Subexponential AC^0-Frege Simulates Frege

Yuval Filmus[1] Toniann Pitassi[1]
Rahul Santhanam[2]

[1]University of Toronto

[2]University of Edinburgh

International Colloquium on
Automata, Languages and Programming 2011

Proof complexity

Propsitional proof complexity studies how hard it is to prove propositions in weak proof systems.

Motivation: If no proof system can prove all tautologies in polynomial size, then NP$\neq$coNP.

Proof complexity

Propsitional proof complexity studies how hard it is to prove propositions in weak proof systems.

Motivation: If no proof system can prove all tautologies in polynomial size, then NP$\neq$coNP.

Some proof systems:

- Frege: Undergraduate propositional logic.
- AC^0_d-Frege: Can only use depth-d formulas.

Statement of main result

Theorem

Suppose Frege proves some formula φ in size s. For every $d \geq 1$, Frege with depth-$d+2$ cuts proves φ in size

$$2^{ds^{1/d}}$$

Statement of main result

Theorem

Suppose Frege proves some formula φ in size s. For every $d \geq 1$, Frege with depth-$d+2$ cuts proves φ in size

$$2^{ds^{1/d}}$$

Corollary

If Frege proves depth-d formula φ in size $|\varphi|^c$, then AC^0_{d+2}-Frege proves φ in size

$$2^{cd|\varphi|^{1/d}}$$

Consequences

Our result relates two barriers in proof complexity:

- Superpolynomial lower bounds for Frege.
- 2^{n^ϵ} lower bounds for AC^0_d-Frege with ϵ independent of d.

The result shows that the latter imply the former.

Consequences

Proof system has *Feasible Interpolation* if given a proof of $A(x, y) \vee B(x, z)$ of size s, can construct a circuit $C(x)$ of size $poly(s)$ deciding whether A or B is satisfiable.

Consequences

Proof system has *Feasible Interpolation* if given a proof of $A(x, y) \vee B(x, z)$ of size s, can construct a circuit $C(x)$ of size $poly(s)$ deciding whether A or B is satisfiable.

Proof system is *weakly automatizable* if there exists a polytime algorithm that on input $A, 1^r$:

- Outputs 0 if A is not a tautology.
- Outputs 1 if A has a proof of size r.

Consequences

Simplifies proof of [BDGMP] that AC^0-Frege doesn't have FIP and is not weakly automatizable unless DDH has subexponential circuits.

Consequences

Simplifies proof of [BDGMP] that AC^0-Frege doesn't have FIP and is not weakly automatizable unless DDH has subexponential circuits.

Starting point is [BPR]: poly-size Frege proof of

either $\quad x = g^{a_1}, y = g^{b_1}$ and $g^{a_1 b_1}$ even
or $\quad x = g^{a_2}, y = g^{b_2}$ and $g^{a_2 b_2}$ odd

[BDGMP] laboriously translate proof to AC^0-Frege.

Our result gives such a translation in general.

Proof idea

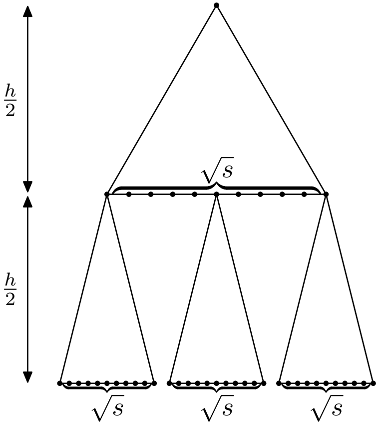
Starting point is a circuit complexity result:

Every NC^1 circuit can be converted to a bounded-depth circuit with sub-exp blow-up.

- Convert all formulas in proof to bounded depth.
- Prove rules of inference hold for converted formulas.
  Main idea: prove $C(P \Diamond Q) \leftrightarrow C(P) \Diamond C(Q)$ for $\Diamond = \vee, \wedge$ (internal comprehension).

Circuit complexity result

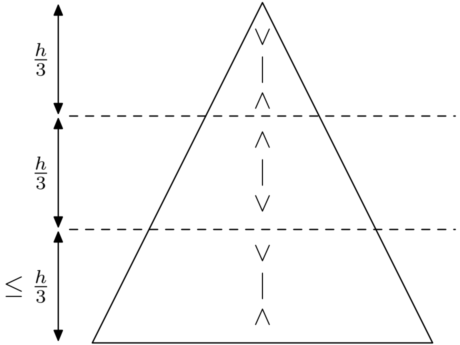
Proof of the circuit complexity result:



Replace each subcircuit with DNF or CNF.

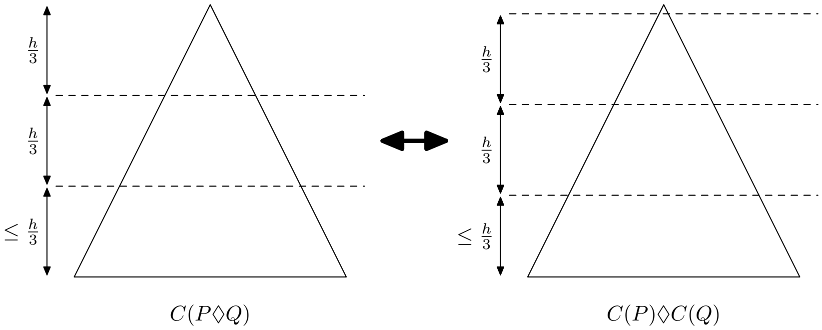
Canonical representation

Let maximal depth of all formulas be *h*.
Convert all formulas to depth 4 (say) using:



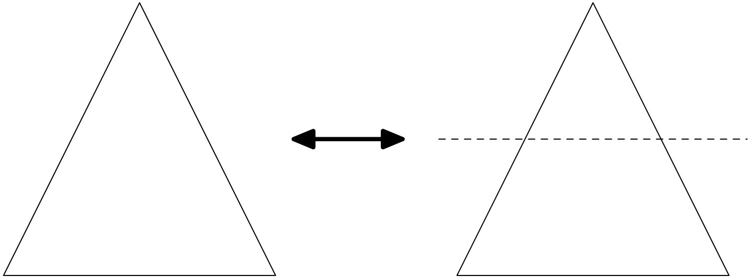
Internal comprehension

Prove that $C(P\Diamond Q) \leftrightarrow C(P)\Diamond C(Q)$ by moving all levels down and adding level at top at depth 1:



Level manipulation

All manipulations reduce to adding/removing one level:



This equivalence is proved by brute force.

Tightness

$2^{s^{1/d}}$ blowup is tight for *tree-like* proofs:

- Start with PHP with $n+1$ pigeons, n holes.
- Buss: poly-size Frege proof of PHP.
- Replace each variable with Sipser function of depth d.
- New formula provable in size $n^{d+O(1)}$.
- Krajíček: $2^{n^{\Omega(1)}}$ lower bound for tree-like AC^0_d-Frege.

Open questions

Extension to theories: ongoing work by Ghasemloo and Cook.

Open questions

Extension to theories: ongoing work by Ghasemloo and Cook.

Do other similar results from circuit complexity carry over to proof complexity?

- Yao's normal form for ACC
- Allender's normal form for arithmetic circuits
- Allender/Koucký self-reducibility: Superlinear separation between Frege and TC^0-Frege implies superpoly separation