crucial innovation that makes it possible exploit the switching lemma and a lower bound for parity to prove quantifier elimination properties and to give a witnessing theorem for the second order bounded arithmetic theory V^0_1. The theory V^0_1 can be viewed as an analogue of the theory $I\Delta_0(R)$ where R is a second order predicate.

Chapters 13-16 take the reader to page 98, and give constructions of models of bounded arithmetic based on functions computable by decision trees based on evaluation of low degree (subpolynomial degree) polynomials mod 2. Algebraic models of arithmetic are defined using these algebraically defined functions and a first-order mod 2 quantifier is introduced. Then, with the aid of the Razborov-Smolensky construction, induction, comprehension, and elimination of quantifiers are proved to hold, a witnessing theorem is proved, and an independence result is obtained.

Chapters 17-22 next address the question of lower bounds for constant depth proofs of the pigeonhole principle. For constant depth Frege systems, exponential lower bounds are known already due to work by M. Ajtai, by S. Bellantoni, T. Pitassi, and A. Urquhart, by J. Krajíček, by T. Pitassi, P. Beame, and R. Impagliazzo, and by J. Krajíček, P. Pudlák, and A. Woods based on random restrictions and switching lemmas. These chapters give a model-theoretical construction for nonstandard models where the pigeonhole fails using decision trees with nodes that query values of the pigeonhole principle. (Here again, Krajíček uses the technique of adding small rudimentary circuits to the leaves of the decision tree.) These models, along with a reflection principle and an appeal to the switching lemma, then establish exponential lower bounds for constant depth Frege proofs. Chapter 22 discusses the prospects for establishing superpolynomial lower bounds for proofs of the pigeonhole principle in constant depth Frege systems augmented with parity gates.

The next chapters take up several short topics about independence results for fragments of bounded arithmetic, oracles, and pseudorandom number generators. It is particularly striking how well the model-theoretic approach can accommodate pseudorandom number generators in a natural way. The final part of the book takes up the subject of τ-tautologies, also known as "proof complexity generators". The τ-tautologies have

been introduced earlier by Krajíček and independently by M. Alekhnovich, E. Ben-Sasson, A. Razborov and A. Wigderson. These tautologies were inspired in part by the Nisan-Wigderson pseudorandom number generators, and are often conjectured to be examples of tautologies that are hard for strong propositional proof systems such as extended Frege. Chapters 29 and 30 give a survey of prior work on τ-tautologies that can be read independently of the rest of the book. The final chapter then discusses how to formulate some of the central results about τ-tautologies in the model-theoretic forcing framework. There is a technical error in one of the core proofs; however, the applications of the theorem in the second part of the chapter are all correct. Corrections to this part can be found on the book's errata page and a detailed correction in a 2012 preprint by Krajíček entitled *Pseudo-finite hard instances for a student-teaching game with a Nisan-Wigderson generator*.

The book is arranged into very short chapters, which may be a little disconcerting at first, but quickly becomes very comfortable. If nothing else, one feels like one is making good progress in reading through multiple chapters in one sitting. More importantly, the chapter lengths are appropriate for introducing topics and results incrementally.

My overall opinion of the book is highly positive. The book is a research-level exposition of new topics that have not appeared in the literature. It gives a fundamentally new approach to model-theoretic forcing, as well as to independence results in bounded arithmetic and proof complexity. The author's goal for the book was to use these methods to establish new proof complexity lower bounds. This has not yet come to fruition; but nonetheless, the directions are highly intriguing as an new approach for attacking fundamental problems in proof complexity. The first parts of the book should be interesting to anyone working in model theoretic constructions for non-standard models of arithmetic. The book as a whole will be interesting to researchers working on the common interface between bounded arithmetic, model theory, and proof complexity.

Sam Buss

Department of Mathematics, University of California, San Diego, La Jolla, California, USA 92093-0112. sbuss@math.ucsd.edu.

Entry for the Table of Contents:

Jan Krajíček, ***Forcing with Random Variables and Proof Complexity***.

Reviewed by Sam Buss xxx