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

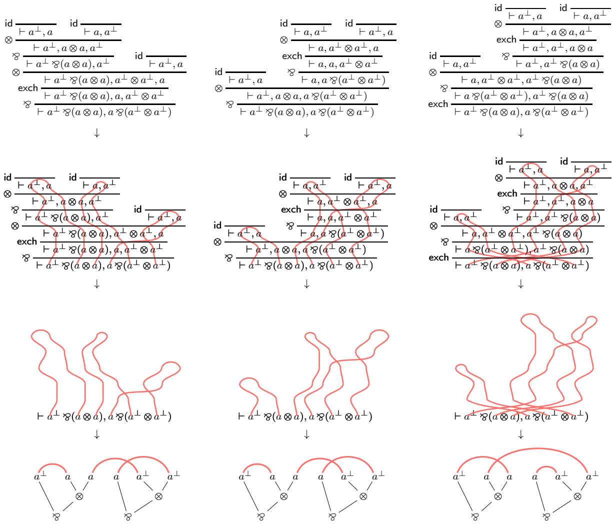
Atomic Flows: locality brings geometry

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



Picture taken from [Straßburger, 2006]

- 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.

Proof Systems

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

$\exists$ *super proof system*

iff

NP $=$ co-NP

where

super = with polysize proofs over each proved tautology

(Proof) System SKS [Brünnler and 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:

$$\text{s}\,\frac{A \wedge [B \vee C]}{(A \wedge B) \vee C} \qquad \text{m}\,\frac{(A \wedge B) \vee (C \wedge D)}{[A \vee C] \wedge [B \vee D]}$$

switch — *medial*

- 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)

- $$\left(\mathsf{m}\,\dfrac{\dfrac{a}{a\wedge a}\vee\dfrac{b}{b\wedge b}}{[a\vee b]\wedge[a\vee b]}\right)\wedge\dfrac{a}{a\wedge a}$$

- $$\mathsf{s}\,\dfrac{\mathsf{m}\,\dfrac{\dfrac{\mathsf{t}}{a\vee\bar{a}}}{[a\vee\mathsf{t}]\wedge[\mathsf{t}\vee\bar{a}]}}{\left[\mathsf{s}\,\dfrac{[a\vee\mathsf{t}]\wedge\bar{a}}{\dfrac{a\wedge\bar{a}}{\mathsf{f}}\vee\mathsf{t}}\vee\mathsf{t}\right]}$$

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 locality,

i.e.,

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

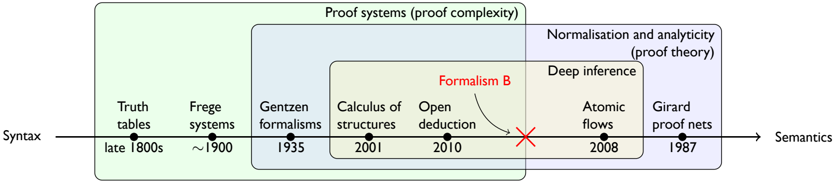
E.g., atomic cocontraction:

$$\mathsf{m}\,\dfrac{\dfrac{a}{a \wedge a} \vee \dfrac{b}{b \wedge b}}{[a \vee b] \wedge [a \vee b]} \quad \wedge \quad \dfrac{a}{a \wedge a}$$

In Gentzen:

- no locality for (co)contraction (counterexample in [Brünnler, 2004]),
- no local reduction of cut into atomic form.

Overview and Slogans



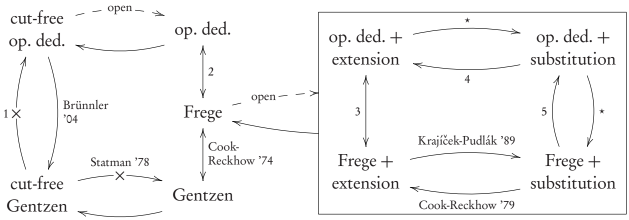
Deep inference = locality (+ symmetry).

Locality = linearity + atomicity.

Geometry = syntax independence (elimination of bureaucracy).

Locality $\rightarrow$ geometry $\rightarrow$ semantics of proofs.

Deep Inference and Proof Complexity



$\longrightarrow =$ 'polynomially simulates'.

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

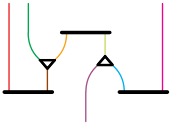
and

cut elimination is quasipolynomial (instead of exponential).

(See [Jeřábek, 2009, Bruscoli and Guglielmi, 2009, Bruscoli et al., 2010]).

Atomic Flows

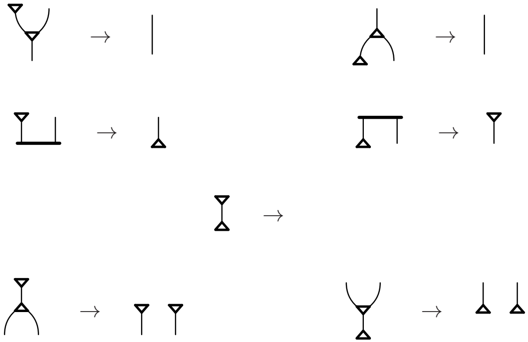
$$\mathsf{s}\,\dfrac{\mathsf{m}\,\dfrac{\dfrac{\mathsf{t}}{a\vee\bar a}}{[a\vee \mathsf{t}]\wedge[\mathsf{t}\vee\bar a]}}{\left[\mathsf{s}\,\dfrac{[a\vee \mathsf{t}]\wedge\bar a}{\dfrac{a\wedge\bar a}{\mathsf{f}}\vee \mathsf{t}}\quad\vee\quad \mathsf{t}\right]}
=\dfrac{\left(\mathsf{s}\,\dfrac{a\wedge\left[\bar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



Below proofs, their (atomic) flows are shown:

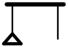
- only structural information is retained in flows;
- logical information is lost;
- flow size is polynomially related to derivation size.

Flow Reductions: (Co)Weakening (1)



Each flow reduction corresponds to a correct proof reduction.

Flow Reductions: (Co)Weakening (2)

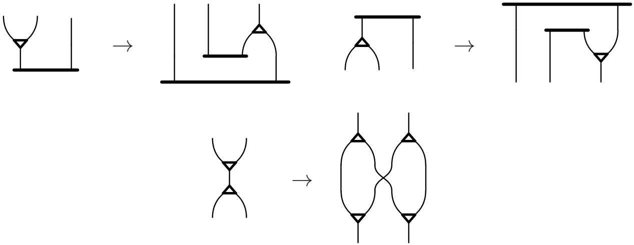
E.g.,  $\rightarrow$  specifies that

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

We can operate on flow reductions instead than on derivations:

- much easier,
- we get natural, syntax-independent induction measures.

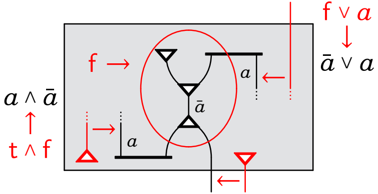
Flow Reductions: (Co)Contraction



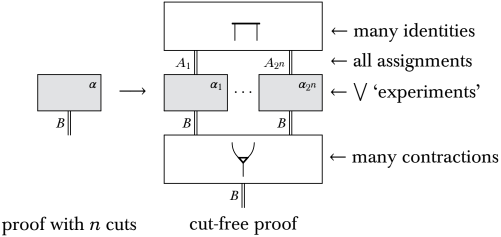
- These reductions conserve the number and length of paths.
- Open problem: does cocontraction yield exponential compression?

Cut Elimination by 'Experiments'

Experiment over a proof:



We do:



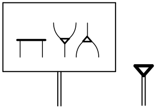
- Simple, exponential cut elimination;
- 2^n experiments, where n is the number of atoms;
- fairly syntax independent method.

The secret of success is in the proof composition mechanism.

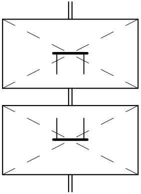
WHY IS THIS IMPOSSIBLE IN THE SEQUENT CALCULUS?

Generalising the Cut-Free Form

- Normalised proof:



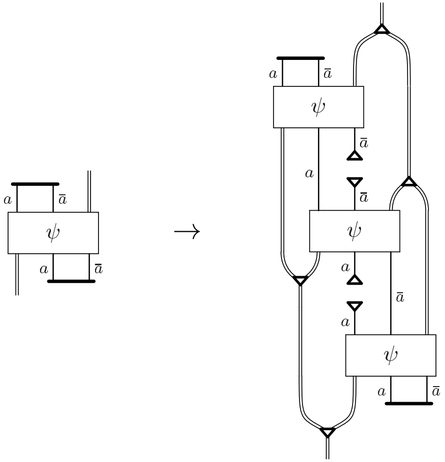
- Normalised derivation:



- 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]:



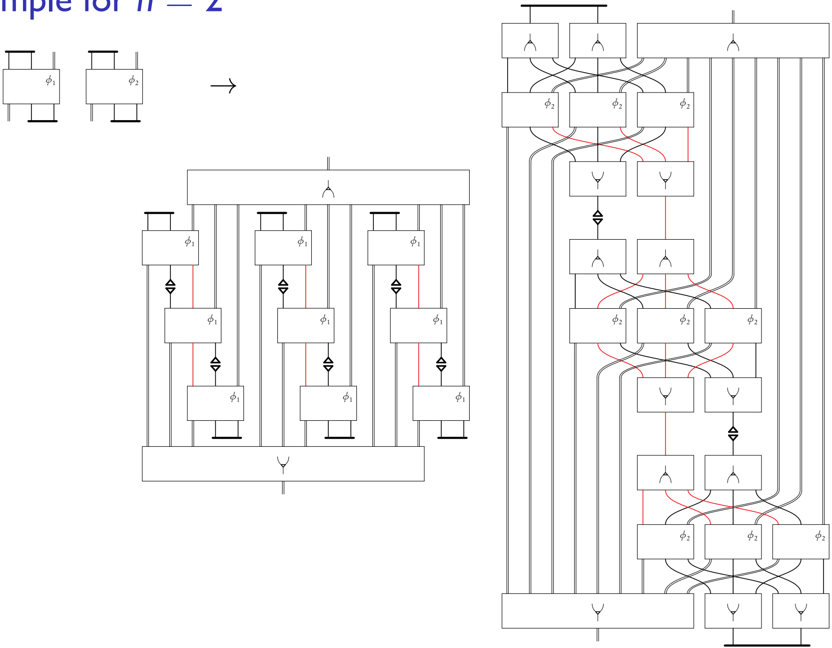
Even if there is a path between identity and cut on the left, there is none on the right.

We Can Do This on Derivations, of Course

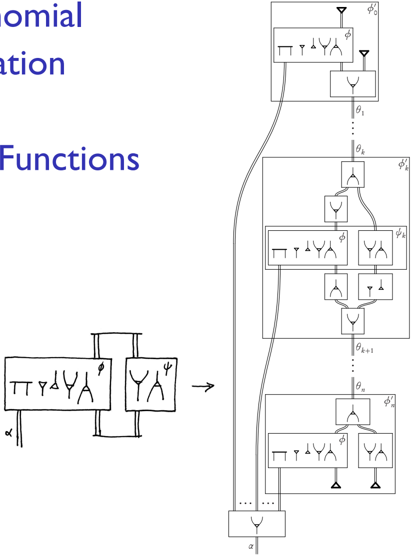
$$\dfrac{\dfrac{A}{[a \vee \bar{a}] \wedge A}\; \begin{array}{c} \Psi \Big\| \end{array}}{\dfrac{B \vee (a \wedge \bar{a})}{B}} \quad \longrightarrow \quad \begin{array}{c} A \\ \Big\| \{\mathsf{c}\!\uparrow, \mathsf{ai}\!\downarrow, =\} \\ (([a \vee \bar{a}] \wedge A) \wedge A) \wedge A \\ {\scriptstyle (\Psi \wedge A) \wedge A} \Big\| \\ ([B \vee (a \wedge \bar{a})] \wedge A) \wedge A \\ {\scriptstyle \Phi_a \wedge A} \Big\| \\ [B \vee ([a \vee \bar{a}] \wedge A)] \wedge A \\ {\scriptstyle [B \vee \Psi] \wedge A} \Big\| \\ B \vee ([B \vee (a \wedge \bar{a})] \wedge A) \\ {\scriptstyle B \vee \Phi_{\bar{a}}} \Big\| \\ B \vee [B \vee ([a \vee \bar{a}] \wedge A)] \\ {\scriptstyle B \vee [B \vee \Psi]} \Big\| \\ B \vee [B \vee [B \vee (a \wedge \bar{a})]] \\ \Big\| \{\mathsf{c}\!\downarrow, \mathsf{ai}\!\uparrow, =\} \\ B \end{array}$$

- 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 $n = 2$

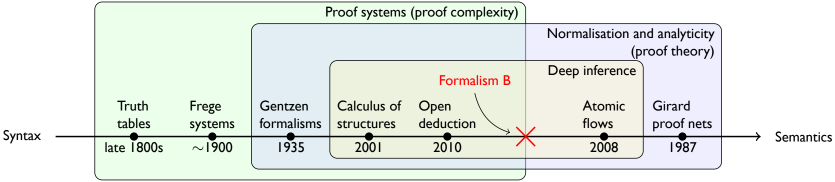


Quasipolynomial Cut Elimination by Threshold Functions

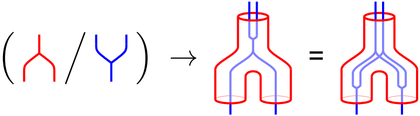


- Only $n + 1$ copies of the proof are stitched together.
- Note local cocontraction (= better sharing, not available in Gentzen).

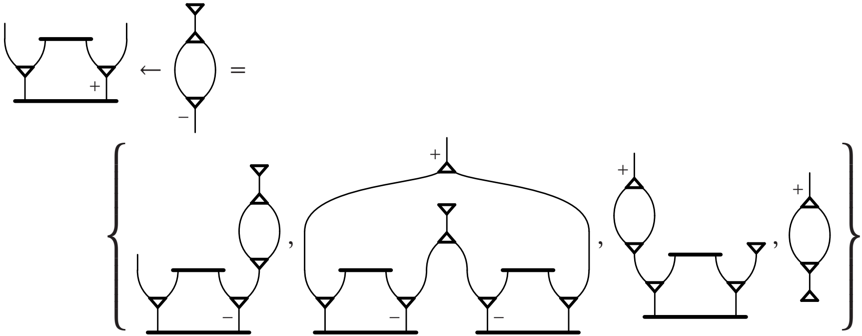
Formalism B: Extending with Substitution



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



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:

$$\phi = {\scriptstyle =}\,\dfrac{{\scriptstyle \mathsf{i}\downarrow}\,\dfrac{\mathsf{t}}{{\scriptstyle \mathsf{c}\uparrow}\,\dfrac{a}{a\wedge a}\vee\bar{a}}\;\vee\;\bar{a}}{(a\wedge a)\;\vee\;{\scriptstyle \mathsf{c}\downarrow}\,\dfrac{\bar{a}\vee\bar{a}}{{\scriptstyle \mathsf{w}\uparrow}\,\dfrac{\bar{a}}{\mathsf{t}}}} \qquad \text{and} \qquad \psi = \dfrac{b\vee\dfrac{\mathsf{f}}{b}}{b} \quad .$$

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

$$ {\scriptstyle =}\,\dfrac{{\scriptstyle \mathsf{i}\downarrow}\,\dfrac{\mathsf{t}}{{\scriptstyle \mathsf{c}\uparrow}\,\dfrac{b\vee\mathsf{f}}{\left[b\vee\dfrac{\mathsf{f}}{b}\right]\wedge[b\vee\mathsf{f}]}\;\vee\;(\bar{b}\wedge\mathsf{t})}\;\vee\;\dfrac{\bar{b}}{\bar{b}\wedge\bar{b}}}{\left(\dfrac{b\vee b}{b}\;\wedge\;\dfrac{b\vee\dfrac{\mathsf{f}}{b}}{b}\right)\;\vee\;{\scriptstyle \mathsf{c}\downarrow}\,\dfrac{(\bar{b}\wedge\mathsf{t})\vee\left(\bar{b}\wedge\dfrac{\bar{b}}{\mathsf{t}}\right)}{{\scriptstyle \mathsf{w}\uparrow}\,\dfrac{\bar{b}\wedge\mathsf{t}}{\mathsf{t}}}} \quad .$$

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/`

References

Brünnler, K. (2004).
Deep Inference and Symmetry in Classical Proofs.
Logos Verlag, Berlin.
http://www.iam.unibe.ch/~kai/Papers/phd.pdf.

Brünnler, K. and Tiu, A. F. (2001).
A local system for classical logic.
In Nieuwenhuis, R. and Voronkov, A., editors, *Logic for Programming, Artificial Intelligence, and Reasoning (LPAR)*, volume 2250 of *Lecture Notes in Computer Science*, pages 347–361. Springer-Verlag.
http://www.iam.unibe.ch/~kai/Papers/lcl-lpar.pdf.

Bruscoli, P. and Guglielmi, A. (2009).
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.

Bruscoli, P., Guglielmi, A., Gundersen, T., and Parigot, M. (2010).
A quasipolynomial cut-elimination procedure in deep inference via atomic flows and threshold formulae.
In Clarke, E. M. and Voronkov, A., editors, *Logic for Programming, Artificial Intelligence, and Reasoning (LPAR-16)*, volume 6355 of *Lecture Notes in Computer Science*, pages 136–153. Springer-Verlag.
http://cs.bath.ac.uk/ag/p/QPNDI.pdf.

Guglielmi, A., Gundersen, T., and Parigot, M. (2010a).
A proof calculus which reduces syntactic bureaucracy.
In Lynch, C., editor, *21st International Conference on Rewriting Techniques and Applications*, volume 6 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 135–150. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.
http://drops.dagstuhl.de/opus/volltexte/2010/2649.

Guglielmi, A., Gundersen, T., and Straßburger, L. (2010b).
Breaking paths in atomic flows for classical logic.
In Jouannaud, J.-P., editor, *25th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 284–293. IEEE.
http://www.lix.polytechnique.fr/~lutz/papers/AFII.pdf.

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.

Straßburger, L. (2006).
Proof nets and the identity of proofs.
Technical Report 6013, INRIA.
http://hal.inria.fr/docs/00/11/43/20/PDF/RR-6013.pdf.