Proofs with monotone cuts

Emil Jeřábek
jerabek@math.cas.cz
http://math.cas.cz/˜jerabek/

Institute of Mathematics of the Academy of Sciences, Prague

Propositional proof complexity

Fix a language $L \subseteq \Sigma^*$ (think $L = TAUT =$ classical propositional tautologies).

A proof system P for L:

- φ has a P-proof iff $\varphi \in L$
- polynomial-time decidable whether π is a P-proof of φ

P is p-bounded if every $\varphi \in L$ has a proof of length $poly(|\varphi|)$

P p-simulates a proof system Q ($Q \leq_p P$) if we can translate Q-proofs to P-proofs of the same formula in polynomial time

P is p-equivalent to Q ($P \equiv_p Q$) if $P \leq_p Q \wedge Q \leq_p P$

Propositional proof complexity (cont'd)

Theorem [Cook, Reckhow '79]: There exists a p-bounded proof system for $TAUT$ iff $NP = coNP$.

Goal: prove that every proof system for $TAUT$ requires exponentially long proofs

Reality:

- exponential lower bounds and nonsimulation (speed-up) results for some specific, rather weak, proof systems
- simulations

Frege systems

Usual propositional sequent calculus LK:

- operates with sequents $\varphi_1, \dots, \varphi_n \vdash \psi_1, \dots, \psi_m$
- structural rules: identity, cut, weakening, contraction, exchange
- logical rules: left and right introduction rules for each connective

LK is p-equivalent to

- Frege systems: operate with formulas, finite list of schematic rules (e.g., modus ponens + axioms), sound and implicationally complete
- natural deduction

Subsystems of Frege

LK/Frege is a very strong proof system, no lower bounds in sight

Weaken the proof system by restricting formulas in the proof to some subset Θ. Examples:

- bounded-depth LK/Frege: $\Theta =$ formulas of depth $\leq$ a constant d (need $\bigwedge$ and $\bigvee$ of unbounded arity)
  - exponential lower bounds: PHP
- monotone sequent calculus MLK: $\Theta =$ monotone formulas (= using $\wedge$, $\vee$, but no $\neg$)

Monotone sequent calculus

Motivation: exponential lower bounds on monotone circuit complexity (even separation from nonmonotone circuits)

- maybe we could exploit these to get an exponential separation of MLK and LK?

The answer is no:

Theorem [AGP '02]: MLK quasipolynomially simulates LK: a monotone sequent in n variables with an LK-proof of size s has an MLK-proof of size $s^{O(1)} n^{O(\log n)}$.

- also: certain hypothesis (see next slide) implies polynomial simulation

Threshold functions

$T^n_k(p_1, \ldots, p_n) = 1 \Leftrightarrow \left|\{i \mid p_i = 1\}\right| \geq k$

- poly-size formulas by carry-save addition
- size $n^{O(\log n)}$ monotone formulas by divide-and-conquer
- in fact: poly-size monotone formulas, but randomized construction (Valiant ’84) or very complicated (AKS ’83)

Hypothesis (let’s call it H):
There exists poly-size monotone formulas for T^n_k whose basic properties have poly-time constructible LK-proofs.

- some progress towards H in [J. ’08]

Less restrictive subsystems of Frege

Bad: Restricting formulas appearing in a proof to Θ also restricts sequents that can be proved in the system!

- MLK can only prove monotone sequents

Alternative approach: relax the restriction

- any formula can appear in a proof, but cut formulas can only come from Θ
- conservative extension of the other approach: when proving a sequent $\Gamma \vdash \Delta$ where $\Gamma \cup \Delta \subseteq \Theta$, all formulas in the proof will be from Θ ($\because$ subformula property)
- complete proof system for full propositional logic ($\because$ contains cut-free LK)

LK with monotone cuts

$MCLK$:
sequent calculus where only monotone formulas can be cut

- coincides with MLK when proving monotone sequents
- unlike MLK, can also prove all nonmonotone tautological sequents

We know from [AGP '02] that $MCLK$ quasipolynomially simulates LK-proofs of monotone sequents.

What about general sequents? In principle, $MCLK$ could be as bad as the cut-free sequent calculus for these.

Complexity of $MCLK$

Theorem [J.]: $MCLK$ quasipolynomially simulates LK.
A sequent in m variables with an LK-proof of size s has an $MCLK$-proof of size $s^{O(1)} n^{O(\log n)}$.

- in other words: given any sequent proof, we can transform it into a not much bigger proof with no cuts on nonmonotone formulas
- if H holds, the simulation can be made polynomial

Proof idea

The idea is based on Wegener's slice functions:

If $T^n_k(\vec{p}) \wedge \neg T^n_{k+1}(\vec{p})$, then

$$\neg p_i \leftrightarrow T^{n-1}_k(p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n)$$

This allows for every formula to be translated with a monotone formula.

Refutation systems

Refutation system: a kind of propositional proof system where we prove $\neg\varphi$ by deriving a contradiction from φ

Often: φ is CNF, given as a set of clauses

$$p_{i_1} \vee \cdots \vee p_{i_k} \vee \neg p_{j_1} \vee \cdots \vee \neg p_{j_l}$$

Examples:

- resolution
- algebraic systems: polynomial calculus, Lovász–Schrijver, cutting planes
- LK or Frege as a refutation system: if unrestricted, p-equivalent to its use as a normal proof system

MLK as a refutation system

We can represent a clause $C = p_{i_1} \vee \cdots \vee p_{i_k} \vee \neg p_{j_1} \vee \cdots \vee \neg p_{j_l}$ by a monotone sequent $C^{\vdash}$:

$$p_{j_1}, \ldots, p_{j_l} \vdash p_{i_1}, \ldots, p_{i_k}$$

An MLK-refutation of a CNF φ is a derivation of the contradictory sequent

$$\vdash$$

from the set of initial sequents $\{C^{\vdash} \mid C \in \varphi\}$ using the rules of MLK

- resolution = fragment of MLK using only the cut rule

Complexity of MLK refutations

Theorem [J.]: MLK as a refutation system quasipolynomially simulates LK:
A CNF in m variables with an LK-refutation of size s has an MLK-refutation of size $s^{O(1)} n^{O(\log n)}$.

- again, the simulation can be made polynomial under H

Thank you for attention!

References

M. Ajtai, J. Komlós, E. Szemerédi, *An* $O(n \log n)$ *sorting network*, Proc. 15th STOC, 1983, 1–9.

A. Atserias, N. Galesi, P. Pudlák, *Monotone simulations of non-monotone proofs*, J. Comput. System Sci. 65 (2002), 626–638.

S. Cook, R. Reckhow, *The relative efficiency of propositional proof systems*, JSL 44 (1979), 36–50.

E. Jeřábek, *A sorting network in bounded arithmetic*, preprint, 2008.

L. Valiant, *Short monotone formulae for the majority function*, J. Algorithms 5 (1984), 363–366.