Improving Strong Exponential Time Hypothesis lower bounds for tree-like resolution

Ilario Bonacina    Navid Talebanfard *

June 4, 2014

Abstract

A Strong Exponential Time Hypothesis lower bound for resolution has the form $2^{(1-\epsilon_k) n}$ for some $k$-CNF on $n$ variables such that $\epsilon_k \to 0$ as $k \to \infty$. For every large $k$ we prove that there exists an unsatisfiable $k$-CNF formula on $n$ variables which requires tree-like resolution refutations of size at least $2^{\left(1-O(\frac{k}{3})\right) n}$. This improves the previous bound of $2^{\left(1-O(\frac{k}{4})\right) n}$ due to Beck and Impagliazzo [BI13].

1 Introduction

The Exponential Time Hypothesis (ETH) formulated by Impagliazzo et al. [IPZ01] states that the SAT problem requires exponential time. This was strengthened by Impagliazzo and Paturi [IP01] to the so-called Strong Exponential Time Hypothesis (SETH) which is stating that the complexity of $k$-SAT grows as $k$ increases and it approaches that of exhaustive search. Of course these are both stronger than $\text{NP} \neq \text{P}$ and hence any proof is far beyond reach at the moment. However, since the running times of the best known $k$-SAT algorithms have the form $2^{(1-\epsilon_k) n}$ where $\epsilon_k \to 0$ as $k \to \infty$ (see e.g. [PPSZ05]), one can ask whether SETH holds for specific algorithms, that is whether there are $k$-CNF instances on which the algorithms run for at least $2^{(1-\epsilon_k) n}$ steps. This turns out to be the case for certain classes of algorithms. For the PPSZ algorithm such a lower bound was proved by Chen et al. [CSTT13]. For DPLL the connection with resolution complexity has been used to derive SETH lower bounds: indeed it is well known that a run of a DPLL algorithm on an unsatisfiable $k$-CNF gives a tree-like refutation, then a tree-like resolution refutation lower bound would imply a DPLL running time lower bound. Pudlák and Impagliazzo [PI00] constructed unsatisfiable $k$-CNF formulas that require tree-like resolution refutations of size

*The author acknowledges support from the Danish National Research Foundation and The National Science Foundation of China (under the grant 61061330540) for the Sino-Danish Center for the Theory of Interactive Computation, within which this work was performed. He also acknowledges support from the Center for Research in Foundations of Electronic Markets (CFEM), supported by the Danish Strategic Research Council
\(\Omega(2^{(1-\epsilon_k)n})\) where \(\epsilon_k = O(1/k^{1/8})\). A recent construction by Beck and Impagliazzo [BI13] improves this to \(\epsilon_k = O(1/k^{1/4})\), where the \(O\) notation is hiding log factors.

In this paper we clarify and simplify the result in [BI13] making a further improvement to \(\epsilon_k = \tilde{O}(1/k^{1/3})\). One can also ask how far this improvement can go. Using the Switching Lemma, we can show that for every unsatisfiable \(k\)-CNF on \(n\) variables, there exists a tree-like resolution of size at most \(2^{(1-\Omega(1/k))n}\). A similar argument was used by Miltersen et al. [MRW05] to prove upper bounds on the size of decision trees for \(k\)-CNF’s. However, we are not aware of any adaptation of this in the proof complexity literature and will hence present a formal account of this observation.

**Relationship with [BI13]** As already said this paper simplifies, clarifies and improves the results from Beck and Impagliazzo [BI13]. They construct unsatisfiable linear systems of equations over \(\mathbb{F}_p\) with a certain kind of expansion property. Then they encode each variable from \(\mathbb{F}_p\) using a sum of roughly \(p^2\) boolean variables and show that with this encoding the linear system requires very large resolution width.

The key property of this representation used in the proof is the following: let \(z = \sum_{i=0}^{p^2} x_i\), where \(x_i\) are boolean variables. Even setting a lot of variables (i.e. \(p^2 - p\)) and still we can obtain all possible \(\mathbb{F}_p\) values for \(z\) setting the remaining variables.

In other words what Beck and Impagliazzo really require is just a disperser for a bit-fixing source that can extract \(\log p\) bits even after many bits in the seed are fixed. Our contribution is thus to show that a random function satisfies this property (Lemma 3.3), and we use this function instead of the sum of \(p^2\) boolean variables used by Beck and Impagliazzo. The arguments of [BI13] still goes through. Beck and Impagliazzo use roughly \(p^2\) bits for each \(\mathbb{F}_p\) variable, whereas with our construction we only require around \(p\) bits and hence we get the improvement.

**Notations** Resolution (RES) is one of the most fundamental and extensively studied proof systems. Using this proof system one can refute unsatisfiable CNF formulas using the following inference rule

\[
\frac{C \lor x \quad D \lor \neg x}{C \lor D},
\]

where \(C\) and \(D\) are disjunctions of literals and \(x\) is some variable. Every resolution refutation induces a DAG in the following way. There is a node for each clause appearing in the proof and every such node will be connected by an edge to the nodes corresponding to the two clauses from which this clause was derived. Given a formula \(\phi\) we denote a RES refutation of \(\phi\) using the notation \(\phi \vdash_{\text{RES}} \bot\).

Tree-like resolution (treeRES) is referred to a subclass of resolution for which the induced DAG is in fact a tree. Let \(C\) be a clause, the width of \(C\), \(|C|\), is the
number of literals appearing in $C$. The resolution width of a formula $\phi$ denoted by $\text{width}(\phi \vdash \bot)$ is the minimum of the width of the largest clause appearing in any resolution refutation of $\phi$, more formally

$$\text{width}(\phi \vdash \bot) := \min_{\pi} \max\{|C| : \phi \vdash_{\pi} \bot \land C \text{ appears in } \pi\}.$$ 

A restriction on a set of variables $X$ is a mapping $\rho : X \rightarrow \{0, 1, \star\}$. We call a variable unfixed by $\rho$ if it is assigned $\star$, and we call it fixed otherwise. The domain of $\rho$, denoted by $\text{dom}(\rho)$, is the set of variables fixed by $\rho$ and $|\rho| := |\text{dom}(\rho)|$. For a function $f$, we define $f|_{\rho}$ to be the function after setting values to the fixed variables according to $\rho$. A random restriction leaving $\ell$ variables free can be obtained as follows: first pick a subset $S$ of the variables of size $|X| - \ell$ uniformly at random, then set each $x \in S$ to either 0 or 1 with equal probability.

## 2 Size upper bound

A decision tree for an unsatisfiable $k$-CNF $\varphi$ is a just a standard decision tree, except that each leaf is labeled with some clause $C$ of $\varphi$ with the condition that the unique (partial) assignment reaching that leaf falsifies $C$. Following Beame [Bea94] we define the canonical decision tree. Given $\varphi = \bigwedge_i C_i$ consider an ordering of the variables and an ordering of the clauses. The canonical decision tree of $\varphi$, denoted by $T(\varphi)$, is inductively defined as follows: look at the first clause $C$ of $\varphi$ according to the ordering and assume $\varphi = C \land \varphi'$. Then do a full decision tree on the variables of $C$ respecting the order of the variables. To the leaf corresponding to the restriction which falsifies $C$, we assign $C$. For other leaves corresponding to restriction $\sigma$, we replace the leaf with $T(\varphi'|\sigma)$. Note that for an unsatisfiable $\varphi$, $T(\varphi)$ corresponds to a tree-like resolution refutation of $\varphi$. Notice that canonical decision trees in [Bea94] are defined for general CNFs. Our main observation, here, is that we can adopt them for the unsatisfiable setting. We need the following variant of the Switching Lemma due to Beame [Bea94].

**Lemma 2.1** (Switching Lemma). Let $\varphi$ be a $k$-CNF on $n$ variables. Let $\rho$ be a random restriction leaving $\ell$ variables free. The probability that the canonical decision tree of $\varphi|_{\rho}$ has depth bigger than $d$ is at most $(\frac{7k\ell}{n})^d$.

**Theorem 2.2.** For any unsatisfiable $k$-CNF $\varphi$ on $n$ variables

$$\text{size}_{\text{tree-RES}}(\phi \vdash \bot) \leq 2^{(1-\Omega(\frac{1}{k}))n}.$$ 

**Proof.** We first note that a tree-like resolution refutation can be thought of as a decision tree in the following sense (see e.g. [BGL13]).

Then we follow an argument due to Miltersen et al. [MRW05] who showed that every $k$-CNF has a decision tree representation of size $2^{(1-\Omega(\frac{1}{k})))n}$ and adjust it to the unsatisfiable setting. We set $\ell = n/14k$. By the Switching
Lemma, for a $1 - 2^{-d}$ fraction of restrictions $\sigma$ with $|\sigma| = n - \ell$, we know that the depth of $T(\varphi|_{\sigma})$ is at most $d$.

Then, by an averaging argument, there exists a set $S \subseteq X$ with $|S| = n - \ell$ such that the same statement holds for all restrictions fixing variables only in $S$. We can construct a decision tree for $\varphi$ as follows: first we do a full decision tree on variables in $S$; then for each leaf with the corresponding restriction $\sigma$, we append $T(\varphi|_{\sigma})$ to that leaf. The number of leaves of this tree is upper bounded by

$$2^d 2^{n-\ell} + 2^{n-\ell-\ell}$$

Hence setting $d := \ell/2$ the number of leaves of the tree is upper bounded by

$$2^{n-\ell} = 2^{(1-\Omega(\frac{1}{k}))n}.$$  Hence we have the required upper bound on the size of the decision tree constructed. \qed

### 3 Size lower bound

Let $v = (v_1, v_2, \ldots)$ be a vector over $\mathbb{F}_p$, then with supp($v$) we denote the indices of $v$ with non-zero entries, that is supp($v$) := \{i : v_i \neq p \ 0\}.

In what follows we construct a system of linear equations over $\mathbb{F}_p$. Let $m$ be the total number of equations, $n$ the total number of variables, and $\{z_1, \ldots, z_n\}$ the variables taking values over $\mathbb{F}_p$. We use the letter $E$, with subscripts, to denote linear equations mod $p$, that is an expression of the form $\sum_j a_j z_j \equiv_p b$, with $a_j, b \in \mathbb{F}_p$. We denote with supp($E$) the set of non-zero $a_j$s. The following definition is essentially the same from [BI13].

**Definition 3.1 ((\(\alpha, \beta, \gamma\))-expander).** Let $\alpha, \beta, \gamma \in \mathbb{R}_{\geq 0}$, $m, n \in \mathbb{N}$ and $\mathcal{E} := \{E_1, \ldots, E_m\}$, a set of $m$ linear equations over $\mathbb{F}_p$. We say that $\mathcal{E}$ is an $(\alpha, \beta, \gamma)$-expander if and only if

$$\forall v \in \mathbb{F}_p^m, \ |\text{supp}(v)| \in [\alpha, \beta] \Rightarrow |\text{supp}(\sum_{i=1}^m v_i E_i)| \geq \gamma.$$  

The next Proposition is just a particular case of Lemma 4.2 from [BI13].

**Proposition 3.2.** There exists a set $\mathcal{E} := \{E_1, \ldots, E_m\}$ of linear equations in $n$ variables over $\mathbb{F}_p$ such that:

1. $\mathcal{E}$ is unsatisfiable,
2. for each $E_i \in \mathcal{E}$ \(|\text{supp}(E_i)| \leq p^2\),
3. $\mathcal{E}$ is $(3n, 3\delta n, (1 - c\theta)n)$-expander, where $\delta = O(1/p)$, $\theta = \tilde{O}(1/p)$ and $c$ is a constant,
4. no subset of at most $3\delta n$ equations from $\mathcal{E}$ is unsatisfiable.

**Lemma 3.3.** Let $\theta$ be the parameter coming from Proposition 3.2. Then there exists a function $g : \{0, 1\}^{\Theta - 1 \log p} \rightarrow \{0, 1\}^{\Theta \log p}$ such that for any restriction $\sigma$ with $|\sigma| \leq \log p$ we have $\text{Im}(g|_\sigma) = \{0, 1\}^{\Theta \log p}$.  

4
Proof. Let \( u := \theta^{-1} \log p \) and \( g \) be random function that assigns to every \( x \in \{0,1\}^u \) a value in \( \{0,1\}^{\log p} \) independently and uniformly at random. We bound the probability that there exist a \( y \in \{0,1\}^{\log p} \) and a restriction \( \sigma \) with \( |\sigma| = \log p \) such that \( y \notin \text{Img}(g|_\sigma) \). This is easily given as follows

\[
\Pr[\exists y, \sigma : y \in \{0,1\}^{\log p}, |\sigma| = \log p, y \notin \text{Img}(g|_\sigma)] \leq p^2 \left( \frac{u}{\log p} \right)^2 (1 - 1/p)^{2u} \leq p^2 (\log p)^2 \log p e^{\log p - 1/p^2 u} = o(1).
\]

Then clearly we have that there must exist at least one function \( g \) realizing the complementary event that we bounded. Such function works also for each \( \sigma \) such that \( |\sigma| \leq \log p \).

The function \( g : \{0,1\}^{\theta^{-1} \log p} \to \{0,1\}^{\log p} \) obtained from Lemma 3.3 can be used to define each variable \( z_i \) over \( \mathbb{F}_p \) using \( u = \theta^{-1} \log p \) new boolean variables \( x_{i1}, \ldots, x_{iu} \):

\[
z_i = \sum_{j=1}^{\log p} 2^{j-1} g_j(x_{i1}, \ldots, x_{iu}),
\]

where \( g_j \) represents the \( j \)-th coordinate of \( g \). Hence a linear equation mod \( p \) in \( n \) variables, say \( \sum a_{ij} z_i \equiv_p b \), can be transformed into a boolean function using equation (1) using \( N := nu = n\theta^{-1} \log p \) boolean variables \( x_{ij} \). Moreover if \( |\text{supp}(a_1, \ldots, a_n)| \leq d \) then the boolean encoding of that function as a CNF turns out to be a \((du)\)-CNF. More precisely we have the following definition.

**Definition 3.4.** Take the set \( \mathcal{E} := \{E_1, \ldots, E_n\} \) of linear equations in \( n \) variables over \( \mathbb{F}_p \) from Proposition 3.2. This can be expanded as a CNF over the \( z_i \) variables:

\[
\bigwedge_{i=1}^m E_i = \bigwedge_{i=1}^m \left( \sum_{j=1}^n a_{ij} z_j \equiv_p b_i \right),
\]

where \( E_i \) is the linear equation \( \sum_{j=1}^n a_{ij} z_j \equiv_p b_i \) and \( a_{ij}, b_i \in \mathbb{F}_p \). Replacing each \( z_j \) with expression given in (1) we obtain a boolean function

\[
E_i^b := \sum_{j=1}^n a_{ij} \sum_{k=1}^{\log p} 2^{k-1} g_k(x_{i1}, \ldots, x_{iu}) \equiv_p b_i
\]

and then the boolean function we consider is just the CNF encoding of the following:

\[
\phi := \bigwedge_{i=1}^m E_i^b.
\]

Note that since for each \( i \) we have \( |\text{supp}(E_i)| \leq p^2 \), \( \phi \) is a \((p^2 \theta^{-1} \log p)\)-CNF in \( N := n\theta^{-1} \log p \) variables.
Let $\mathcal{E} := \{ E^b : E \in \mathcal{E} \}$ and $\mu(C) := \min\{|S| : S \subseteq \mathcal{E}^b \land S \models C\}$. We say that a clause $C$ has medium complexity w.r.t. $\mu$ iff $\mu(C) \in (\frac{3}{2} \delta n, 3 \delta n]$, with $\delta$ the parameter coming from Proposition 3.2.

The proof of the following Theorem is similar to the analogous result in [BI13].

**Theorem 3.5.** Let $\phi$ and $\mu$ as above and let $C$ be a clause over the $x_{ij}$ variables of medium complexity w.r.t. $\mu$ then

$$\text{width}(C) \geq (1 - (c + 1) \theta) N,$$

where $c$ and $\theta$ are as in Proposition 3.2.

**Proof.** Let $C$ be a clause of medium complexity, that is $\mu(C) \in (\frac{3}{2} \delta n, 3 \delta n]$ and by contradiction $\text{width}(C) \leq (1 - (c + 1) \theta) N$. Take the minimal restriction $\rho$ setting $C$ to $\bot$, then $|\rho| = \text{width}(C)$.

We say that a variable $z_i$ is free if and only if $|\text{dom}(\rho) \cap \{x_i1, \ldots, x_{iN}\}| \leq \log p$.

First we prove that there are at least $c\theta n$ free variables.

Let $Z$ be the number of $z_i$ variables that are free. We have an upper bound for the number of $x_{ij}$ variables non-assigned by $\rho$:

$$(c + 1) \theta N \leq N - \text{width}(C) \leq (n - Z) \log p + uZ.$$

Hence

$$c\theta N + \theta N \leq n \log p - Z \log p + uZ.$$

Now if $Z \leq c\theta n$ a contradiction follows immediately recalling that $N = un$ and $\theta N = n \log p$.

An extension of $\rho$ to all the $x_{ij}$ variables for $i$ such that $z_i$ is not free induces a restriction over the $z_i$ variables mapping them in $\mathbb{F}_p$: let $\rho^*$ denote such an extension. We look at it both as a restriction over the $x_{ij}$ variables or a restriction (taking values in $\mathbb{F}_p$) over the $z_i$ variables.

So the $z_i$ variables that are free are exactly, by construction, the ones unfixed by $\rho^*$. As observed we have that the number of free variables is at least $c\theta n$ and hence $|\rho^*| \leq n - c\theta n = (1 - c\theta)n$.

As $C$ is of medium complexity, there exists some set of equations $S \subseteq \mathcal{E}^b$ such that $S \models C$, $|S| \in (\frac{3}{2} \delta n, 3 \delta n]$ and $S$ is minimal w.r.t. inclusion.

This implies that for each possible $\rho^*$ of the form described above, $\{S|_{\rho^*}\}$ is unsatisfiable. Moreover, by minimality of $S$, for each equation $E \in S$ there exists some $\rho^*$ such that $E|_{\rho^*}$ is not an empty constraint.

The fact that, for each $\rho^*$ we have that $S|_{\rho^*}$ is unsatisfiable means exactly that for all $\rho^*$ there exists some $v \in \mathbb{F}_p^n$ (dependent on $\rho^*$) with $|\text{supp}(v)| \leq |S|$ and $\sum_i v_i E_i|_{\rho^*}$ is unsatisfiable. Hence for each such $\rho^*$ $\text{supp}(\sum_i v_i E_i|_{\rho^*}) \subseteq \text{dom}(\rho^*)$, otherwise we could use the variables unfixed by $\rho^*$ to satisfy $\sum_i v_i E_i|_{\rho^*}$. Let $E^\rho := \sum_i v_i E_i|_{\rho^*}$ (where $v$ depends on $\rho^*$).

Take a random linear combination of all the $E^\rho$ for all the possible $\rho^*$: $\sum_{\rho^*} \alpha_{\rho^*} E^\rho$. Again we have that $\text{supp}(\sum \alpha_{\rho^*} E^\rho) \subseteq \bigcup_{\rho^*} \text{dom}(\rho^*)$. 

6
Each $E_i$ from $S$ appears in this sum and its coefficient is uniformly random, and hence by averaging, there exists a linear combination such that at least $(1 - 1/p)^{\frac{1}{2}}\delta n \geq \delta n$ of the $E_i$ have non-zero coefficient. But this contradicts the expansion property as we have that $|\text{supp}(\sum_{\rho^*} \alpha_{\rho^*}E^{\rho^*})| \leq |\bigcup_{\rho^*} \text{dom}(\rho^*)| = (1 - c\theta)n$.

**Corollary 3.6.** For any large enough $k \in \mathbb{N}$ there exists an unsatisfiable CNF $\phi$ in $N$ variables such that

- $\phi$ is a $k$-CNF;
- $\text{size}_{\text{treeRES}}(\phi \vdash \bot) \geq 2^{(1-O(k^{-1/3}))N}$.

**Proof.** We have that if $C, D \models E$ then $\mu(E) \leq \mu(C) + \mu(D)$ and hence in each possible refutation of $\phi$ there will be a clause of medium complexity. Hence from the previous Theorem we have that $\text{width}(\phi \vdash \bot) \geq (1-O(k^{-1/3}))N$. Then we just apply the width-size relationship from [BSW01].

## 4 Acknowledgements

Part of this work was done while the authors were visiting KTH Royal Institute of Technology. We are grateful to Jakob Nordström for his hospitality and for providing an inspiring environment and to Nicola Galesi for discussions and suggestions.

## References


