Review of[12]
Boolean Function Complexity: Advances and Frontiers
by Stasys Jukna
Springer, 2012
600 pages, \$85.00, HARDCOVER

Review by
William Gasarch gasarch@cs.umd.edu
University of Maryland, College Park, 20742

1 Introduction

(**Disclaimer:** I was one of the proofreaders for two chapters of this book.)

In 1986 David S. Johnson published a survey in his NP-Completeness Column called *Computing with One Hand Tied Behind Your Back*. To quote it

... in the circuit complexity model the best lower bound known for a problem in NP has only increased from $2.5n$ *to* $3n$ *since [G&J] (Garey and Johnson) was published seven years ago. Many researchers have thus turned their attention to machine models whose computational power is sufficiently limited that super-polynomial lower bounds may be easier to prove. Such a lower bound would imply only that the problem at hand is hard when your machine has one hand tied behind its back, but the techniques and insights developed might eventually be of use in attacking more general models. In any case the mathematics involved offers its own challenges and rewards. This column will cover three popular ways of restricting general Boolean circuit models and the surprising developments that have recently occurred relating to each.*

The three restrictions he is referring to are monotone circuits, bounded depth circuits, and bounded width branching programs.

This line of research has produced many many results since 1986. So many that its hard (at least for me) to keep track of what lower bounds are known in which models. Fortunately it is not hard for Stasys Jukna! He has written a book that explains (with proofs) most of the progress made in this area.

The book is well written. This is partially because he put the book out on the web asking people to read some of the chapters *ahead of time*. Hence the final product is very polished. Note also that many of the results he is proving were only in conference form with incomplete proofs, or in journals that were behind paywalls, or in Russian. Hence his book does a great service.

Putting that aside, has the program of proving lower bounds on weak models been a success? There are two answers: YES and NO. This depends on what the goals are. There are many results where we have fairly close upper and lower bounds on concrete problems in a simple model of computation. For example, the upper and lower bounds on how many gates you need to compute PARITY with depth k (a constant) match (up to certain factors). We have pinned down the complexity of PARITY in that model! If that is an end in itself then the answer is YES. If it was meant to be a stepping stone to resolving P vs NP then the answer is (so far) NO.

The mathematics used in the book is mostly combinatorics, though clever combinatorics. There are some Fourier transforms and some Linear Algebra; however, there are large parts that can be read without too much background. And the background you do need for the rest isn't that hard to pick up.

The field of Boolean Function Complexity is still quite active. Hence there is a website associated to the book that reports when open problems in the book are solved. It is at

`http://www.thi.informatik.uni-frankfurt.de/~jukna/boolean/index.html`.

2 Summary

The book is in six Parts: The Basics (2 chapters), Communication Complexity (3 chapters), Circuit Complexity (6 chapters), Bounded Depth Circuits (3 chapters), Branching Programs (4 chapters), and Fragments of Proof Complexity (2 chapters). There is also an Epilogue[13] and an Appendix that includes some of the Mathematical background needed.

2.1 Part 1: The Basics

This chapter has a few theorems of interest but is mostly setting up theorems about Boolean Functions to be used later. Here is a theorem of interest that is proven:

(Schnorr 1974) The minimal number of AND and OR gates in an AND-OR-NOT circuit for computing PARITY of n variables is at least $3n - 3$.

Is this still the best known? No. There is a table of many known lower bounds at the end of Chapter 1 and it states that the PARITY of n variables is known to take exactly $4n - 4$ gates- upper and lower bound, due to Redkin. Johnson's comment above about $3n$ being the best known lower bounds for general circuits is no longer true! Its now $4n$. I do not know whether to be happy or sad.

The theorems stated here to be used later have to do with approximating circuits by polynomials. Most of the theorems are rather technical to state; however, here is one:

(Nisan and Szegedy, 1994) Let f be a Boolean function on n variables. Let $deg_\epsilon(f)$ be the lowest degree of a polynomial $p : \mathsf{R}^n \rightarrow \mathsf{R}$ such that, for all $x \in \{0,1\}^n$, $|f(x) - p(x)| \leq \epsilon$. Then $deg_{1/k}(OR_n) = O(\sqrt{n} \ln k)$.

2.2 Part 2: Communication Complexity

There are two ways to view Communication Complexity. Its original motivation was for lower bounds on a certain model for VLSI. It was later used to obtain lower bounds on circuits, branching programs, data structures, and other models. This is all well and good. But questions about communication complexity can also be studied in their own right, without relation to other models. For example, the fact that the communication complexity of equality is exactly $n + 1$ is interesting even if it has no application[14] to lower bounds in other models.

This book mostly, but not strictly, takes the view of using Communication Complexity in the service of other models. As such this Part has chapters on *Games on Relations* (used for lower bounds on monotone circuits), *Games on 0-1 Matrices* (large lower bounds on these yield large lower bounds for other models), *Multi-Party Games* (used for lower bounds on streaming algorithms and for Branching programs).

2.3 Part 3: Circuit Complexity

I was surprised to find one of the Parts labeled *Circuit Complexity* since not much is known about lower bounds on general circuits. In fact, this Part has chapters on Formulas (circuits of fan-in 2), Monotone Formulas (no NOT gates), Span Programs, Monotone Circuits, and a more speculative chapter entitled *The Mystery of Negation*. And note that Part 4 is on Bounded Depth Circuits.

We state some theorems of interest.

[13] the Epilogue looks like its part of the Proof Complexity Chapter, but it is not

[14] My students find this an odd use of the word "application"

Let ED_n be the function on $n = 2m \log m$ variables that views the variables as m blocks of $2 \log m$ each, and outputs YES iff all of the blocks are distinct. The number of gates needed in a formula for ED_n is $\Theta(n^2/\log n)$. (In this theorem formulas are fan-out-1 circuits with arbitrary gates. That is, the gates can be any Boolean function of the input).
(Raz and Wigderson 1992) Every monotone circuit for determining if a graph (encoded as $\binom{n}{2}$ boolean variables) has a matching with $n/3$ vertices has depth at least $\Omega(n)$.

2.4 Part 4: Bounded Depth Circuits

The first chapter of this section, Chapter 11, is entirely on depth-3 circuits. This reminds me of the quote that *Getting a PhD means learning more and more about less and less until you've written 400 pages on depth 3 circuits.* To be fair, the book only has around 40 pages on depth 3 circuits. Why are depth 3 circuits interesting? The cynical answer is that we prove things about depth 3 circuits because we can. (Depth 4 seems much harder.) Less cynically, depth 3 is the first interesting level and some of the theorems that were first proven for depth 3 were later proven for general bounded depth circuits. Also, in Section 11.1 the authors notes that high lower bounds for depth three circuits imply superlinear lower bounds for non-monotone log-depth circuits.

As an example of the non-cynical attitude, this book has Hastad's proof that any depth 3 circuit for MAJORITY requires $2^{\Omega(\sqrt{n})}$ gates. It is now known that any depth d circuit for MAJORITY requires $2^{\Omega(1/d)}$. However, the earlier result is interesting for two reasons (1) (minor) for the case of $d = 3$ the earlier results is better, and (2) the proof for just the $d = 3$ case uses no machinery. No Hastad Switching Lemma. It can be taught to High School Student (I've done this.) The proof is very enlightening.

The other chapters are about depth d circuits for constant d. The chapter contains the cornerstone result of the field: PARITY not in constant depth, and also not in constant depth with MOD n gates for n a power of a prime. These were well presented. There are also less well known about circuits with arbitrary gates.

2.5 Part 5: Branching Programs

The first chapter on this section is on Decision Trees which are a special case of branching programs. When I hear *Decision Trees* I think *Sorting requires $\Omega(n \log n)$ comparisons* and *ith largest requires $n + (i-1)\log n$ comparisons*. Those results are not here. However, the book is on Boolean Function Complexity (Element Distinctness IS discussed) and, once again, if he included everything that people wanted him to include it would double its weight.

This part also has chapters on General Branching Programs, Bounded Replication BP's (e.g., read-once), and Bounded Time. Barrington's theorem is included.

2.6 Fragments of Proof Complexity

This was my personal favorite chapter. It was perfect in terms of material I wanted to learn and had enough background to learn. I learned about Prover-Delayer games and Tree-resolution, regular resolution, (ordinary) resolution, Cutting plane proofs. I have used this material directly in my research. I can't give it a higher compliment than that.

3 Opinion

This book contains everything YOU want to know about Boolean Function Complexity and, at 600 pages, more. Of more importance, its well written and the topics are well considered. It should not just be on the bookshelf of every complexity theorist— it should be on their desk, open to their favorite section.