MINING CIRCUIT LOWER BOUND PROOFS FOR META-ALGORITHMS

RUIWEN CHEN, VALENTINE KABANETS, ANTONINA KOLOKOLOVA, RONEN SHALTIEL, AND DAVID ZUCKERMAN

Abstract. We show that circuit lower bound proofs based on the method of random restrictions yield non-trivial compression algorithms for “easy” Boolean functions from the corresponding circuit classes. The compression problem is defined as follows: given the truth table of an \( n \)-variate Boolean function \( f \) computable by some unknown small circuit from a known class of circuits, find in deterministic time \( \text{poly}(2^n) \) a circuit \( C \) (no restriction on the type of \( C \)) computing \( f \) so that the size of \( C \) is less than the trivial circuit size \( 2^n/n \). We get non-trivial compression for functions computable by \( \text{AC}^0 \) circuits, (de Morgan) formulas, and (read-once) branching programs of the size for which the lower bounds for the corresponding circuit class are known.

These compression algorithms rely on the structural characterizations of “easy” functions, which are useful both for proving circuit lower bounds and for designing “meta-algorithms” (such as Circuit-SAT). For (de Morgan) formulas, such structural characterization is provided by the “shrinkage under random restrictions” results by Subbotovskaya (Doklady Akademii Nauk SSSR 136(3):553–555, 1961) and Håstad (SIAM J Comput 27:48–64, 1998), strengthened to the “high-probability” version by Santhanam (Proceedings of the Fifty-First Annual IEEE Symposium on Foundations of Computer Science, pp 183–192, 2010), Impagliazzo, Meka & Zuckerman (Proceedings of the Fifty-Third Annual IEEE Symposium on Foundations of Computer Science, pp 111–119, 2012b), and Komargodski & Raz (Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, pp 171–180, 2013). We give a new, simple proof of the “high-probability” version of the shrinkage result for (de Morgan) formulas, with improved parameters. We use this shrink-
age result to get both compression and \#SAT algorithms for (de Morgan) formulas of size about $n^2$. We also use this shrinkage result to get an alternative proof of the result by Komargodski & Raz (Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, pp 171–180, 2013) of the average-case lower bound against small (de Morgan) formulas.

Finally, we show that the existence of any non-trivial compression algorithm for a circuit class $\mathcal{C} \subseteq P/poly$ would imply the circuit lower bound $\text{NEXP} \not\subseteq \mathcal{C}$; a similar implication is independently proved also by Williams (Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, pp 21–30, 2013). This complements the result by Williams (Proceedings of the Forty-Second Annual ACM Symposium on Theory of Computing, pp 231–240, 2010) that any non-trivial Circuit-SAT algorithm for a circuit class $\mathcal{C}$ would imply a superpolynomial lower bound against $\mathcal{C}$ for a language in $\text{NEXP}$.

**Keywords.** Average-case circuit lower bounds, Circuit-SAT algorithms, compression, meta-algorithms, natural property, random restrictions, shrinkage of de Morgan formulas.

**Subject classification.** 03D15.

## 1. Introduction

Circuit lower bounds (proved or assumed) have a number of algorithmic applications. The most notable examples are in cryptography, where a computationally hard problem is used to construct a secure cryptographic primitive (Blum & Micali 1984; Yao 1982), and in the derandomization of probabilistic polynomial-time algorithms, where a hard problem is used to construct a source of pseudorandom bits that can replace truly random ones when simulating an efficient randomized algorithm (Nisan & Wigderson 1994). In both cases, we in fact have an equivalence between the existence of appropriately hard computational problem and the existence of a corresponding algorithmic procedure (appropriate pseudorandom generator), cf. Håstad et al. (1999); Kabanets & Impagliazzo (2004); Nisan & Wigderson (1994).

In both mentioned examples, a circuit lower bound is used in a “black-box” fashion: The knowledge that a lower bound holds