This note is superseded by ***On the Proof Complexity of Deep Inference*** *by Paola Bruscoli and Alessio Guglielmi, 2008, ACM Transactions on Computational Logic, URL: http://cs.bath.ac.uk/ag/p/PrComplDI.pdf.*

AG12

POLYNOMIAL SIZE DEEP-INFERENCE PROOFS INSTEAD OF EXPONENTIAL SIZE SHALLOW-INFERENCE PROOFS

Alessio Guglielmi (Bath)

10.8.2004 - updated on 22.9.2007

By a simple example, I show how deep inference can provide for an exponential speed-up in the size of proofs with respect to shallow inference. In particular, there are classes of tautologies whose cut-free proofs only grow polynomially with their size, instead of exponentially, as in the sequent calculus.

There are two areas where the use of deep inference can lead to lower complexity: complexity of cut elimination and complexity in proof search. In both cases the greater liberality of deep inference rules is advantageous. In many important cases, the complexity passes from being exponential to being polynomial (with low exponent). Here we concentrate on the proof search case.

The big picture is the following:

- with shallow inference one has (seemingly!, relatively!) low nondeterminism and long proofs;

- with (uncontrolled!, naif!) deep inference one has high nondeterminism and short proofs.

One goal is to show that in the more liberal framework of deep inference one can develop search algorithms that drastically cut down on nondeterminism and still find short proofs (for example, something along the lines of a deep version of uniform provability [MNPS]). To this purpose, I’d like to remind the reader that very successful techniques like resolution are immediately available with deep inference, contrary to what happens in shallow inference [AG].

In any case, a preliminary technical point we should make is that the proofs available in deep inference are indeed shorter than those available in shallow inference. Of course, miracles are unlikely, so, since it's reasonable to believe that NP $\neq$ coNP, we cannot reasonably hope for polynomial-size proofs in all cases. But we can of course hope for *exponential speed-ups* with respect to other deduction formalisms, which we do get!

This area is very active. In general, people study classes of tautologies and try to establish bounds on the size of their proofs, in systems with and without cut. One of the most studied such classes of tautologies is derived from the pigeonhole principle. For these formulae, in shallow inference, proofs with cuts can be polynomial (result by Buss), while proofs without cuts must be exponential (result by Haken).

Below, I show a simple argument which proves that there are polynomial-size proofs for a class of tautologies, studied by Richard Statman, that has the same properties of pigeonhole for our purposes here, but it’s simpler: cut-free-shallow/exponential, with-cut-shallow/polynomial, cut-free-deep/polynomial.

In fact, *every* with-cut-shallow proof can be transformed into a deep-inference proof, in system SKS [KB], whose complexity only differs for a polynomial (as a function of the size of the conclusion) and which only adopts a finite-choice version of the cut rule. In this case, the cut rule behaves like a contraction: it completely loses the infinitary character that prevents its implementation in proof-search. The necessary transformations are outlined in [KB] and [BG]: 1) transform a proof with cuts in the sequent calculus into a proof in system SKS (see [KB], Theorem 2.3.3); 2) transform this proof into one that only employs finite choice cuts ([BG], Section 3).

But what about proofs in a system where cuts are completely absent, including the finite choice, harmless ones? For these systems we don’t know (so far) any automatic transformation that could transform with-cut-shallow polynomial proofs into cut-free-deep polynomial proofs.

Nonetheless, some ideas seem general enough to be widely exploitable. One feature that helps in reducing the complexity of proofs is the absence of branching in deep inference. Thanks to this, I will show below how the Statman class of tautologies receives fair polynomial treatment by CoS system KS. It's a rather simple example that makes the point in a striking way.

Polynomial Cut-free Proofs for Statman’s Tautologies

We start from propositional variables c_i and d_i, for $i \geq 1$. We then define:

$$F_k = \bigwedge_{j=1}^{k} (c_j \vee d_j) \ , \quad \text{for } k \geq 1 \ ;$$

$$A_1 = c_1 \ ;$$
$$B_1 = d_1 \ ;$$
$$\ldots$$
$$A_{i+1} = F_i \Rightarrow c_{i+1} \ ;$$
$$B_{i+1} = F_i \Rightarrow d_{i+1} \ ;$$

$$G_n = ((A_1 \vee B_1) \wedge \ldots \wedge (A_n \vee B_n)) \Rightarrow (c_n \vee d_n) \ .$$

For example:

$$G_1 = (c_1 \vee d_1) \Rightarrow (c_1 \vee d_1) \ ,$$

$$\begin{array}{l}
G_2 = ((\ c_1 \vee d_1) \qquad\qquad \wedge \\
\qquad (((c_1 \vee d_1) \Rightarrow c_2) \vee \\
\qquad\ \ ((c_1 \vee d_1) \Rightarrow d_2) \\
\qquad) \\
\quad\ \ ) \Rightarrow (c_2 \vee d_2) \ ,
\end{array}$$

$$\begin{array}{l}
G_3 = ((\ c_1 \vee d_1 \\
\qquad) \qquad\qquad\qquad\qquad\qquad\qquad \wedge \\
\qquad (((c_1 \vee d_1) \Rightarrow c_2) \vee \\
\qquad\ \ ((c_1 \vee d_1) \Rightarrow d_2) \\
\qquad) \qquad\qquad\qquad\qquad\qquad\qquad \wedge \\
\qquad ((((c_1 \vee d_1) \wedge (c_2 \vee d_2)) \Rightarrow c_3) \vee \\
\qquad\ \ (((c_1 \vee d_1) \wedge (c_2 \vee d_2)) \Rightarrow d_3) \\
\qquad) \\
\quad\ \ ) \Rightarrow (c_3 \vee d_3) \ .
\end{array}$$

One can easily check that, for $n \geq 1$, the formulae G_n are tautologies. The semantic argument for showing this is straightforward and amounts to checking the chain of implications

$$(c_1 \vee d_1) \Rightarrow \ldots \Rightarrow (c_n \vee d_n) \ ,$$

from left to right.

In the sequent calculus, the size of proofs of formulae G_n grows exponentially, if cuts are not allowed. In order to get an intuition about this, consider G_3 and the one-sided sequent one immediately obtains from it:

$$\vdash \neg A_1 \wedge \neg B_1 \ , \ \neg A_2 \wedge \neg B_2 \ , \ \neg A_3 \wedge \neg B_3 \ , \ c_3 \ , \ d_3 \ ,$$

which can be expanded to

$$\begin{array}{l}
\vdash \neg c_1 \wedge \neg d_1 \qquad\qquad\qquad\qquad\quad , \\
\quad (c_1 \vee d_1) \wedge \neg c_2 \wedge \\
\quad (c_1 \vee d_1) \wedge \neg d_2 \qquad\qquad\qquad\quad , \\
\quad (c_1 \vee d_1) \wedge (c_2 \vee d_2) \wedge \neg c_3 \wedge \\
\quad (c_1 \vee d_1) \wedge (c_2 \vee d_2) \wedge \neg d_3 \quad\ , \\
\quad c_3 \ , \ d_3 \ .
\end{array}$$

The following is a possible proof, of which one branch is shown in part (all the others are similar):

$$\begin{array}{c} \vdots \\ \hline \vdash \neg c_1 , (c_1 \vee d_1) \wedge \neg d_2 , (c_1 \vee d_1) \wedge (c_2 \vee d_2) \wedge \neg c_3 , c_3 , d_3 \\ = \\ \vdash \neg A_1, \neg B_2, \neg A_3, c_3, d_3 \\ \hline \end{array}$$

$$\dfrac{\dfrac{\vdots}{\vdash \neg A_1, \neg A_2 \wedge \neg B_2, \neg A_3 \wedge \neg B_3, c_3, d_3} \qquad \dfrac{\vdots}{\vdash \neg B_1, \neg A_2 \wedge \neg B_2, \neg A_3 \wedge \neg B_3, c_3, d_3}}{\vdash \neg A_1 \wedge \neg B_1, \neg A_2 \wedge \neg B_2, \neg A_3 \wedge \neg B_3, c_3, d_3}$$

Clearly, for G_n there are 2^n branches. Statman [RS] proved that in a cut free system the size of proofs always grows exponentially with n.

This is not the case if we allow the cut rule, because in this case we can exploit the fact that all sequents

$$\vdash \neg F_i , \neg A_{i+1} \wedge \neg B_{i+1} , F_{i+1}$$

are provable with bounded complexity proofs, and then join them by using cuts, what is linear in n.

In the cut free CoS system KS, there are linear proofs. I show just an example for G_3 but the general pattern is the same (the syntax below is the CoS one):

$$
\begin{array}{rl}
 & \mathtt{t} \\ \cline{2-2}
\mathtt{i}\downarrow & [(-c_3,-d_3)\ ,\ c_3,d_3] \\ \cline{2-2}
2\times\mathtt{i}\downarrow & [([c_2,d_2,(-c_2,-d_2)],-c_3,[c_2,d_2,(-c_2,-d_2)],-d_3)\ ,\ c_3,d_3] \\ \cline{2-2}
2\times\mathtt{s} & [(-c_2,-d_2),(-c_2,-d_2)\ , \\
 & \ ([c_2,d_2],-c_3,[c_2,d_2],-d_3)\ ,\ c_3,d_3] \\ \cline{2-2}
1\times\mathtt{c}\downarrow & [(-c_2,-d_2)\ , \\
 & \ ([c_2,d_2],-c_3,[c_2,d_2],-d_3)\ ,\ c_3,d_3] \\ \cline{2-2}
4\times\mathtt{i}\downarrow & [([c_1,d_1,(-c_1,-d_1)],-c_2,[c_1,d_1,(-c_1,-d_1)],-d_2)\ , \\
 & \ ([c_1,d_1,(-c_1,-d_1)],[c_2,d_2],-c_3,[c_1,d_1,(-c_1,-d_1)],[c_2,d_2],-d_3)\ , \\
 & \ c_3,d_3] \\ \cline{2-2}
4\times\mathtt{s} & [(-c_1,-d_1),(-c_1,-d_1),(-c_1,-d_1),(-c_1,-d_1)\ , \\
 & \ ([c_1,d_1],-c_2,[c_1,d_1],-d_2)\ , \\
 & \ ([c_1,d_1],[c_2,d_2],-c_3,[c_1,d_1],[c_2,d_2],-d_3)\ ,\ c_3,d_3] \\ \cline{2-2}
3\times\mathtt{c}\downarrow & [(-c_1,-d_1)\ , \\
 & \ ([c_1,d_1],-c_2,[c_1,d_1],-d_2)\ , \\
 & \ ([c_1,d_1],[c_2,d_2],-c_3,[c_1,d_1],[c_2,d_2],-d_3)\ ,\ c_3,d_3]
\end{array}
\quad .
$$

The secret of success here is, of course, the absence of branching in CoS.

Remark To be precise, one has to be more careful than I was with brackets and associativity; however, in all the arguments above, the substance would not change.

References

[AG] Alessio Guglielmi. Resolution in the calculus of structures. Manuscript, 2003. URL: http://cs.bath.ac.uk/ag/p/AG10.pdf.

[BG] Kai Brünnler and Alessio Guglielmi. A first order system with finite choice of premises. In Hendricks *et al.*, editors, *First-Order Logic Revisited*. Logos Verlag, Berlin, 2004. URL: http://www.iam.unibe.ch/~kai/Papers/FinitaryFOL.pdf.

[KB] Kai Brünnler. Deep inference and symmetry in classical proofs. PhD thesis, Technische Universität Dresden, 2003. URL: http://www.iam.unibe.ch/~kai/Papers/phd.pdf.

[MNPS] D. Miller, G. Nadathur, F. Pfenning and A. Scedrov. Uniform proofs as a foundation for logic programming. *Annals of Pure and Applied Logic*. 51:125-157, 1991.

[RS] R. Statman. Bounds for proof-search and speed-up in predicate calculus. *Annals of Mathematical Logic*. 15:225-287, 1978.

Web Site

[WS] http://alessio.guglielmi.name/res/cos.