Annals of Pure and Applied Logic 166 (2015) 29–45

Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

www.elsevier.com/locate/apal

Circuit lower bounds in bounded arithmetics

Ján Pich

Department of Algebra, Faculty of Mathematics and Physics, Charles University in Prague, Sokolovska 83, Prague, CZ-186 75, Czech Republic

ARTICLE INFO

Article history:
Received 14 May 2013
Received in revised form 16 August 2014
Accepted 21 August 2014
Available online 2 September 2014

MSC:
03B70
03D15
03F20
68Q17

Keywords:
Bounded arithmetic
Circuit lower bounds

ABSTRACT

We prove that T_{NC^1}, the true universal first-order theory in the language containing names for all uniform NC^1 algorithms, cannot prove that for sufficiently large n, SAT is not computable by circuits of size n^{4kc} where $k \geq 1, c \geq 2$ unless each function $f \in SIZE(n^k)$ can be approximated by formulas $\{F_n\}_{n=1}^{\infty}$ of subexponential size $2^{O(n^{1/c})}$ with subexponential advantage: $P_{x\in\{0,1\}^n}[F_n(x) = f(x)] \geq 1/2+1/2^{O(n^{1/c})}$. Unconditionally, V^0 cannot prove that for sufficiently large n, SAT does not have circuits of size $n^{\log n}$. The proof is based on an interpretation of Krajíček's proof (Krajíček, 2011 [15]) that certain NW-generators are hard for T_{PV}, the true universal theory in the language containing names for all p-time algorithms.

1. Introduction

We investigate the provability of polynomial circuit lower bounds in weak fragments of arithmetic including Buss's [1] theory S_2^1 and its subsystems. These theories are sufficiently strong to prove many important results in Complexity Theory. In fact, they can be considered as formalizations of feasible mathematics. A motivation behind the investigation of these theories is the general question whether the existential quantifiers in complexity-theoretic statements can be witnessed feasibly and so that to derive the witnessing we do not need to exceed feasible reasoning.

Informally, our formalization of n^k-size circuit lower bounds for SAT, denoted by $LB(SAT, n^k)$, has the following form:

$$\forall n > n_0,\ \forall \text{ circuit } C \text{ with } n \text{ inputs and size } n^k\ \exists y, a \text{ such that}$$
$$\big(C(y) = 0 \wedge SAT(y, a)\big) \vee \big(C(y) = 1 \wedge \forall z \neg SAT(y, z)\big)$$

E-mail address: janpich@yahoo.com.

http://dx.doi.org/10.1016/j.apal.2014.08.004
0168-0072/

where n_0, k are constants and $SAT(y, z)$ means that z is a satisfying assignment to the propositional 3CNF formula y, see Section 2.

If S^1_2 proves the formula $LB(SAT, n^k)$ for some constant n_0, then by the usual kind of witnessing, Buss's witnessing [1] or the KPT theorem [12], for any n^k-size circuit with n inputs we can efficiently find a formula of size n on which the circuit fails to solve SAT, see Proposition 4.1.

One could hope to use the p-time algorithm to derive a contradiction with some established hardness assumption, however, Atserias and Krajíček noticed that the same p-time algorithm follows from standard cryptographic conjectures, see Proposition 4.2. (Actually, as discussed in Section 4, a randomized version of such observations appeared already in Buss [3, Section 4.4] and Cook-Mitchell [6, Section 6].) It is an interesting question to ask how strong theories are needed to derive these conjectures.

We do not know how to obtain the unprovability of SAT circuit lower bounds in S^1_2 but we can do it basically for any weaker theory with stronger witnessing properties. We present it in the case of theory T_{NC^1} which is the true universal first-order theory in the language containing names for all uniform NC^1 algorithms.

In theories weaker than S^1_2, like the theory T_{NC^1}, the situation is less natural because they cannot fully reason about p-time concepts. In particular, some universal quantifiers in $LB(SAT, n^k)$ can be replaced by existential quantifiers without changing the intuitive meaning of the sentence. The resulting formula $LB_\exists(SAT, n^k)$ (defined in Section 5) is equivalent to $LB(SAT, n^k)$ in S^1_2 but not necessarily in T_{NC^1}. This is because $LB_\exists(SAT, n^k)$ asserts among other things the existence of computations of general n^k-size circuits, a fact which may not be T_{NC^1}-provable. Therefore, it is essentially trivial to obtain a conditional unprovability of $LB_\exists(SAT, n^k)$ in T_{NC^1}, see Proposition 6.1. This is not the case with the formalization $LB(SAT, n^k)$ and in this sense it is easier and more suitable for the theory T_{NC^1} to reason about $LB(SAT, n^k)$.

The main result of this paper is that we can obtain a conditional unprovability of $LB(SAT, n^k)$ as well. We show that $LB(SAT, n^{4kc})$ for $k \geq 1, c \geq 2$ is unprovable in T_{NC^1} unless each function $f \in SIZE(n^k)$ can be approximated by formulas F_n of size $2^{O(n^{1/c})}$ with subexponential advantage: $P_{x\{0,1\}^n}[F_n(x) = f(x)] \geq 1/2 + 1/2^{O(n^{1/c})}$. The proof will be quite generic. In particular, using known lower bounds on PARITY function, we will obtain that, unconditionally, V^0 cannot prove quasi polynomial ($n^{\log n}$-size) circuit lower bounds on SAT. Here, V^0 is a second-order theory of bounded arithmetic such that its provably total functions are computable in AC^0, see Section 5.

To prove our main theorem we firstly observe that by the KPT theorem [16] the provability of $LB(SAT, n^{4kc})$ in universal theories like T_{NC^1} gives us an $O(1)$-round Student–Teacher (S–T) protocol finding errors of n^{4kc}-size circuits attempting to compute SAT. Then, in particular, it works for n^{4kc}-size circuits encoding Nisan–Wigderson (NW) generators based on any function $f \in SIZE(n^k)$ and any suitable design matrix [17]. The interpretation of NW-generators as p-size circuits comes from Razborov [20]. In this situation we apply Krajíček's proof from [15] showing that certain NW-generators are hard for the true universal theory T_{PV} in the language containing names for all p-time algorithms. This is the main technique we use. We show that it works in our context as well and allows us to use the S–T protocol to compute f by subexponential formulas with a subexponential advantage.

Perhaps the most significant earlier result of this kind was obtained by Razborov [19]. Using natural proofs he showed that theory $S^2_2(\alpha)$ cannot prove superpolynomial circuit lower bounds on SAT unless strong pseudorandom generators do not exist. In fact, his proof works even for sufficiently big polynomial circuit lower bounds. The second-order theory $S^2_2(\alpha)$ is however quite weak with respect to the formalization Razborov used. As far as we know his technique does not imply the unprovability of circuit lower bounds (formalized as here, see Section 2) even for V^0. In this respect, our proof applies to much stronger theories, basically to any theory weaker than S^1_2 in terms of provably feasible functions.

The paper is organized as follows. In Section 2 we formalize circuit lower bounds in the language of bounded arithmetic. In Section 3 we define a conservative extension of the theory S^1_2 denoted $S^1_2(bit)$ and