On monotone sequent calculus

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

Institute of Mathematics of the Academy of Sciences, Prague

Monotone sequent calculus

MLK: sequents $\Gamma \vdash \Delta$, where Γ, Δ finite sets of monotone ($\wedge$, $\vee$) propositional formulas

$$\text{i}\ \frac{}{\Gamma, \varphi \vdash \varphi, \Delta} \qquad \text{cut}\ \frac{\Gamma \vdash \varphi, \Delta \qquad \Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta}$$

$$\wedge\text{-l}\ \frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta} \qquad \wedge\text{-r}\ \frac{\Gamma \vdash \varphi, \Delta \qquad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \varphi \wedge \psi, \Delta}$$

$$\vee\text{-l}\ \frac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta} \qquad \vee\text{-r}\ \frac{\Gamma \vdash \varphi, \psi, \Delta}{\Gamma \vdash \varphi \vee \psi, \Delta}$$

Main problem

Problem ("Think Positively Conjecture"):
Does MLK p-simulate LK-proofs of monotone sequents?

Note: there exist monotone Boolean functions computable by poly-size circuits which require exponential size monotone circuits (Razborov '85; Alon, Boppana '87)

Theorem (Atserias, Galesi, Pudlák '02):
MLK quasipolynomially simulates LK.

A monotone sequent $\Gamma \vdash \Delta$ in n variables with an LK-proof of size s has an MLK-proof with $s^{O(1)}$ lines and size $s^{O(1)}n^{O(\log n)}$.

Threshold functions

$$\theta^n_m(x_0, \ldots, x_{n-1}) = 1 \Leftrightarrow |\{i < n \mid x_i = 1\}| \geq m$$

The simulation by AGP uses $n^{O(\log n)}$-size monotone formulas for θ^n_m. Better formulas give a better result:

Theorem (AGP '02): Assume that there are monotone formulas $T^n_m(p_0, \ldots, p_{n-1})$ such that the formulas

$$T^n_0(p_0, \ldots, p_{n-1}) \tag{1}$$

$$\neg T^n_{n+1}(p_0, \ldots, p_{n-1}) \tag{2}$$

$$T^n_m(p_0, \ldots, p_k/\bot, \ldots, p_{n-1}) \to T^n_{m+1}(p_0, \ldots, p_k/\top, \ldots, p_{n-1}) \tag{3}$$

have poly-time constructible LK-proofs. Then MLK p-simulates LK on monotone sequents.

Formulas for threshold functions

Threshold functions have uniform poly-size formulas as $TC^0 \subseteq NC^1$. However, we need monotone formulas.

Known constructions of monotone formulas for threshold functions:

- Ajtai, Komlós, Szemerédi '83: Log-depth sorting network.
- Valiant '84: Simple probabilistic argument.

Valiant's construction

Formula F:

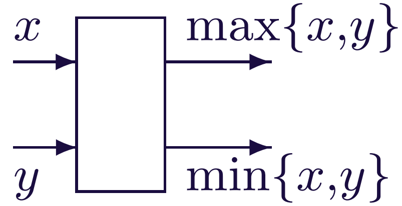
- the complete binary tree of depth $c \log n$ with alternating layers of $\wedge$ and $\vee$
- each leaf: a randomly chosen variable p_i, $i < n$

If c is a large enough constant, F will whp compute $\theta^n_{\alpha n}$, where $\alpha = (3 - \sqrt{5})/2$. A simple modification will yield any desired θ^n_m.

Unfortunately: Probabilistic construction $\Rightarrow$ no explicit formulas $\Rightarrow$ no hope for short LK-proofs of (1)–(3)

Sorting networks

A comparator network is a circuit with n inputs and n outputs using comparator gates



such that any input or output of any gate is used exactly once.

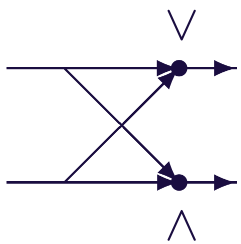
It can be evaluated on a sequence of n elements of any linearly ordered set, its output is a permutation of the input.

A comparator network is a sorting network if the output is always ordered wrt the given linear order.

Optimal sorting networks

Theorem (Ajtai, Komlós, Szemerédi '83):
It is possible to construct sorting networks of depth $O(\log n)$.

Sorting a 0-1 input $\langle x_0, \ldots, x_{n-1} \rangle$ amounts to computing $\langle \theta^n_n, \theta^n_{n-1}, \ldots, \theta^n_1 \rangle$. A comparator on a 0-1 input can be

simulated by 

Corollary: We can construct monotone circuits of depth $O(\log n)$ (hence poly-size formulas) for the threshold functions.

The strategy

One way to prove the Think Positively Conjecture:

- Formalize the AKS sorting network in a suitable theory of bounded arithmetic.
- Use the correspondence of bounded arithmetic to propositional proof systems to get poly-time Frege ($=LK$) proofs of (1)–(3).

Some issues:

- Which theory to use? It should be roughly an NC^1-theory, but the exact choice is a bit delicate.
- The AKS network relies on explicit expanders, we thus need to formalize an expander construction in bounded arithmetic. We leave this for future work.

VNC^1

VNC^1: An extension of the second-order arithmetic V^0, corresponds to (U_E-)uniform NC^1 = $ALOGTIME$.

Unfortunately, it is too weak for our purposes:

- We need to evaluate the AKS network on 0-1 inputs, i.e., a log-depth monotone circuit.
- In fully uniform NC^1, we can only evaluate log-depth circuits given by their extended connection language (ecl) of Ruzzo.
- There does not seem to be any way of computing the ecl of the AKS network, it looks like a pretty general log-depth monotone circuit.

Second try

An obvious choice: take V^0 + “log-depth circuits can be evaluated on any input”.

It does not work either, it is too strong:

- Our theory must correspond to a subclass of nonuniform NC^1, so that we can translate it to poly-size Frege proofs.
- Somewhat counterintuitively, the evaluator function for log-depth circuits is (apparently) not in nonuniform NC^1. It is mutually NC^1-Turing-reducible with log-bounded reachability in directed graphs of constant out-degree.

Solution

We develop a new theory VNC^1_*:

- Roughly, V^0 + “log-depth circuits described by Δ_1^B-formulas without second-order parameters can be evaluated on any input”.
- Contains VNC^1. Can evaluate sufficiently uniform families of log-depth circuits, such as the AKS network.
- Corresponds to a subclass of L-uniform NC^1. Translates to L-constructible Frege proofs.

Formalization

Paterson's variant of the AKS network (sans expanders) can be defined and analyzed in VNC^1_*:

Theorem: If VNC^1_* proves the existence of suitable expander graphs, it also proves the existence of log-depth sorting networks.

Corollary: Assume that VNC^1_* proves the existence of suitable expander graphs. Then MLK p-simulates LK on monotone sequents.

Open problems

Problem: Formalize expanders in VNC^1_*.

- Some work on combinatorial analysis of zig-zag-based expander constructions has been done by Koucký, Kabanets and Kolokolova.

Question: What about tree-like MLK?

- The inductive argument by AGP '02 which allows us to make do with LK-proofs of (1)–(3) results in heavily non-tree-like proofs.
- The usual simulation of dag-like Frege proofs by tree-like proofs needs $\rightarrow$.

Thank you for attention!

References

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

N. Alon, R. Boppana, *The monotone circuit complexity of Boolean functions*, Combinatorica 7 (1987), 1–22.

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

S. Cook, P. Nguyen, *Logical foundations of proof complexity*, book in preparation.

E. Jeřábek, *On theories of bounded arithmetic for* NC^1, preprint.

———, *A sorting network in bounded arithmetic*, preprint.

M. Koucký, V. Kabanets, A. Kolokolova, *Expanders made easy: The combinatorial analysis of an expander construction*, unpublished manuscript, 2007.

M. Paterson, *Improved sorting networks with* $O(\log N)$ *depth*, Algorithmica 5 (1990), 75–92.

A. Razborov, *Lower bounds on the monotone complexity of some Boolean functions*, Soviet Math. Doklady 31 (1985), 354–357.

W. Ruzzo, *On uniform circuit complexity*, J. Comput. System Sci. 22 (1981), 365–383.

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