Lifting Lower Bounds for Tree-Like Proofs

Alexis Maciel
Clarkson University

Phuong Nguyen
University of Montréal

Toniann Pitassi
University of Toronto

Banff 2011

Introduction

General goal: Prove that some tautology requires very large $\mathcal{P}$ proofs, for increasingly more general $\mathcal{P}$.

Famous example: Resolution

Virtually all propositional theorem provers attempt to construct Resolution proofs.

Theorem [Haken 85] Resolution proofs of the Pigeonhole Principle have exponential size.

Next: Extensions of Resolution. . .

The Sequent Calculus

Lines in a proof: $(A_1 \wedge \cdots \wedge A_n) \rightarrow (B_1 \vee \cdots \vee B_m)$

Sequents: $A_1, \ldots, A_n \rightarrow B_1, \ldots, B_m$

Axiom: $A \rightarrow A$

Some inference rules:

NEG-left: From $\Gamma \rightarrow A, \Delta$, derive $\neg A, \Gamma \rightarrow \Delta$.

AND-right: From $\Gamma \rightarrow A, \Delta$ and $\Gamma \rightarrow \wedge(F), \Delta$, derive $\Gamma \rightarrow \wedge(A, F), \Delta$.

Cut rule: From $\Gamma, A \rightarrow \Delta$ and $\Gamma \rightarrow A, \Delta$, derive $\Gamma \rightarrow \Delta$.

Constant-Depth Frege

Constant-depth Frege: The depth of all formulas is bounded by some constant d.

Depth 0: Resolution.

Theorem [PBI 93, KPW 95] Constant-depth Frege proofs of the Pigeonhole Principle have exponential size.

Constant-depth Frege $=$ AC^0-Frege.

Next: $\mathrm{ACC}^0[r]$-Frege.

ACC$^0[r]$-Frege

Modular connectives: $\oplus_r^b(F)$ is true if $\sum_{A \in F} A \equiv b \pmod{r}$.

Additional rules:

Mod-left: From $A, \oplus_r^{b-1}(F), \Gamma \to \Delta$ and $\oplus_r^b(F), \Gamma \to A, \Delta$, derive $\oplus_r^b(A, F), \Gamma \to \Delta$.

Idea: Adapt circuit lower bound technique.

$\mathsf{AC}^0 \subset \mathsf{ACC}^0[q] \subset \mathsf{ACC}^0[r]$, if q is prime and r is divisible by q and some other prime p. [Håstad 86, Smolensky 87]

Idea: Use circuit lower bound directly.

Example: Cutting planes, interpolation.

Problem: AC^0-Frege and all of its extensions probably do not have the interpolation property. [BDGMT 04]

In fact: No lower bound result known for $\mathsf{ACC}^0[r]$-Frege (or any other extension of AC^0-Frege).

Alternative Extensions of Resolution

Idea: Restrict only cut formulas.

$ACC^0[r]$-Frege	$ACC^0[r]$-PK^*	$ACC^0[r]$-PK
AC^0-Frege	AC^0-PK^*	AC^0-PK
Resolution		

Complete for all tautologies, not just constant-depth formulas.

Conservative extensions of AC^0-Frege and $ACC^0[r]$-Frege.

Corollary AC^0-PK proofs of PHP have exponential size.

Theorem $\mathsf{ACC}^0_d[r]$-PK^* proofs of $\mathsf{PHP}(\mathsf{MOD}_2)$ have exponential size, assuming a plausible circuit complexity conjecture.

$\mathsf{ACC}^0[r]$-Frege	$\mathsf{ACC}^0[r]$-PK^*	$\mathsf{ACC}^0[r]$-PK
AC^0-Frege	AC^0-PK^*	AC^0-PK
Resolution		

Note: Size-s $\mathsf{ACC}^0_d[r]$-PK^* proofs of $\mathsf{PHP}(\mathsf{MOD}_2)$ imply size-s $\mathsf{ACC}^0_d[r]$-Frege* proofs of PHP.

General Strategy

$\mathcal{C}$-PK*	AC^0_d-PK*	$ACC^0_d[r]$-PK*
PK* proofs with cuts limited to circuit class $\mathcal{C}$.	$\mathcal{C} = AC^0_d$	$\mathcal{C} = ACC^0_d$
Cut-free PK* proofs of S have exponential size.	S = Statman or PHP	
$\mathcal{C}$ circuits of subexponential size cannot approximate f.	$f = MOD_2$ [Håstad 86]	$f = MAJ$?
"Lifted" lower bound: $\mathcal{C}$-PK* proofs of $S(f)$ have exp size.		

Main Result

Theorem $\mathcal{C}$-PK* proofs of $S(f)$ have exponential size if

$\mathcal{C}$ is a set of formulas that is closed with respect to sub-formulas and restrictions,

f, as a function, is balanced and hard to approximate by $\mathcal{C}$ formulas, and

S has the Statman property of order n.

Definition S has the **Statman property of order** n if the following hold:

> S is of the form $\rightarrow \Gamma$ where Γ is not empty and consists of nonempty conjunctions.
>
> Removing from S every occurrence of any of these conjunctions results in an invalid sequent.
>
> If $n \geq 2$, let S' be obtained from S by replacing a conjunction $\wedge(A, F)$ by either A or $\wedge(F)$. Then there is a partial assignment ρ such that $S'|\rho$ has the Statman property of order $n - 1$, modulo a possible renaming of the variables.

Examples: Statman and PHP.

Theorem If S has the Statman property of order n, then any cut-free PK^* proof of S requires size 2^n.

Proof Overview

Suppose that S has the Statman property of order n and suppose that $\mathcal{C}$ and f satisfy the conditions of the theorem.

S has the form $\to \Gamma$.

Suppose that π is a $\mathcal{C}$-PK* proof of $\to \Gamma(f)$.

From the root of π, follow all paths until: an axiom, a sequent where a formula of $\Gamma(f)$ is introduced by weakening, or a sequent where a formula of $\Gamma(f)$ is introduced by an AND-right rule.

Result: a subtree π' of π in which all sequents are of the form $\Lambda \to \Delta, \Gamma(f)$ with all the formulas in Λ and Δ belonging to $\mathcal{C}$.

Goal: Show that little progress is made in π'.

In $\Lambda \to \Delta, \Gamma(f)$, the formulas in Λ and Δ are side formulas.

An assignment is critical if is satisfies Λ and falsifies Δ.

All assignments are critical for the root sequent $\to \Gamma(f)$.

Critical assignments are preserved as we travel from the root to the leaves of π'.

If π' is of size 2^n, done.

Otherwise, a $1/2^n$ fraction of all assignments is critical for some leaf L of π'.

L is of the form $\Lambda \to \Delta, \Gamma(f)$.

Goal: Show that L is just as hard to prove as $\to \Gamma(f)$.

$L = \Lambda \rightarrow \Delta, \Gamma(f)$ cannot be an axiom.

Suppose that L is derived from L' and L'' by an application of the AND-right rule that introduces a formula of $\Gamma(f)$.

L' is of the form $\Lambda \rightarrow \Delta, \Gamma'(f)$ where Γ' contains all the formulas of Γ but with some $\wedge(A, F)$ replaced by either A or $\wedge(F)$.

There is a partial assignment ρ to the variables of $\rightarrow \Gamma$ such that $(\rightarrow \Gamma')|_\rho$ has the Statman property of order $n - 1$.

Goal: Achieve ρ with a large number of critical assignments to the variables of L'.

All the assignments that are critical for $L = \Lambda \to \Delta, \Gamma(f)$ are also critical for $L' = \Lambda \to \Delta, \Gamma'(f)$.

Since f is hard for the side formulas, at least $1/4$ of the critical assignments satisfy f and at least $1/4$ falsify f.

Therefore, ρ can be achieved with a large number of critical assignments to the variables of L'.

There is a partial assignment τ to the variables of L' that is consistent with ρ and such that $L'|_\tau = \Lambda|_\tau \to \Delta|_\tau, \Gamma'|_\rho(f)$ still has a large number of critical assignments.

By induction, $L'|_\tau$, and therefore L', requires a proof of size 2^{n-1}.

Same for L''. Therefore, π has size at least 2^n. $\square$

Missing: Weakening. Contractions. Numbers of critical assignments. Arity of f.

Lower Bounds

$\mathrm{ACC}^0[r]$-Frege $\mathrm{ACC}^0[r]$-PK* $\mathrm{ACC}^0[r]$-PK

AC^0-Frege AC^0-PK* AC^0-PK

Resolution

Theorem If f is balanced and hard for $\mathrm{ACC}^0_d[r]$, then $\mathrm{PHP}(f)$ requires $\mathrm{ACC}^0_d[r]$-PK* proofs of exponential size.

Theorem $\mathrm{PHP}(\mathrm{MOD}_2)$ requires AC^0_d-PK* proofs of exponential size.

Tree-Like Versus Dag-Like Proofs

$\mathsf{ACC}^0[r]$-Frege	$\mathsf{ACC}^0[r]$-PK*	$\mathsf{ACC}^0[r]$-PK
AC^0-Frege	AC^0-PK*	AC^0-PK
Resolution		

Theorem If f is balanced and hard for $\mathsf{ACC}^0_d[r]$, then Statman(f) has polynomial-size cut-free PK proofs but requires $\mathsf{ACC}^0_d[r]$-PK* proofs of exponential size.

Theorem Statman(MOD_2) has polynomial-size cut-free PK proofs but requires AC^0_d-PK* proofs of exponential size.

Key: Statman has polynomial-size cut-free PK proofs.

Separation Results

Theorem Statman(MOD_2) has polynomial-size $\mathrm{ACC}^0_3[2]$-PK* proofs but requires AC^0_d-PK* proofs of exponential size.

Theorem If p is a prime that does not divide r and if $f \in \mathrm{ACC}^0[p]$ is balanced and hard for $\mathrm{ACC}^0_d[r]$, then Statman(f) has polynomial-size $\mathrm{ACC}^0[p]$-PK* proofs but requires $\mathrm{ACC}^0_d[r]$-PK* proofs of exponential size.

Key: Statman has polynomial-size AC^0_1-PK* proofs.

Other Results

Hierarchy theorems for AC^0-PK^* and $\mathsf{ACC}^0[r]$-PK^*.

Similar results for TC^0-PK^*.

New proof of the non-finite axiomatizability of the theory of bounded arithmetic $I\Delta_0(R)$.

The hierarchy G_i^* of quantified propositional proof systems does not collapse, assuming a plausible hardness conjecture concerning the polynomial-time hierarchy.

Summary

$ACC^0[r]$-Frege	$ACC^0[r]$-PK*	$ACC^0[r]$-PK
AC^0-Frege	AC^0-PK*	AC^0-PK
Resolution		

Lower bounds.

Separation of tree-like and dag-like.

Separation of various MOD's.

Hierarchy theorems.

Some Open Problems

$\mathrm{ACC}^0[r]$-Frege	$\mathrm{ACC}^0[r]$-PK*	$\mathrm{ACC}^0[r]$-PK
AC^0-Frege	AC^0-PK*	AC^0-PK
Resolution		

Lower bound for $\mathrm{ACC}_d^0[r]$-PK.

Lower bound for $\mathrm{ACC}_d^0[r]$-Frege.

Strong hardness result for $\mathrm{ACC}^0[r]$.