Lower Bounds for Bounded Depth Frege

Ivan Monakhov

Academical Physico-Technical University

Abstract. This paper describes author's talk during JASS'2009 on course Proposisional Proofs and presents some proofs and remarks that were omitted in the presentation. Readers are refered to presentation and original papers for detailed definition of k-transformations and their properties. As stated in [BSH03] the version of Switching Lemma used for proving the existanse of k-transformations can be proved by similar to [Bea94] methods and also is a restatement of switching lemma of [UF96].

1 Introduction

The proof of lower bound for bounded depth Frege is the hardest proof of lower bound for proof sytems since there are no known super-polynomial lower bounds proved even for unbounded Frege [Urq95].

This paper could also be interesting for researchers both from areas of mathematical logic (propositional proofs) and computational complexity, because it is presented here very simple and natural relation between bounded depth Frege and Buss-Pudlák Games. This result was originally proved by [PR95] for Frege proof systems and then their proof was applied to bounded Frege in [BSH03].

2 Preliminaries

In this section are presented some basic definitions and remarks on them.

Definition 1. *Frege system* $\boldsymbol{H}$ *is complete proof system over the basis* $\{\vee, \neg\}$

1. *Excluded Middle axiom:* $\frac{}{A \vee \neg A}$
2. *Weakening Rule:* $\frac{A}{A \vee B}$
3. *Merging Rule:* $\frac{\vee(\{\vee\Gamma\} \cup \Delta)}{\vee(\Gamma \cup \Delta)}$
4. *Unmerging Rule:* $\frac{\vee(\Gamma \cup \Delta)}{\vee(\{\vee\Gamma\} \cup \Delta)}$
5. *Cut Rule:* $\frac{(A \vee B),\ (\neg A \vee C)}{B \vee C}$

By $\frac{\phi_1 \ldots \phi_k}{\psi}$ *we denote that* ψ *can be derived from* $\{\phi_1, \ldots \phi_k\}$.

Remark 1. As it was noticed by one of participants after the talk, this Frege proof system is rather special. In sense that it has only one splitting rule, and hence for this proof system Cut Rule couldn't be eliminated.

Fix sets D, R: $D \cap R = \emptyset$, $|D| = n + 1$, $|R| = n$, and denote $S = D \cup R$.

Definition 2. *The pigeonhole principle of size n, denoted PHP_n, is the disjunction of four sets of formulas over the variable set p_{ij}, $i \in D$, $j \in R$:*

$$\begin{array}{ll} \neg \bigvee_{j \in R} p_{ij},\ i \in D & p_{ik} \wedge p_{jk},\ i \neq j \in D,\ k \in R \\ \neg \bigvee_{i \in D} p_{ij},\ j \in R & p_{ij} \wedge p_{ik},\ i \in D,\ j \neq k \in R \end{array}$$

Where each variable p_{ij} states whether pigeon i occupies pigeonhole j.

3 Buss-Pudlák Games

Here are listed notions and theorems from the talk. But some important technical details are ommited. They could be found in slides or in original papers.

Definition 3. *The Frege proof of a tautology Φ is a two player game:*

- *Pavel claimes that Φ is a tautology.*
- *Sam says that he knows an assignment α setting Φ to 0.*
- *In round t Pavel presents Sam a Boolean formula ϕ_t.*
- *Sam answers with a bit b_t, wich is the "value" of $\phi_t(\alpha)$.*
- *Pavel needs to present an immediate contradiction from Definition 4.*

Let B be a set of Boolean gates. In our case $B = \{\neg, \vee\}$.

Definition 4. *An immediate contradiction with respect to B is a set of formulas $\psi, \phi_1, \ldots, \phi_k$ and a set of bits $a, b_1, \ldots, b_k$:*

1. *ψ is $g(\phi_1, \ldots, \phi_k)$, where $g \in B$.*
2. *Sam was asked formulas $\psi, \phi_1, \ldots, \phi_k$, and gave answers $a, b_1, \ldots, b_k$.*
3. *$a \neq g(b_1, \ldots, b_k)$.*

Theorem 1. *For any Frege system $\mathcal{F}$ there exist integer c: If Φ has a standard $\mathcal{F}$-proof of size S and maximal depth d, then Φ has a Buss-Pudlák proof of height $\log(S) + O(1)$ and depth $d + c$ and each query is of size at most S.*

Proof. Let $\phi_1, \ldots \phi_S = \Phi$ be a standard Frege proof, where each ϕ_i has depth at most d. Now we construct from it Buss-Pudlák Game:

- At first round Pavel query for value of Φ. Sam must answer with 0.
- Then Pavel asks Sam about formula $\wedge(\phi_1, \ldots \phi_S)$. Again Sam answers 0.
- Pavel makes $\log(S)$ queries for finding the smallest k such that the answer on $\wedge(\phi_1, \ldots \phi_k)$ was 1 and the answer on $\wedge(\phi_1, \ldots \phi_{k+1})$ was 0.

If there is no such k, then Sam's answer on ϕ_1 was 0, and this is immediate contradiction. The case when ϕ_{k+1} is an axiom is similar.

Otherwise, ϕ_{k+1} was derived by some derivation rule from some previous formulas $\phi_{i_1}, \dots \phi_{i_c}$.

- Then Pavel queries $\phi_{i_1}, \dots \phi_{i_c}$, Sam must answer with 1 or it will contradicts with his answer to $\wedge(\phi_1, \dots \phi_k)$

But even in this case there is immediate contradiction with aplied rule.

Definition 5. *Let S be a set, $D \subseteq S$ and $f : D \to \{0,1\}$ a function on D. The ordered pair (D, f) is called a partial Boolean function on S. The set D is the domain of f, denoted by Dom(f). For any set S, let*

$$\Delta^S = \{(D, f) | D \subseteq S, f : D \to \{0,1\}\}$$

For any (D, f) and $b \in \{0,1\}$, $f^{-1}(b) = \{x \in D | f(x) = b\}$.

Let $\mathcal{T}$ be the game-tree for tautology Φ, proposed by Pavel. Sam applies a transformation, mapping each formula $\phi \in \Sigma_{\mathcal{T}}$ to partial function (D_ϕ, f_ϕ), that satisfies the conditions:

1. $\forall x \in D_\Phi, f_\Phi(x) = 0$.
2. There exists a branch $((\phi_1, b_1), \dots, (\phi_s, b_s))$ in the game-tree $\mathcal{T}$:

$$\bigcap_{i=1}^{s} (f_{\phi_i})^{-1}(b_i) \neq 0$$

3. For any $\Omega \subseteq \Sigma_{\mathcal{T}}$, if there exists $x \in \cap_{\phi \in \Omega} D_\Phi$, then the answers $(f_\phi(x))_{\phi \in \Omega}$ to the queries $(\phi)_{\phi \in \Omega}$ are locally consistent.

Theorem 2. *Let Φ be a formula and $\mathcal{T}$ a game-tree for Φ. If there exists a set S and a transformation $\phi \overset{\Gamma}{\mapsto} (D_\phi, f_\phi)$: conditions 1,2 and 3 are satisfied, then the game-tree does not convict Sam.*

Proof. Lines of our proof following [BSH03]:

- Consider a branch $((\phi_1, b_1), \dots, (\phi_s, b_s))$ of $\mathcal{T}$ provided by 2.
- Choose any $x \in \bigcap_{i=1}^{s} (f_{\phi_i})^{-1}(b_i)$. Sam answers Pavel's queries $\phi_1, \dots \phi_s$ along this branch with $b_1, \dots, b_s$ respectively.
- By 1 Sam answers Pavel's first query $\phi_1 = \Phi$ with $b_1 = 0$.
- Since $x \in \bigcap_{i=1}^{s} \mathrm{Dom}(f_{\phi_i})$, Sam's responses to Pavel's queries along this branch are locally consistent by 3.

4 *k*-transformations

At this section are defined notions of k-transformations and covering partial functions. It follows from Switching lemma that k-transformation exists. And this is almost the same transformation that could be used by Sam. Hence, we could prove the existing of such transformation for Theorem 2. Together with the Theorem 1 this implies the lower bound for bounded depth Frege proof systems.

Definition 6. *Let D, R be some sets such that $D \cap R = \emptyset$, $|D| = n+1$, $|R| = n$, and let $S = D \cup R$. M^S denotes the set of matchings between D and R.*
For any $I \subseteq S$ such that $D \not\subseteq I$, define

$$Cover(I) = \{\pi \in M^S \mid \text{ matching } \pi \text{ covers all vertices in } I\}$$

$$MinCover(I) = \{\pi \in M^S \mid \pi \text{ is a minimal matching that covers } I\}$$

Note that for all $\pi \in \text{MinCover}(I)$, $|\pi| \leq |I|$.

Lemma 1. *Consider $I \subseteq S$ and ρ a matching in M^S such that $|\rho| + |I| \leq n$. Then there exists $\pi \in MinCover(I)$ such that $\pi \cup \rho \in M^S$.*

Definition 7. *A covering partial function is an ordered pair (I, f) such that*

- *$(Cover(I), f)$ is a partial function on M^S.*
- *If $\pi, \pi' \in Cover(I)$ and $\pi \subseteq \pi'$, then $f(\pi') = f(\pi)$.*

Let Σ be closed under taking subformula.

Definition 8. *A k-transformation T is a mapping of formulas $\phi \in \Sigma$ to covering partial functions (I_ϕ, f_ϕ) over S such that*

1. *For all $\phi, |I_\phi| \leq k$.*
2. *$I_0 = I_1 = \emptyset$,*
   $\forall \pi \in Cover(I_0)$, $f_0(\pi) = 0$,
   $\forall \pi \in Cover(I_1)$, $f_1(\pi) = 1$.
3. *$I_{p_{ij}} = \{i, j\}$,*
   if $\{i, j\} \in \pi$, $f_{p_{ij}}(\pi) = 1$, otherwise $f_{p_{ij}}(\pi) = 0$.
4. *[Negation]*
   $I_{\neg\phi} = I_\phi$, $\forall \pi \in Cover(I_\phi), f_{\neg\phi}(\pi) = \neg f_\phi(\pi)$.
5. *[Disjunction]*
   If ϕ is a disjunction and $\vee_{j \in J} \phi_j$ is the merged form of ϕ,
   then (I_ϕ, f_ϕ) satisfies $Disj\Big[\bigcup_{j \in J}\{(I_{\phi_j}, f_{\phi_j})\}\Big]$

Proposition 1. *Let Σ be a set of formulas closed under the operation of taking subformula. Let T be a k-transformation mapping formulas $\phi \in \Sigma$, to covering partial funcitons (I_ϕ, f_ϕ) over S. If for $\Omega \subset \Sigma$, there exists a $\pi \in \bigcap_{\phi \in \Omega} Dom(f_\phi)$, then the answers $(f_\phi(\pi))_{\phi \in I}$ to the queries $(\phi)_{\phi \in I}$ are locally consistent.*

Proposition 2. *If T is k-transformation for a set of formulas containing PHP_n, $k < n - 1$, then $f_{PHP_n}(\pi) = 0$ for all $\pi \in Cover(I_{PHP_n})$.*

Proof. PHP_n is the disjunction of formulas of the form $\neg\phi$, where ϕ ranges over

$$\begin{array}{ll} \bigvee_{j\in R} p_{ij},\ i \in D & \neg p_{ik} \vee \neg p_{jk},\ i \neq j \in D,\ k \in R \\ \bigvee_{i\in D} p_{ij},\ j \in R & \neg p_{ij} \vee \neg p_{ik},\ i \in D,\ j \neq k \in R \end{array}$$

From the definition of a k-transformation, it suffices to show that $f_\phi(\pi) = 1, \forall \pi \in \mathrm{Cover}(I_\phi)$ for each of the above ϕ.

Let $i \in D$ and $\phi = \bigvee_{j\in R} p_{ij}$. Suppose $f_\phi(\pi) = 0$ for some $\pi \in \mathrm{Cover}(I_\phi)$. $|I_\phi| \leq k$,$\pi \in \mathrm{MinCover}(I_\phi)$ and $k < n-1$, imply $|\pi| < n-1$. Hence, there exists a $\pi' \in M^S$ such that $\pi \subseteq \pi'$ and π' covers i. Let $\{i, j\} \in \pi'$ for some $j \in R$. But then $f_{p_{ij}}(\pi') = 1$ while $f_\phi(\pi') = f_\phi(\pi) = 0$ contradicts the definition of a k-transformation. Hence, $f_\phi(\pi) = 1, \forall \pi \in \mathrm{Cover}(I_\phi)$ for ϕ of the specified type.

Let $i \neq j \in D, k \in R$ and $\phi = \neg p_{ik} \vee \neg p_{jk}$. Suppose $f_\phi(\pi) = 0$ for some $\pi \in \mathrm{Cover}(I_\phi)$. As before, we have $|\pi| < n-1$. Since π is a matching, either $\{i, k\} \notin \pi$ or $\{j, k\} \notin \pi$. Assume $\{i, k\} \notin \pi$. Since $|\pi| < n-1$, there exists a $\pi' \in M^S$: $\pi \subseteq \pi'$ and $\{i, r\}, \{s, k\} \in \pi'$ for some $r \neq k \in R$ and $s \neq i \in D$.
We have $\pi' \in \mathrm{Cover}(I_{p_{ik}})$ and $f_{p_{ik}}(\pi') = 0$. Hence, $f_{\neg p_{ik}}(\pi') = 1$.
But $f_\phi(\pi') = f_\phi(\pi) = 0$ again contradicts definition.

The other two types of formulas are proved similarly.

Definition 9. *We define $I|_\rho = I \setminus V(\rho)$ for any $I \subseteq S$. For (I, f) a covering partial function over S, we define $f|_\rho : Cover(I|_\rho) \to \{0, 1\}$ as $f|_\rho(\pi) = f(\pi \cup \rho)$ for all $\pi \in Cover(I|_\rho)$.*

Proposition 3. *Let $\mathcal{T}$ be a game-tree of height r for PHP_n. Let T be a k-transformation mapping formulas ϕ to covering partial functions (I_ϕ, f_ϕ) over $S|_\rho$ for some matching $\rho \in M^S$ of size $n - m$. If $kr \leq m$, then there exists a branch $((\phi_1, b_1), \ldots, (\phi_s, b_s))$ in the game-three $\mathcal{T}$:*

$$\bigcap_{i=1}^{s} (f_{\phi_i})^{-1}(b_i) \neq 0$$

Proof. Consider the following procedure *Walk*($\mathcal{T}$), outputing branch of $\mathcal{T}$

1. Set $\pi \leftarrow \emptyset$ and $i \leftarrow 1$.
2. Walk along $\mathcal{T}$ from the root till a leaf reached:
   - (a) Set $\phi_i \leftarrow$ label of current node.
   - (b) Choose a $\pi_i \in \mathrm{MinCover}(I_{\phi_i})$: $\pi \cup \pi_i \in M^{S|_\rho}$.
   - (c) Set $b_i \leftarrow f_{\phi_i}(\pi_i)$ and $\pi \leftarrow \pi \cup \pi_i$.
   - (d) Walk along edge labeled b_i leading out of current node.
   - (e) Increment i.
3. Output $((\phi_1, b_1), \ldots, (\phi_s, b_s))$.

- Since $\mathcal{T}$ is a game-tree for PHP_n, $\phi_1 = PHP_n$ and $b_1 = 0$ for any branch.
- By Proposition 1, $f_{PHP_n}(\pi) = 0$ for all $\pi \in \mathrm{Cover}(PHP_n)$.

– *Walk* algorithm choose some matching $\pi \in \text{MinCover}(I_{PHP_n})$.
– A matching π_i can be chosen in the loop at Step 2b as long as $|\pi| + k \leq m$.
– $|\pi|$ is extended at most r times by at most k, and $rk \leq m$.
Hence, the condition $|\pi| + k \leq m$ is true.

Let π be the matching at the final step of *Walk*.
The branch $((\phi_1, b_1), \ldots, (\phi_s, b_s))$ satisfies $b_i = f_{\phi_i}(\pi)$.
Hence, $\pi \in \bigcap_{i=1}^{s} (f_{\phi_i})^{-1}(b_i)$ and $\bigcap_{i=1}^{s} (f_{\phi_i})^{-1}(b_i) \neq \emptyset$.

Theorem 3. (Switching Lemma) *Let (I_j, f_j) be covering partial functions over $S, |I_j| \leq r$ for all $j \in J$. Let $\ell \geq 10$ and $p = \ell/n$. If $r \leq \ell$ and $p^4 n^3 \leq 1/10$, then for random $\rho \in M^S$, $|\rho| = n - \ell$,* $\Pr\{$ *"There exists a covering partial function (I, f) over $S|_\rho$: (I, f) satisfies Disj $\left[\bigcup_{j \in J} \{(I_j|_\rho, f_j|_\rho)\}\right]$ and $|I| < 2s$"$\} \geq 1 - (11p^4 n^3 r)^s$.*

Theorem 4. *Let d be an integer, $0 < \epsilon < 1/5, 0 < \delta < \epsilon^d$ and Σ a set of formulas of depth d. If $|\Sigma| < 2^{n^\delta}, q = n^{\epsilon^\delta}$ and n is sufficiently large, then there exists a matching $\rho \in M^S$ of size $n - n^{\epsilon^\delta}$: there is a $2n^\delta$-transformation T mapping formulas $\phi \in \Sigma$, to covering partial functions (I_ϕ, f_ϕ) over $S|_\rho$.*

Theorem 5. (Main result) *Let $\mathcal{F}$ be a Frege system and let c be the constant that occurs in theorem about Buss-Pudlák Games. Then for sufficiently large n, every depth d proof in $\mathcal{F}$ of PHP_n must have size at least 2^{n^μ}, for $\mu < \frac{1}{2}(\frac{1}{5})^{d+c}$.*

Proof. Let $0 < \epsilon < \frac{1}{5}$ and $0 < \mu < \epsilon^{d+c}/2$. Suppose PHP_n has a depth d proof in $\mathcal{F}$ of size 2^{n^μ}. By the Theorem 1, there exists Buss-Pudlák game-tree $\mathcal{T}$ of height n^μ consisting of formulas of size at most 2^{n^μ} and depth at most $d + c$ convicting Sam on PHP_n. Let Σ be the set of all formulas in $\mathcal{T}$. Clearly, $|\Sigma| \leq 2^{2n^\mu}$.

– Choose δ: $\mu < \delta < \epsilon^d/2$. For sufficiently large n, $|\Sigma| < 2^{n^\delta}$.
– By the previous theorem, there exists a partial matching ρ of size $n - n^{\epsilon^d}$: Σ has a $2n^\delta$-transformation T mapping formulas $\phi \in \Sigma$ to covering partial functions, (I_ϕ, f_ϕ) over $S|_\rho$.
– By Proposition 2, we have that condition 1 is satisfied since $2n^\delta < n^{\epsilon^d} - 1$.
– Also $2n^\delta \cdot n^\mu \leq n^{\epsilon^d}$ and the conditions of Proposition 3 are satisfied.
– Hence, $2n^\delta$-transformation satisfies condition 2.
– By Proposition 1, we have that condition 3 is also satisfied.
– Thus, by the Theorem 2, game-tree $\mathcal{T}$ does not convict Sam.
– And there exists no depth d proof of PHP_n in $\mathcal{F}$ of size less then 2^{n^μ}.

Acknowledgments

The author is grateful to organizers and participants of JASS'09.

References

[Bea94] Paul Beame. A switching lemma primer. Technical Report UW-CSE-95-07-01, University of Wshington, 1994.

[BSH03] Eli Ben-Sasson and Prahladh Harsha. Lower bounds for bounded depth frege proofs via buss-pudlák games. Technical Report 4, Electronic Colloquium on Computational Complexity, 2003.

[PR95] Pavel Pudlák and Samuel R.Buss. How to lie without being (easily) convicted and the length of proofs in propositional calculus. In Leszek Pacholski and Jerzy Tiuryn, editors, *Lecture Notes in Computer Science*, volume 933, pages 151–162. Springer, Kazimierz, Poland, 1995.

[UF96] Alasdair Urquhart and Xudong Fu. Simplified lower bounds for proposotional proofs. *Journal of Formal Logic*, 37(4):523–544, 1996.

[Urq95] Alasdair Urquhart. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 1(4):425–467, 1995.