Geometric Ideas in the Design of Efficient and Natural Proof Systems

Alessio Guglielmi

University of Bath

Joint work with
Paola Bruscoli, Tom Gundersen, Michel Parigot and Lutz Straßburger

24 September 2013

This talk is available at http://cs.bath.ac.uk/ag/t/GIDENPS.pdf
Deep inference web site: http://alessio.guglielmi.name/res/cos/
Outline

Problem: Getting rid of bureaucracy in proofs

Open Deduction (Deep Inference): locality (atomicity + linearity)

Deep Inference and Proof Complexity: proofs are small, so it is OK

Atomic Flows: locality brings geometry

Cut Elimination by Experiments: Gentzen’s structure is too rigid

Normalisation with Atomic Flows: geometry is enough to normalise

Substitution: more geometry, more efficiency, more naturality
Problem: getting rid of bureaucracy in proofs

▶ From ‘different’ Gentzen sequent proofs we get proof nets (Girard),
▶ but they are too small: for propositional logic, they probably do not form a proof system.

Picture taken from [Straburger, 2006]
Proof Systems

- **Proof system** = algorithm checking proofs in polytime.
- Theorem (Cook and Reckhow):

  \[ \exists \text{ super proof system} \]
  \[ \text{iff} \]
  \[ \text{NP} = \text{co-NP} \]

  where

  super = with polysize proofs over each proved tautology
(Proof) System SKS  
[Brünner and Tiu, 2001]

- **Atomic rules:**

- **Linear rules:**

  - Plus an ‘=’ linear rule (associativity, commutativity, units).
  - Negation on atoms only.
  - Cut is atomic.
  - SKS is complete for propositional logic.
Examples in Open Deduction (Deep Inference)

\[
\frac{a \lor b}{a \land a} \quad \frac{b \land b}{a \land a}
\]

\[
\frac{[a \lor b] \land [a \lor b]}{a \land a}
\]

\[
\frac{t}{a \lor \bar{a}}
\]

\[
\frac{[a \lor t] \land [t \lor \bar{a}]}{m}
\]

\[
\frac{[a \lor t] \land \bar{a}}{s}
\]

\[
\frac{a \land \bar{a}}{a \lor \bar{a}} \quad \frac{\lor t}{[a \lor t] \land \bar{a}}
\]

\[
\frac{\lor t}{f}
\]

Proofs are composed by the same operators as formulae.

Top-down symmetry: so inference steps can be made atomic (the medial rule, m, is impossible in Gentzen).

(In [Guglielmi et al., 2010a].)
Locality

Deep inference allows \textit{locality}, \hspace{0.5cm} i.e.,

inference steps can be \textit{checked in constant time} (so, they are small).

\textit{E.g.}, atomic cocontraction:

\[
\frac{a}{a \land a} \lor \frac{b}{b \land b} \land \frac{a}{a \land a} \lor \frac{[a \lor b] \land [a \lor b]}{m}
\]

\textbf{In Gentzen:}

\begin{itemize}
  \item no locality for (co)contraction (counterexample in [Brünnler, 2004]),
  \item no local reduction of cut into atomic form.
\end{itemize}
Overview and Slogans

Deep inference = locality (+ symmetry).

Locality = linearity + atomicity.

Geometry = syntax independence (elimination of bureaucracy).

Locality $\rightarrow$ geometry $\rightarrow$ semantics of proofs.
Deep Inference and Proof Complexity

Open deduction has as small proofs as the best formalisms and it has a normalisation theory and its cut-free proof systems are more powerful than Gentzen ones and cut elimination is quasipolynomial (instead of exponential). (See [Jeřábek, 2009, Bruscoli and Guglielmi, 2009, Bruscoli et al., 2010]).
Atomic Flows

Below proofs, 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)

Each flow reduction corresponds to a correct proof reduction.
Flow Reductions: (Co)Weakening (2)

E.g., \( \begin{array}{c}
\Delta \\
\end{array} \) \( \rightarrow \) \( \triangledown \) specifies that

\[
\text{\( \Pi'' \)} \\
\xi \left\{ \begin{array}{l}
t \\
\frac{a^\varepsilon \lor \bar{a}}{\phi}
\end{array} \right\} \\
\Phi \mid \\
\zeta \left\{ \begin{array}{l}
a^\varepsilon \\
t
\end{array} \right\} \\
\Psi \mid \\
\alpha
\]

becomes

\[
\text{\( \Pi'' \)} \\
\xi \left[ t \lor \frac{f}{\bar{a}} \right] \\
\Phi \{a^\varepsilon /t\} \mid \\
\zeta \{t\} \\
\Psi \mid \\
\alpha
\]

We can operate on flow reductions instead than on derivations:

- much easier,
- we get natural, syntax-independent induction measures.
Flow Reductions: (Co)Contraction

These reductions conserve the number and length of paths.

Open problem: does cocontraction yield exponential compression?
Cut Elimination by ‘Experiments’

We do:

- Simple, exponential cut elimination;
- $2^n$ experiments, where $n$ is the number of atoms;
- fairly syntax independent method.

The secret of success is in the proof composition mechanism.

**WHY IS THIS IMPOSSIBLE IN THE SEQUENT CALCULUS?**
Generalising the Cut-Free Form

- Normalised proof:

- Normalised derivation:

- The symmetric form is called streamlined.

- Cut elimination is a corollary of streamlining.

- We just need to break the paths between identities and cuts, and (co)weakenings do the rest.
How Do We Break Paths?

With the path breaker [Guglielmi et al., 2010b]:

Even if there is a path between identity and cut on the left, there is none on the right.
We Can Do This on Derivations, of Course

\[ \frac{A \quad \Psi}{[a \lor \bar{a}] \land A} \quad \frac{B \lor (a \land \bar{a})}{B} \rightarrow \]

\[ \frac{A}{((a \lor \bar{a}) \land A) \land A} \quad \frac{([a \lor \bar{a}] \land A) \land A}{B \lor ([a \lor \bar{a}] \land A) \land A} \quad \frac{([B \lor (a \land \bar{a})] \land A)}{B \lor ([B \lor (a \land \bar{a})] \land A)} \quad \frac{B \lor [B \lor ([a \lor \bar{a}] \land A)]}{B \lor [B \lor (a \land \bar{a})]} \quad \frac{\{c \uparrow, a \downarrow, =\}}{\{c \downarrow, a \uparrow, \bar{a}, =\}} \]

- We can compose this as many times as there are paths between identities and cut.
- We obtain a family of normalisers that only depends on \( n \).
- The construction is exponential.
- Finding something like this is unthinkable without flows.
Example for $n = 2$

Given a derivation $\Phi$ where the atoms $a$ and $b$ occur, such that the atomic flow associated with $\Phi$ is $\phi_1 \phi_2 \psi_1$, where $\phi_1$ is the atomic flow associated with $a$, $\phi_2$ is the atomic flow associated with $b$ and $a$ and $b$ are the only non-weakly-streamlined atoms in $\Phi$, then the atomic flow associated with $\text{Norm}_2(a, b, \text{Core}(\Phi))$ is $\phi_1 \phi_1 \phi_1 \phi_1 \phi_1 \phi_1 \phi_1 \phi_1$.
Quasipolynomial Cut Elimination by Threshold Functions

Figure 5. Atomic flow of a proof in cut-free form.

where \( \psi \) is the union of flows \( \phi_1, \ldots, \phi_n \), and where we denote by \( \alpha \) the edges corresponding to the atom occurrences appearing in the conclusion \( \alpha \) of \( \Pi \). We then have that, for \( 0 < k < n \), the flow of \( \Phi_k \) is \( \phi_k' \), as in Figure 5, where \( \psi_k \) is the flow of the derivation \( \Psi_k \).

7. Normalisation Step 3: Analytic Form

In this section, we show that we can get proofs in analytic SKS, i.e., system aSKS, in quasipolynomial time from proofs in SKS.

Transforming a proof in cut-free form into an analytic one requires eliminating co-weakening rule instances. This can be done by transformations that are the dual of those over weakening instances, employed in Step (1) of the proof of Theorem 12.

Theorem 27. Given any proof \( \Pi \) of \( \alpha \) in SKS, we can construct a proof of \( \alpha \) in aSKS in time quasipolynomial in the size of \( \Pi \).

- Only \( n + 1 \) copies of the proof are stitched together.
- Note local cocontraction (= better sharing, not available in Gentzen).
Formalism B: Extending with Substitution

Achieving the power of Frege + extension (possibly optimal proof system) by incorporating substitution, guided by the geometry of flows:

\[
\left( \frac{\text{Syntax}}{\text{Semantics}} \right) \rightarrow \quad =
\]

\[
\text{Truth tables} \quad \text{Frege systems} \quad \text{Gentzen formalisms} \quad \text{Calculus of structures} \quad \text{Open deduction} \quad \text{Atomic flows} \quad \text{Girard proof nets}
\]

\[
\text{late 1800s} \quad \sim 1900 \quad 1935 \quad 2001 \quad 2010 \quad 2008 \quad 1987
\]
Example of Flow Substitution

Note the variety of shapes, all of which are equivalent. This is far more flexible than permutation of rules and similar Gentzen mechanisms.
Lifting Substitution to Proofs

Consider the following two synchronal open deduction derivations:

\[
\phi = \frac{t}{i\downarrow} \quad \frac{a}{c\uparrow} \quad \frac{a \lor \bar{a}}{a \land a} \quad \frac{\bar{a} \lor \bar{a}}{c\downarrow} \quad \frac{(a \land a) \lor \bar{a}}{w\uparrow} \quad \frac{\bar{t}}{t} 
\]

and

\[
\psi = \frac{b \lor f}{b \lor \bar{b}} \quad \frac{\bar{b} \lor (\bar{b} \lor t)}{b \lor \bar{b}} .
\]

We want to define a denotation for the formal substitution \( \phi|a \leftarrow \psi \). One element in the set of denotations of \( \phi|a \leftarrow \psi \) is

\[
\frac{t}{i\downarrow} \quad \frac{b \lor f}{c\uparrow} \quad \frac{\left[ b \lor \bar{b} \right] \land [b \lor f]}{b \lor \bar{b}} \quad \frac{(\bar{b} \lor t) \lor (\bar{b} \lor \bar{b})}{c\downarrow} \quad \frac{\left( b \lor \bar{b} \right) \lor \left( b \lor \bar{b} \right)}{w\uparrow} \quad \frac{\bar{t}}{t} .
\]
Conclusion

- We are interested in proof composition (so in the first and second order propositional proof theory).
- Composition in Gentzen is rigid (it was designed for consistency proofs, not much else).
- Deep inference composition is free and yields local proof systems.
- Locality = linearity + atomicity, so we are doing an extreme form of linear logic.
- Because of locality we obtain a sort of geometric control over proofs.
- So we obtain an efficient and natural formalism for proofs, where more proof theory can be done with lower complexity.
- We are obtaining interesting notions of proof identity.

This talk is available at http://cs.bath.ac.uk/ag/t/GIDENPS.pdf
Deep inference web site: http://alessio.guglielmi.name/res/cos/

*Deep Inference and Symmetry in Classical Proofs.*
Logos Verlag, Berlin.
http://www.iam.unibe.ch/~kai/Papers/phd.pdf.


A local system for classical logic.


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


A quasipolynomial cut-elimination procedure in deep inference via atomic flows and threshold formulæ.
http://cs.bath.ac.uk/ag/p/QPNDI.pdf.


A proof calculus which reduces syntactic bureaucracy.


Proof nets and the identity of proofs.
Technical Report 6013, INRIA.
http://hal.inria.fr/docs/00/11/43/20/PDF/RR-6013.pdf.


Proof complexity of the cut-free calculus of structures.