Some News on the Proof Complexity of Deep Inference

Alessio Guglielmi

University of Bath and LORIA & INRIA Nancy-Grand Est

11 November 2009

This talk is available at `http://cs.bath.ac.uk/ag/t/dipc.pdf`

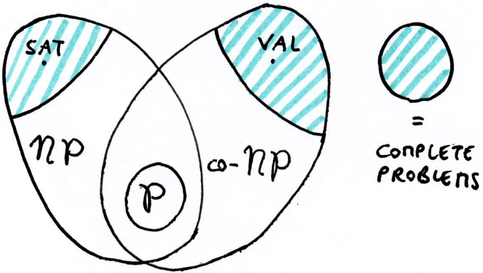
Outline

Aims of the talk:

- Put some of the current deep-inference research in the wider context of proof complexity.
- State a surprising result on cut elimination being at most quasipolynomial in deep inference (instead of exponential).
- Provide an introduction for the following talk by Tom, who will get into some details of quasipolynomial cut elimination.

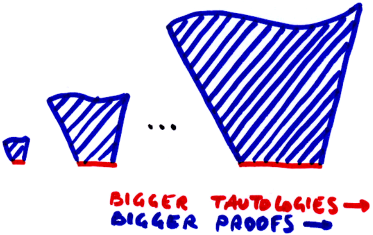
Contents:

Overview of (Some!) Complexity Classes



- $\mathcal{NP}$ = class of problems that are verifiable in polynomial time.
- SAT = 'Is a propositional formula satisfiable?' (Yes: here is a satisfying assignment.)
- co-$\mathcal{NP}$ = class of problems that are disqualifiable in polynomial time.
- VAL = 'Is a propositional formula valid?' (No: here is a falsifying assignment.)
- $\mathcal{P}$ = class of problems that can be solved in polynomial time.
- $\mathcal{NP} \neq$ co-$\mathcal{NP}$ implies $\mathcal{P} \neq \mathcal{NP}$.

Proof Systems



- Proof complexity = proof size.
- Proof system = algorithm that verifies proofs in polynomial time on their size.
- Important question: What is the relation between size of tautologies and size of minimal proofs?

Example of Proof System: Frege

Axioms:

$$A \supset (B \supset A),$$
$$(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C)),$$
$$(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B),$$

Modus ponens, or cut, rule: $\dfrac{A \quad A \supset B}{B}$.

Example:

$$\dfrac{\dfrac{}{a \supset (a \supset a)} \qquad \dfrac{\dfrac{}{a \supset ((a \supset a) \supset a)} \quad \dfrac{}{(a \supset ((a \supset a) \supset a)) \supset ((a \supset (a \supset a)) \supset (a \supset a))}}{(a \supset (a \supset a)) \supset (a \supset a)}}{a \supset a}$$

Robustness: all Frege systems are polynomially equivalent.

Example of Proof System: Gentzen Sequent Calculus

One axiom, many rules.

Example:

$$
\supset_{R}\dfrac{\vee_{L}\dfrac{\supset_{L}\dfrac{\vee_{RL}\dfrac{a \vdash a}{a \vdash a \vee (a \supset \bot)} \qquad a, \bot \vdash \bot}{a, (a \vee (a \supset \bot)) \supset \bot \vdash \bot} \qquad \supset_{L}\dfrac{\vee_{RR}\dfrac{\supset_{R}\dfrac{\supset_{L}\dfrac{a \vdash a \qquad \bot, a \vdash \bot}{a \supset \bot, a \vdash \bot}}{a \supset \bot \vdash a \supset \bot}}{a \supset \bot \vdash a \vee (a \supset \bot)} \qquad a \supset \bot, \bot \vdash \bot}{a \supset \bot, (a \vee (a \supset \bot)) \supset \bot \vdash \bot}}{a \vee (a \supset \bot), (a \vee (a \supset \bot)) \supset \bot \vdash \bot}}{a \vee (a \supset \bot) \vdash ((a \vee (a \supset \bot)) \supset \bot) \supset \bot}
$$

This is a special case of Frege, important because it admits complete and analytic proof systems (*i.e.*, cut-free proof systems, by which consistency proofs can be obtained).

Frege and Gentzen systems are polynomially equivalent.

Example of Proof System: Deep Inference

Proofs can be composed by the same operators as formulae.

Example:

$$
= \frac{\left(\mathsf{s}\,\dfrac{a \wedge \left[\bar{a} \vee \dfrac{\mathsf{t}}{\bar{a} \vee a} \right]}{\dfrac{a \wedge \dfrac{\bar{a} \vee \bar{a}}{\bar{a}}}{\mathsf{f}} \vee \dfrac{a}{a \wedge a}} \wedge \bar{a} \right)}{a \wedge \dfrac{a \wedge \bar{a}}{\mathsf{f}}}
$$

This is a generalisation of Frege, which admits complete and local proof systems (*i.e.*, where steps can be verified in constant time).

Frege and deep-inference systems are polynomially equivalent.

The calculus of structures (CoS) is now a completely developed deep inference formalism.

Proof Complexity and the $\mathcal{NP}$ Vs. co-$\mathcal{NP}$ Problem

- Theorem [Cook & Reckhow(1974)]:

  There exists an efficient proof system
  iff
  $$\mathcal{NP} = \text{co-}\mathcal{NP}$$

  where 'efficient' = admitting proofs that are verifiable in polynomial time over the size of the proved formula.

- Is there an always efficient proof system? Probably not, and this is, obviously, hard.
- Is there an optimal proof system? (in the sense that it polynomially simulates all others.) We don't know, and this is perhaps feasible.

Compressing Proofs 1

Thus, an important question is:
How can we make proofs smaller?

These are known mechanisms:

1. Use higher orders (for example, second order propositional, for propositional formulae).
2. Add substitution: $\text{sub}\,\dfrac{A}{A\sigma}$.
3. Add Tseitin extension: $p \leftrightarrow A$ (where p is a fresh atom).
4. Use the same sub-proof many times, via the cut rule.
5. Use the same sub-proof many times, in dag-ness, or cocontraction.

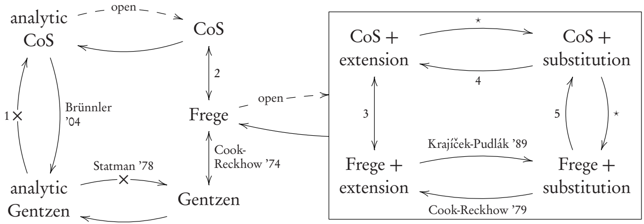
Only 5 is allowed in analytic proof systems.
4 is the most studied form of compression, and the main topic of this talk, together with 5.

Compressing Proofs 2

Some facts:

- Substitution and extension are equivalent when added to Frege and to deep inference (not a trivial result).
- Any of these systems is usually called EF (for Extended Frege) and is considered the most interesting candidate as optimal proof system.
- Deep inference has the best representation for EF (the equivalence between extension and substitution becomes almost trivial).
- The EF compression in deep inference leads to a bureaucracy-free formalism (but this is a topic for another talk).

Proof Complexity and Deep Inference



Deep inference has as small proofs as the best systems (2,3,4,5,*)
and
it has a normalisation theory
and
its analytic proof systems are more powerful than Gentzen ones (1)
and
cut elimination is $n^{O(\log n)}$, *i.e.*, quasipolynomial (instead of exponential).
(See [Jeřábek(2009), Bruscoli & Guglielmi(2009), Bruscoli et al.(2009)Bruscoli, Guglielmi, Gundersen, & Parigot]).

(Proof) System SKS [Brünnler & Tiu(2001)]

- Atomic rules:

$$\text{ai}\!\downarrow \frac{\mathsf{t}}{a \vee \bar{a}} \quad \text{aw}\!\downarrow \frac{\mathsf{f}}{a} \quad \text{ac}\!\downarrow \frac{a \vee a}{a}$$

identity *weakening* *contraction*

$$\text{ai}\!\uparrow \frac{a \wedge \bar{a}}{\mathsf{f}} \quad \text{aw}\!\uparrow \frac{a}{\mathsf{t}} \quad \text{ac}\!\uparrow \frac{a}{a \wedge a}$$

cut *coweakening* *cocontraction*

- Linear rules:

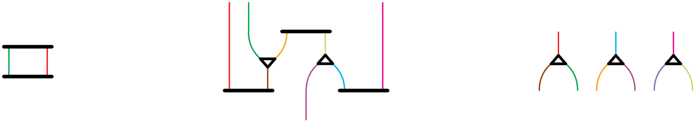
$$\mathsf{s}\frac{\alpha \wedge [\beta \vee \gamma]}{(\alpha \wedge \beta) \vee \gamma} \quad \mathsf{m}\frac{(\alpha \wedge \beta) \vee (\gamma \wedge \delta)}{[\alpha \vee \gamma] \wedge [\beta \vee \delta]}$$

switch *medial*

- Plus an '$=$' linear rule (associativity, commutativity, units).
- Rules are applied anywhere inside formulae.
- Negation on atoms only.
- Cut is atomic.
- SKS is complete and implicationally complete for propositional logic.

(Atomic) Flows

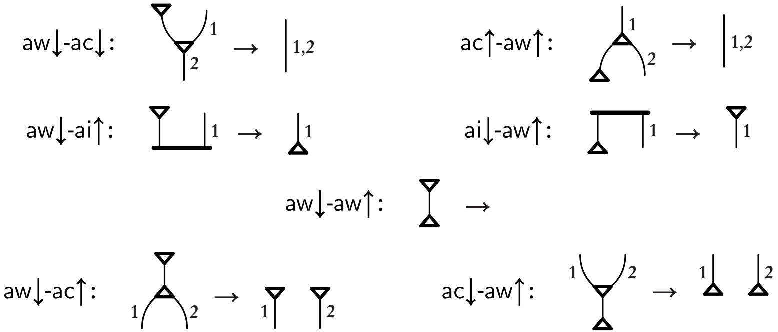
$$\mathsf{s}\,\frac{\mathsf{m}\,\dfrac{\dfrac{\mathsf{t}}{a \vee \bar{a}}}{[a \vee \mathsf{t}] \wedge [\mathsf{t} \vee \bar{a}]}}{\left[\mathsf{s}\,\dfrac{[a \vee \mathsf{t}] \wedge \bar{a}}{\dfrac{a \wedge \bar{a}}{\mathsf{f}} \vee \mathsf{t}} \vee \mathsf{t}\right]}
\qquad
=\frac{\left(\mathsf{s}\,\dfrac{a \wedge \left[\bar{a} \vee \dfrac{\mathsf{t}}{\bar{a} \vee a}\right]}{\dfrac{a \wedge \dfrac{\bar{a} \vee \bar{a}}{\bar{a}}}{\mathsf{f}} \vee \dfrac{a}{a \wedge a}} \wedge \bar{a}\right)}{a \wedge \dfrac{a \wedge \bar{a}}{\mathsf{f}}}
\qquad
\mathsf{m}\,\frac{\dfrac{a}{a \wedge a} \vee \dfrac{b}{b \wedge b}}{[a \vee b] \wedge [a \vee b]} \wedge \frac{a}{a \wedge a}$$



- Below derivations, their (atomic) flows are shown.
- Only structural information is retained in flows.
- Logical information is lost.
- Flow size is polynomially related to derivation size.

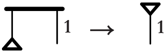
Flow Reductions: (Co)Weakening (1)

Consider these flow reductions:



Each of them corresponds to a correct derivation reduction.

Flow Reductions: (Co)Weakening (2)

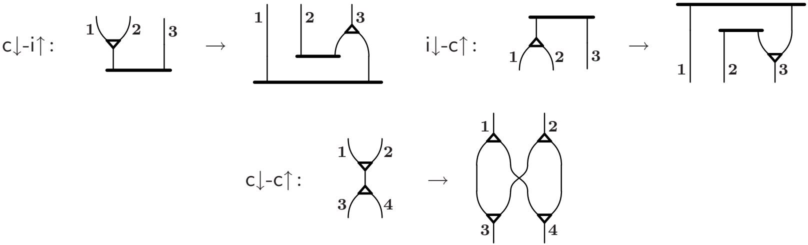
For example, ai↓-aw↑:  specifies that

$$\begin{array}{c} \Pi'' \Big\| \\ \xi\left\{\dfrac{\mathsf{t}}{a^{\epsilon} \vee \bar{a}}\right\} \\ \Phi \Big\| \\ \zeta\left\{\dfrac{a^{\epsilon}}{\mathsf{t}}\right\} \\ \Psi \Big\| \\ \alpha \end{array} \quad \text{becomes} \quad \begin{array}{c} \Pi'' \Big\| \\ \xi\left[\mathsf{t} \vee \dfrac{\mathsf{f}}{\bar{a}}\right] \\ \Phi\{a^{\epsilon}/\mathsf{t}\} \Big\| \\ \zeta\{\mathsf{t}\} \\ \Psi \Big\| \\ \alpha \end{array}$$

We can operate on flow reductions instead than on derivations: it is much easier and we get natural, syntax-independent induction measures.

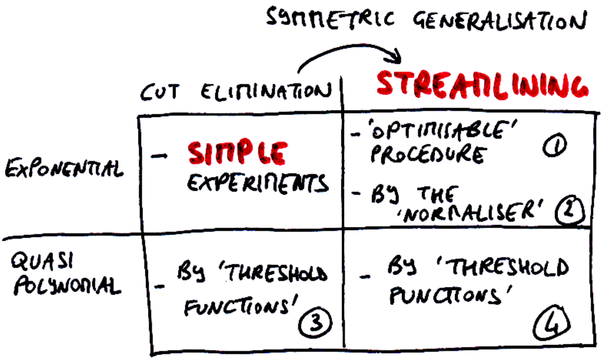
Flow Reductions: (Co)Contraction

Consider these flow reductions:



- They conserve the number and length of paths.
- Note that they can blow up a derivation exponentially.
- It's a good thing: cocontraction is a new compression mechanism (sharing?).
- Open problem: does cocontraction provide exponential compression? Conjecture: yes.

Normalisation
Overview

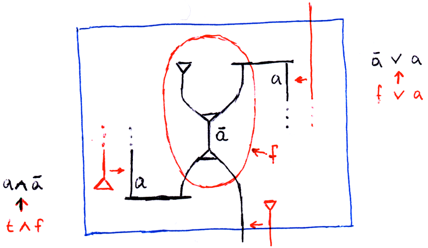


- None of these methods existed before atomic flows, none of them requires permutations or other syntactic devices.
- Quasipolynomial procedures are surprising.
- Conjecture: polynomial normalisation is possible.

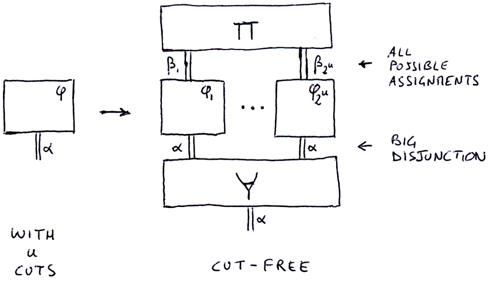
(1) [Guglielmi & Gundersen(2008)]; (2,4) forthcoming; (3) [Bruscoli et al.(2009)Bruscoli, Guglielmi, Gundersen, & Parigot].

Cut Elimination (on Proofs) by 'Experiments'

Experiment:

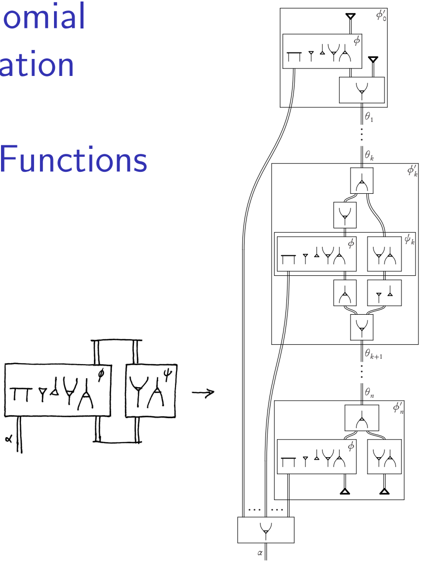


We do:



Simple, exponential cut elimination; proof generates 2^n experiments. (No use of cocontraction!)

Quasipolynomial Cut Elimination by Threshold Functions



Only $n+1$ copies of the proof are stitched together. It's complicated, Tom will explain, but note local cocontraction (= better sharing, not available in Gentzen).

Some Comments

(that don't all follow from what precedes)

- (Exponential) normalisation does not depend on logical rules.
- It only depends on structural information, *i.e.*, geometry.
- Normalisation is extremely robust.
- Deep inference's locality is key.
- Complexity-wise, deep inference is as powerful as the best formalisms,
- and more powerful if analiticity is requested.
- Deep inference is the continuation of Girard politics with other means.

In my opinion, much of the future of structural proof theory is in geometric methods: we have to free ourselves from the tyranny of syntax (so, war to bureaucracy!).

References

Brünnler, K., & Tiu, A. F. (2001).
A local system for classical logic.
In R. Nieuwenhuis, & A. Voronkov (Eds.) *LPAR 2001*, vol. 2250 of *Lecture Notes in Computer Science*, (pp. 347–361). Springer-Verlag.
http://www.iam.unibe.ch/~kai/Papers/lcl-lpar.pdf.

Bruscoli, P., & Guglielmi, A. (2009).
On the proof complexity of deep inference.
ACM Transactions on Computational Logic, *10*(2), 1–34.
Article 14. http://cs.bath.ac.uk/ag/p/PrComplDI.pdf.

Bruscoli, P., Guglielmi, A., Gundersen, T., & Parigot, M. (2009).
Quasipolynomial normalisation in deep inference via atomic flows and threshold formulae.
Submitted. http://cs.bath.ac.uk/ag/p/QuasiPolNormDI.pdf.

Cook, S., & Reckhow, R. (1974).
On the lengths of proofs in the propositional calculus (preliminary version).
In *Proceedings of the 6th annual ACM Symposium on Theory of Computing*, (pp. 135–148). ACM Press.

Guglielmi, A., & Gundersen, T. (2008).
Normalisation control in deep inference via atomic flows.
Logical Methods in Computer Science, *4*(1:9), 1–36.
http://www.lmcs-online.org/ojs/viewarticle.php?id=341.

Jeřábek, E. (2009).
Proof complexity of the cut-free calculus of structures.
Journal of Logic and Computation, *19*(2), 323–339.
http://www.math.cas.cz/~jerabek/papers/cos.pdf.