Introducing Substitution in Proof Theory

Alessio Guglielmi

University of Bath

20 July 2014

This talk is available at `http://cs.bath.ac.uk/ag/t/ISPT.pdf`
It is an abridged version of this other talk: `http://cs.bath.ac.uk/ag/t/PCMTGI.pdf`
Deep inference web site: `http://alessio.guglielmi.name/res/cos/`

Outline

Problem: compressing proofs.

Solution: proof composition mechanisms beyond Gentzen.

Open deduction: composition by connectives and inference, smaller analytic proofs than in Gentzen.

Atomic flows: geometry is enough to normalise.

Composition by substitution: more geometry, more efficiency, more naturality.

Problem: compressing proofs

How can we make proofs smaller? Known mechanisms:

1. Re-use the same sub-proof: cut rule. Proof theory.
2. Re-use the same sub-proof: dagness, or cocontraction: $\mathsf{c}\!\uparrow \dfrac{A}{A \wedge A}$.
3. Substitution: $\mathsf{sub}\,\dfrac{A}{A\sigma}$. In Frege, equivalent to (4).
4. Tseitin extension: $p \leftrightarrow A$ (where p is a fresh atom). Optimal?
5. Higher orders (including 2^{nd} order propositional).

We will see that 1–4 (and a bit also 5) have a lot to do with proof composition: this is our main tool.

Our main objective is providing for small spaces of canonical proofs (= eliminating bureaucracy = getting good proof semantics).

Solution: proof composition mechanisms beyond Gentzen

Less is more. Let's make better use of what we have already.

Given two proofs $\phi : A \Rightarrow B$ and $\psi : C \Rightarrow D$:

1. For a logical connective $\star$ we have:

$$\phi \star \psi : (A \star C) \Rightarrow (B \star D) \quad .$$

   Proofs are composed by the connectives of the formula language.

2. For an inference rule B/C we have:

$$\phi/\psi : A \Rightarrow D \quad .$$

   Proofs are composed by inference rules.

3. For an atom a we have:

$$\phi\{a \leftarrow \psi\} : A\{a \leftarrow C, \bar{a} \leftarrow \bar{D}\} \Rightarrow B\{a \leftarrow D, \bar{a} \leftarrow \bar{C}\} \quad .$$

   Proofs are composed by substitution.

Two (relatively) new formalisms

Open deduction: composition by (1) connectives and (2) inference rules.

- It exists [5] and it can be taken as a definition for deep inference.
- It generalises the sequent calculus by removing its restrictions.
- Sequents $\approx$ 'depth-1 inference without full inference composition'.
- Hypersequents $\approx$ 'depth-2 inference without full inference composition'.
- It compresses proofs by cut, dagness and depth itself (new, exponential speed-up).
- I'll show the main ideas and some results.

'Formalism B': open deduction + (3) substitution.

- It almost exists (work with Bruscoli, Gundersen and Parigot).
- It further compresses proofs by substitution (conjectured further superpolynomial speed-up, it is equivalent to Frege + substitution).
- I'll show some ideas and what I think we can get.

Open-deduction system SKS

- Atomic rules:

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

identity *weakening* *contraction*

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

cut *coweakening* *cocontraction*

- Linear rules:

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

switch *medial*

- Plus an '=' linear rule (associativity, commutativity, units).
- Negation on atoms only.

The cut is atomic.

SKS is complete for propositional logic. See [1].

Examples of open deduction

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

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

Proofs are composed by the same operators as formulae (horizontally) and by inference rules (vertically).

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

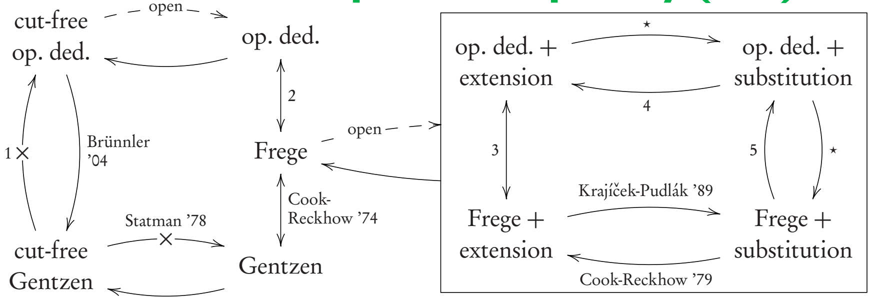
First order example

$$
\mathsf{i}\!\downarrow \frac{\mathsf{t}}{\exists x \forall y \left[\boxed{\mathsf{w}\!\downarrow \dfrac{\mathsf{f}}{\overline{p(x)}}} \vee p(y) \right] \vee \exists x \forall y \left[\overline{p(x)} \vee \boxed{\mathsf{w}\!\downarrow \dfrac{\mathsf{f}}{p(y)}} \right]}
$$

$$
\mathsf{c}\!\downarrow \frac{\exists x \forall y \left[\boxed{\mathsf{w}\!\downarrow \dfrac{\mathsf{f}}{\overline{p(x)}}} \vee p(y) \right] \vee \exists x \forall y \left[\overline{p(x)} \vee \boxed{\mathsf{w}\!\downarrow \dfrac{\mathsf{f}}{p(y)}} \right]}{\exists x \forall y \left[\overline{p(x)} \vee p(y) \right]}
$$

This is much more natural than in Gentzen.

Open deduction and proof complexity (size)



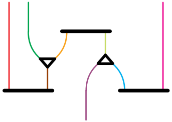
$\longrightarrow$ = ‘polynomially simulates’.

Open deduction:

- in the cut-free case, thanks to deep inference, has an exponential speed-up over the cut-free sequent calculus (e.g., over Statman tautologies)—1, see [2];
- has as small proofs as the best formalisms—2, 3, 4, 5, see [2];
- thanks to dagness, has quasipolynomial cut elimination (instead of exponential) [3, 7].

Atomic flows: locality brings geometry

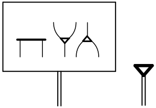
$$\mathsf{s}\,\dfrac{\mathsf{m}\,\dfrac{\dfrac{\mathsf{t}}{a\vee\bar a}}{[a\vee\mathsf{t}]\wedge[\mathsf{t}\vee\bar a]}}{\left[\mathsf{s}\,\dfrac{[a\vee\mathsf{t}]\wedge\bar a}{\dfrac{a\wedge\bar a}{\mathsf{f}}\vee\mathsf{t}}\quad\vee\quad\mathsf{t}\right]}
=\dfrac{\left(\mathsf{s}\,\dfrac{a\wedge\left[\bar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

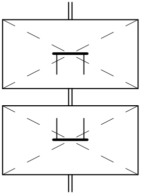




Below the proofs, their (atomic) flows [4] are shown:

- only structural information is retained in flows;
- logical information is lost;
- flow size is polynomially related to derivation size;
- composition of proofs naturally correspond to composition of flows.

Generalising the cut-free form

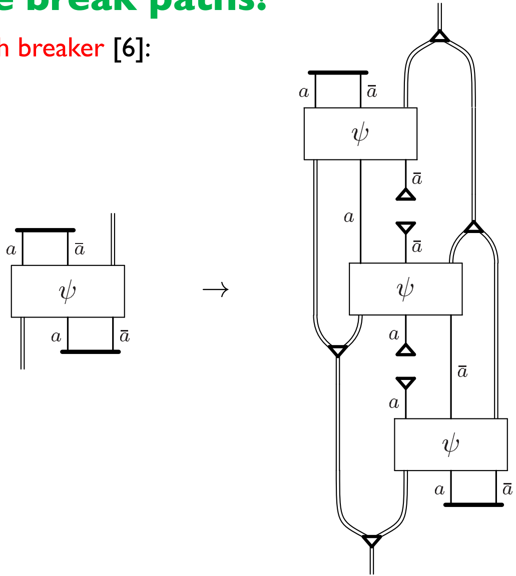
- Normalised proof: 

- 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 [6]:



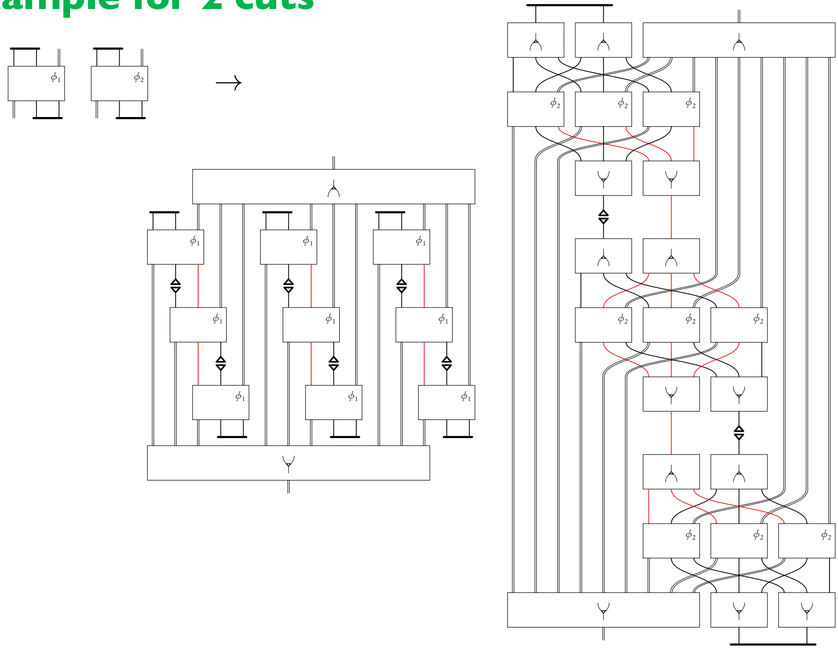
Even if there is a path between identity and cut on the left, there is none on the right.

We can do the same on derivations, of course

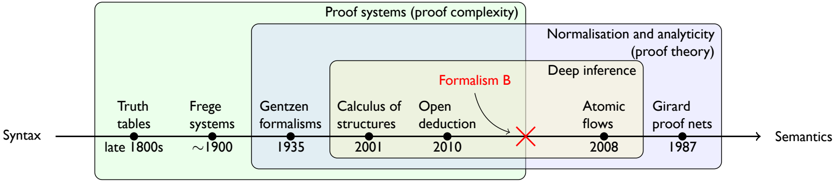
$$
\dfrac{\dfrac{A}{[a \vee \bar{a}] \wedge A}}{\begin{array}{c} \Psi \Big\Vert \\ \dfrac{B \vee (a \wedge \bar{a})}{B} \end{array}}
\quad \rightarrow \quad
\begin{array}{c}
A \\
\Big\Vert \{\mathsf{c}\uparrow,\mathsf{ai}\downarrow,=\} \\
(([a \vee \bar{a}] \wedge A) \wedge A) \wedge A \\
{\scriptstyle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

- 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.

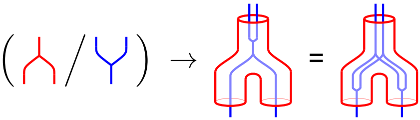
Example for 2 cuts



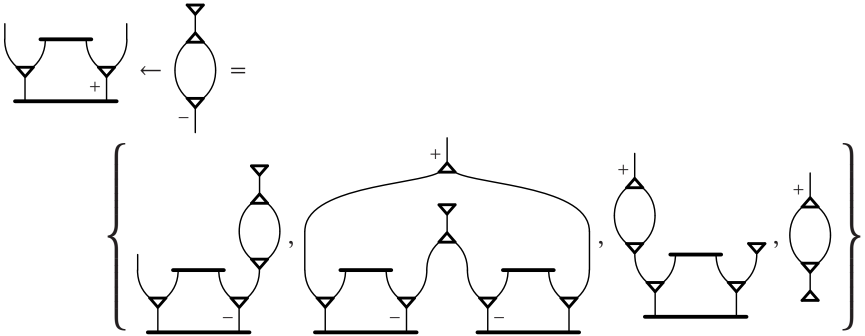
‘Formalism B’: allowing substitution



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



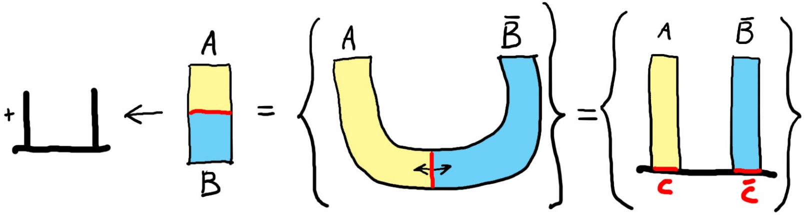
Example of flow substitution



The flows represent proofs. The bigger the set on the right, the more bureaucracy is captured by the substitution, the smaller the set of canonical proofs is.

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

Gundersen's substitution trick



Substituting a proof ϕ inside an identity or cut stands for a set of proofs with as many elements as ways to break ϕ.

This iterated mechanism alone generates one canonical form for an exponentially big class of proofs.

Lifting flow substitutions to proofs

Consider the following two synchronal open deduction derivations:

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

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

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

Conclusions

- Proof composition in Gentzen is too rigid.
- 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 obtain a natural notion of proof substitution that does not interfere with normalisation.
- We obtain interesting notions of proof semantics.

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

References

[1] K. Brünnler and A. F. Tiu.
A local system for classical logic.
In R. Nieuwenhuis and A. Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning (LPAR)*, volume 2250 of *Lecture Notes in Computer Science*, pages 347–361. Springer-Verlag, 2001.

[2] P. Bruscoli and A. Guglielmi.
On the proof complexity of deep inference.
ACM Transactions on Computational Logic, 10(2):14:1–34, 2009.

[3] P. Bruscoli, A. Guglielmi, T. Gundersen, and M. Parigot.
A quasipolynomial cut-elimination procedure in deep inference via atomic flows and threshold formulae.
In E. M. Clarke and A. Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning (LPAR-16)*, volume 6355 of *Lecture Notes in Computer Science*, pages 136–153. Springer-Verlag, 2010.

[4] A. Guglielmi and T. Gundersen.
Normalisation control in deep inference via atomic flows.
Logical Methods in Computer Science, 4(1):9:1–36, 2008.

[5] A. Guglielmi, T. Gundersen, and M. Parigot.
A proof calculus which reduces syntactic bureaucracy.
In C. Lynch, editor, *21st International Conference on Rewriting Techniques and Applications (RTA)*, volume 6 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 135–150. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2010.

[6] A. Guglielmi, T. Gundersen, and L. Straßburger.
Breaking paths in atomic flows for classical logic.
In J.-P. Jouannaud, editor, *25th Annual IEEE Symposium on Logic in Computer Science (LICS)*, pages 284–293. IEEE, 2010.

[7] E. Jeřábek.
Proof complexity of the cut-free calculus of structures.
Journal of Logic and Computation, 19(2):323–339, 2009.