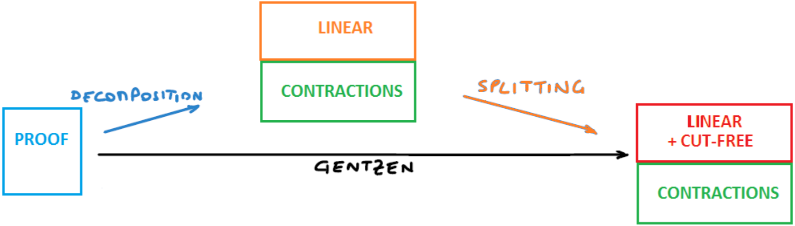
Subatomic Proof Systems

Andrea Aler Tubella,
IRIF, CNRS & Université Paris Diderot

Alessio Guglielmi,
University of Bath

19th of June 2017

Untangling cut-elimination



We generalise

- A procedure to eliminate the cut in 'linear' systems, called splitting.
- A procedure to permute 'contractions' to the bottom of proofs, called decomposition.

What is deep inference [8]?

It's the free composition of proofs via the same connectives as formulae.

If

$$\Phi = \begin{array}{c} A \\ \| \\ B \end{array} \qquad \text{and} \qquad \Psi = \begin{array}{c} C \\ \| \\ D \end{array}$$

are two proofs with, respectively, premisses A and C and conclusions B and D, then

$$(\Phi \wedge \Psi) = \begin{array}{c} (A \wedge C) \\ \| \\ (B \wedge D) \end{array} \qquad \text{and} \qquad [\Phi \vee \Psi] = \begin{array}{c} [A \vee C] \\ \| \\ [B \vee D] \end{array}$$

are valid proofs with, respectively, premisses $(A \wedge C)$ and $[A \vee C]$, and conclusions $(B \wedge D)$ and $[B \vee D]$.

Some advantages

- To obtain new notions of normalisation in addition to cut elimination [11, 10].
- To shorten analytic proofs by exponential factors compared to Gentzen [6, 7].
- To express logics that cannot be expressed in Gentzen [16, 4].
- To make the proof theory of a vast range of logics regular and modular [4].
- To get proof systems whose inference rules are local [14].
- To inspire a new generation of proof nets and semantics of proofs [15].
- To investigate the nature of cut elimination [10, 13].

Introduction

- We observe that deep inference systems have a recurring linear "rule shape".

$$ai{\downarrow}\,\frac{\mathsf{t}}{a \vee \bar{a}} \qquad ai{\uparrow}\,\frac{a \wedge \bar{a}}{\mathsf{f}}$$

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

$$ac{\downarrow}\,\frac{a \vee a}{a} \qquad ac{\uparrow}\,\frac{a}{a \wedge a}$$

$$aw{\downarrow}\,\frac{\mathsf{f}}{a} \qquad aw{\uparrow}\,\frac{a}{\mathsf{t}}$$

Figure: SKS [5]

$$ai{\downarrow}\,\frac{1}{a \parr \bar{a}} \qquad ai{\uparrow}\,\frac{a \otimes \bar{a}}{\bot}$$

$$s\,\frac{(A \parr B) \otimes C}{(A \otimes C) \parr B}$$

$$d{\downarrow}\,\frac{(A \parr B) \,\&\, (C \parr D)}{(A \,\&\, C) \parr (B \oplus D)} \qquad d{\uparrow}\,\frac{(A \oplus B) \otimes (C \,\&\, D)}{(A \otimes C) \oplus (B \otimes D)}$$

$$\oplus{\downarrow}\,\frac{(A \parr B) \oplus (C \parr D)}{(A \oplus C) \parr (B \oplus D)} \qquad \&{\uparrow}\,\frac{(A \,\&\, B) \otimes (C \,\&\, D)}{(A \otimes C) \,\&\, (B \otimes D)}$$

$$m\,\frac{(A \,\&\, B) \oplus (C \,\&\, D)}{(A \oplus C) \,\&\, (B \oplus D)}$$

$$ac{\downarrow}\,\frac{a \oplus a}{a} \qquad ac{\uparrow}\,\frac{a}{a \,\&\, a}$$

$$m_2{\downarrow}\,\frac{(A \otimes B) \oplus (C \otimes D)}{(A \oplus C) \otimes (B \oplus D)} \qquad m_2{\uparrow}\,\frac{(A \,\&\, B) \parr (C \,\&\, D)}{(A \parr C) \,\&\, (B \parr D)}$$

$$at{\downarrow}\,\frac{0}{a} \qquad at{\uparrow}\,\frac{a}{\top}$$

Figure: SLLS [14]

One shape to rule them all

- We observe that deep inference systems have a recurring linear "rule shape".

$$
ai{\downarrow}\,\frac{\mathsf{t}}{a \vee \bar{a}} \qquad ai{\uparrow}\,\frac{a \wedge \bar{a}}{\mathsf{f}}
$$

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

$$
ac{\downarrow}\,\frac{a \vee a}{a} \qquad ac{\uparrow}\,\frac{a}{a \wedge a}
$$

$$
aw{\downarrow}\,\frac{\mathsf{f}}{a} \qquad aw{\uparrow}\,\frac{a}{\mathsf{t}}
$$

Figure: SKS [5]

$$
ai{\downarrow}\,\frac{1}{a \parr \bar{a}} \qquad ai{\uparrow}\,\frac{a \otimes \bar{a}}{\bot}
$$

$$
s\,\frac{(A \parr B) \otimes C}{(A \otimes C) \parr B}
$$

$$
d{\downarrow}\,\frac{(A \parr B) \,\&\, (C \parr D)}{(A \,\&\, C) \parr (B \oplus D)} \qquad d{\uparrow}\,\frac{(A \oplus B) \otimes (C \,\&\, D)}{(A \otimes C) \oplus (B \otimes D)}
$$

$$
\oplus{\downarrow}\,\frac{(A \parr B) \oplus (C \parr D)}{(A \oplus C) \parr (B \oplus D)} \qquad \&{\uparrow}\,\frac{(A \,\&\, B) \otimes (C \,\&\, D)}{(A \otimes C) \,\&\, (B \otimes D)}
$$

$$
m\,\frac{(A \,\&\, B) \oplus (C \,\&\, D)}{(A \oplus C) \,\&\, (B \oplus D)}
$$

$$
ac{\downarrow}\,\frac{a \oplus a}{a} \qquad ac{\uparrow}\,\frac{a}{a \,\&\, a}
$$

$$
m_2{\downarrow}\,\frac{(A \otimes B) \oplus (C \otimes D)}{(A \oplus C) \otimes (B \oplus D)} \qquad m_2{\uparrow}\,\frac{(A \,\&\, B) \parr (C \,\&\, D)}{(A \parr C) \,\&\, (B \parr D)}
$$

$$
at{\downarrow}\,\frac{0}{a} \qquad at{\uparrow}\,\frac{a}{\top}
$$

Figure: SLLS [14]

One shape to rule them all

- Goal: generating propositional proofs by a single, linear, simple and regular inference rule scheme.

$$\frac{(A\,\alpha\,C)\,\beta\,(B\,\gamma\,D)}{(A\,\beta\,B)\,\alpha\,(C\,\delta\,D)}$$

But how do we change the atomic rules to fit our scheme?

- Idea: consider atoms as self-dual, noncommutative binary logical relations.
  - extended language of formulae (atoms inside atoms, whatever that means)
- Why: We can use the rule scheme to reason very generally on proof systems.

Subatomic logic

We use propositional classical logic as an example.

The trick: occurrences of an atom a are interpretations of more primitive expressions involving a noncommutative binary relation denoted by a.

- Formulae A and B in the relation a, in this order, are denoted by $A\, a\, B$.
- Formulae are built over the two units for disjunction and conjunction, respectively f and t.

Example: the following two expressions are SA formulae:

$$(\mathsf{f}\ a\ \mathsf{t}) \vee (\mathsf{t}\ a\ \mathsf{f}) \qquad (\mathsf{f}\ b\ \mathsf{f})\ a\ (\mathsf{t}\ c\ (\mathsf{t}\ d\ \mathsf{f})) \wedge \mathsf{f} \wedge ((\mathsf{f}\ a\ \mathsf{f}) \vee (\mathsf{t}\ b\ \mathsf{t}))$$

We call tame the formulae where atoms do not appear in the scope of other atoms (*e.g.*, left) and wild the others (*e.g.*, right).

Subatomic logic

To interpret our extended language of formulae, we define an interpretation map $\mapsto$ from tame SA formulae to ordinary formulae such that

$$\begin{array}{ll} \mathsf{f}\; a\; \mathsf{t} \mapsto a & \mathsf{t}\; a\; \mathsf{f} \mapsto \bar{a} \\ \mathsf{t}\; a\; \mathsf{t} \mapsto \mathsf{t} & \mathsf{f}\; a\; \mathsf{f} \mapsto \mathsf{f} \end{array}$$

where $\bar{a}$ denotes the negation of a.

Note

- atoms are self dual: $\overline{A\; a\; B} \equiv \bar{A}\; a\; \bar{B}$
- atoms are not commutative
- atoms are not associative

We easily extend $\mapsto$ to all the tame SA formulae in the natural way. For example: $(\mathsf{f}\; a\; \mathsf{t}) \vee (\mathsf{t}\; a\; \mathsf{f}) \mapsto a \vee \bar{a}$ $\qquad (\mathsf{f} \vee \mathsf{f})\; a\; (\mathsf{t} \vee \mathsf{t}) \mapsto a$

Subatomic logic

Consider the usual contraction rule for an atom:

$$\frac{a \vee a}{a}$$

We could obtain this rule via $\mapsto$ as follows:

$$\frac{(\mathsf{f}\ a\ \mathsf{t}) \vee (\mathsf{f}\ a\ \mathsf{t})}{(\mathsf{f} \vee \mathsf{f})\ a\ (\mathsf{t} \vee \mathsf{t})} \mapsto \frac{a \vee a}{a} \qquad \text{and} \qquad \frac{(\mathsf{t}\ a\ \mathsf{f}) \vee (\mathsf{t}\ a\ \mathsf{f})}{(\mathsf{t} \vee \mathsf{t})\ a\ (\mathsf{f} \vee \mathsf{f})} \mapsto \frac{\bar{a} \vee \bar{a}}{\bar{a}} \quad .$$

We might consider those rules as generated by the linear scheme

$$\frac{(A\ a\ C) \vee (B\ a\ D)}{(A \vee B)\ a\ (C \vee D)}$$

Precisely the shape we observed before.

Subatomic Logic

Two more examples, identity and cut:

$$\frac{(\mathsf{f} \vee \mathsf{t})\ a\ (\mathsf{t} \vee \mathsf{f})}{(\mathsf{f}\ a\ \mathsf{t}) \vee (\mathsf{t}\ a\ \mathsf{f})} \mapsto \frac{\mathsf{t}}{a \vee \bar{a}} \qquad \text{and} \qquad \frac{(\mathsf{f}\ a\ \mathsf{t}) \wedge (\mathsf{t}\ a\ \mathsf{f})}{(\mathsf{f} \wedge \mathsf{t})\ a\ (\mathsf{t} \wedge \mathsf{f})} \mapsto \frac{a \wedge \bar{a}}{\mathsf{f}} \quad .$$

They are generated by the linear schemes:

$$\frac{(A \vee C)\ a\ (B \vee D)}{(A\ a\ B) \vee (C\ a\ D)} \qquad \text{and} \qquad \frac{(A\ a\ C) \wedge (B\ a\ D)}{(A \wedge B)\ a\ (C \wedge D)}$$

- Surprisingly, we are able to reduce disparate rules such as contraction, cut and identity into a unique rule scheme.

The proof system

- A subatomic system SA is a deep inference system whose rules are instances of the inference rule scheme

$$\frac{(A \, \alpha \, C) \, \beta \, (B \, \alpha' \, D)}{(A \, \beta \, B) \, \alpha \, (C \, \beta \, D)}$$

where A, B, C, D are formulae and $\alpha, \alpha', \beta, \beta'$ are relations.

- What is a proof in a SA system? A proof is a derivation whose premiss is t.
- A proof composed of only tame formulae corresponds to a proof in our usual proof theory.

Example: SAKS for classical logic

$$a\!\downarrow \frac{(A \vee B)\ a\ (C \vee D)}{(A\ a\ C) \vee (B\ a\ D)} \qquad a\!\uparrow \frac{(A\ a\ B) \wedge (C\ a\ D)}{(A \wedge C)\ a\ (B \wedge D)}$$

$$\wedge\!\downarrow \frac{(A \vee B) \wedge (C \vee D)}{(A \wedge C) \vee (B \vee D)} \qquad \vee\!\uparrow \frac{(A \vee B) \wedge (C \wedge D)}{(A \wedge C) \vee (B \wedge D)}$$

$$m \frac{(A \wedge B) \vee (C \wedge D)}{(A \vee C) \wedge (B \vee D)}$$

$$ac \frac{(A\ a\ B) \vee (C\ a\ D)}{(A \vee C)\ a\ (B \vee D)} \qquad a\bar{c} \frac{(A \wedge B)\ a\ (C \wedge D)}{(A\ a\ C) \wedge (B\ a\ D)}$$

Figure: SAKS

Example: SAMALLS for MALL

$$a\downarrow \; \frac{(A \parr B)\; a\; (C \parr D)}{(A\; a\; C) \parr (B\; a\; D)} \qquad a\uparrow \; \frac{(A\; a\; B) \otimes (C\; a\; D)}{(A \otimes C)\; a\; (B \otimes D)}$$

$$\otimes\downarrow \; \frac{(A \parr B) \otimes (C \parr D)}{(A \otimes C) \parr (B \parr D)} \qquad \parr\uparrow \; \frac{(A \parr B) \otimes (C \otimes D)}{(A \otimes C) \parr (B \otimes D)}$$

$$\&\downarrow \; \frac{(A \parr B) \,\&\, (C \parr D)}{(A \,\&\, C) \parr (B \oplus D)} \qquad \oplus\uparrow \; \frac{(A \oplus B) \otimes (C \,\&\, D)}{(A \otimes C) \oplus (B \otimes D)}$$

$$\oplus\downarrow \; \frac{(A \parr B) \oplus (C \parr D)}{(A \oplus C) \parr (B \oplus D)} \qquad \&\uparrow \; \frac{(A \,\&\, B) \otimes (C \,\&\, D)}{(A \otimes C) \,\&\, (B \otimes D)}$$

$$\parr\downarrow \; \frac{(A \parr B) \parr (C \parr D)}{(A \parr C) \parr (B \parr D)} \qquad \otimes\uparrow \; \frac{(A \otimes B) \otimes (C \otimes D)}{(A \otimes C) \otimes (B \otimes D)}$$

$$m \; \frac{(A \,\&\, B) \oplus (C \,\&\, D)}{(A \oplus C) \,\&\, (B \oplus D)}$$

$$ac\downarrow \; \frac{(A\; a\; B) \oplus (C\; a\; D)}{(A \oplus C)\; a\; (B \oplus D)} \qquad ac\uparrow \; \frac{(A \,\&\, B)\; a\; (C \,\&\, D)}{(A\; a\; C) \,\&\, (B\; a\; D)}$$

$$\otimes c\downarrow \; \frac{(A \otimes B) \oplus (C \otimes D)}{(A \oplus C) \otimes (B \oplus D)} \qquad \parr c\uparrow \; \frac{(A \,\&\, B) \parr (C \,\&\, D)}{(A \parr C) \,\&\, (B \parr D)}$$

$$\oplus c\downarrow \; \frac{(A \oplus B) \oplus (C \oplus D)}{(A \oplus C) \oplus (B \oplus D)} \qquad \&c\uparrow \; \frac{(A \,\&\, B) \,\&\, (C \,\&\, D)}{(A \,\&\, C) \,\&\, (B \,\&\, D)}$$

Cut-elimination in two phases

We can provide a generalised theory of cut-elimination into two different steps:

- Decomposition: we decompose proofs into a top phase without contractions, and a bottom phase made-up only of contractions.
  - Achieved through local rewritings.
  - Potentially increases the size of a proof exponentially.

- Splitting: a cut-elimination procedure for systems without contractions.
  - Global procedure.
  - Polynomial complexity cost.

Decomposition

- In some deep inference systems, we can permute atomic contractions to the bottom of proofs through local reductions.

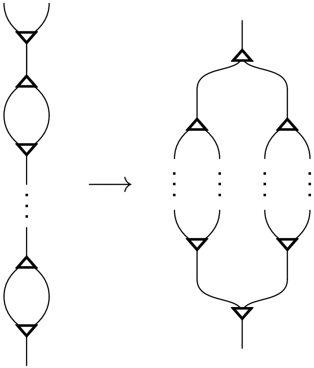
$$
\mathsf{ai}\!\uparrow \dfrac{\boxed{\mathsf{ac}\!\downarrow \dfrac{a \vee a}{a}} \wedge \bar{a}}{\mathsf{f}}
\quad \longrightarrow \quad
= \dfrac{\mathsf{s}\,\dfrac{\mathsf{s}\,\dfrac{(a \vee a) \wedge \boxed{\mathsf{ac}\!\uparrow \dfrac{\bar{a}}{\bar{a} \wedge \bar{a}}}}{(a \wedge (\bar{a} \wedge \bar{a})) \vee a}}{\boxed{\mathsf{ai}\!\uparrow \dfrac{a \wedge \bar{a}}{\mathsf{f}}} \vee \boxed{\mathsf{ai}\!\uparrow \dfrac{a \wedge \bar{a}}{\mathsf{f}}}}}{\mathsf{f}}
$$

$$
\mathsf{ac}\!\uparrow \dfrac{\mathsf{ac}\!\downarrow \dfrac{a \vee a}{a}}{a \wedge a}
\quad \longrightarrow \quad
\mathsf{m}\,\dfrac{\boxed{\mathsf{ac}\!\uparrow \dfrac{a}{a \wedge a}} \vee \boxed{\mathsf{ac}\!\uparrow \dfrac{a}{a \wedge a}}}{\boxed{\mathsf{ac}\!\downarrow \dfrac{a \vee a}{a}} \wedge \boxed{\mathsf{ac}\!\downarrow \dfrac{a \vee a}{a}}}
$$

Decomposition

- We can pinpoint exactly where an exponential increase on the size of proofs occurs.

$$\mathsf{ac}{\uparrow}\dfrac{\mathsf{ac}{\downarrow}\dfrac{a \vee a}{a}}{a \wedge a} \longrightarrow \mathsf{m}\dfrac{\boxed{\mathsf{ac}{\uparrow}\dfrac{a}{a \wedge a}} \vee \boxed{\mathsf{ac}{\uparrow}\dfrac{a}{a \wedge a}}}{\boxed{\mathsf{ac}{\downarrow}\dfrac{a \vee a}{a}} \wedge \boxed{\mathsf{ac}{\downarrow}\dfrac{a \vee a}{a}}}$$



Decomposition

- We are able to generalise these rewriting rules to permute other 'contractive' rules downwards in a proof [1].
- The generalised reduction rules work for any system containing all the rules necessary to make contraction atomic (CL, MALL included).

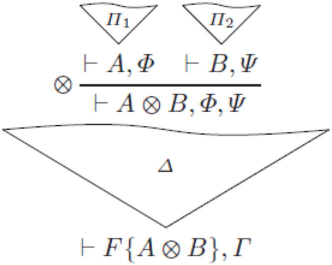
$$
\rho\,\dfrac{\boxed{\alpha c\,\dfrac{(A\,\alpha\,B)\,\nu\,(C\,\alpha\,D)}{(A\,\nu\,C)\,\alpha\,(B\,\nu\,D)}}\;\beta\,(E\,\alpha'\,F)}{(R\,\beta\,E)\,\alpha\,(S\,\beta'\,F)}
\quad\longrightarrow\quad
\alpha c{\downarrow}\,\dfrac{\mu\,\dfrac{((A\,\alpha\,B)\,\nu\,(C\,\alpha\,D))\,\beta\,\boxed{c{\downarrow}\,\dfrac{E\,\alpha'\,F}{(E\,\alpha'\,F)\bar{\nu}(E\,\alpha'\,F)}}}{\boxed{\rho\,\dfrac{(A\,\alpha\,B)\,\beta\,(E\,\alpha'\,F)}{(A\,\beta\,E)\,\alpha\,(B\,\beta'\,F)}}\;\nu\;\boxed{\rho\,\dfrac{(C\,\alpha\,D)\,\beta\,(E\,\alpha'\,F)}{(C\,\beta\,E)\,\alpha\,(D\,\beta'\,F)}}}}{\boxed{\beta c{\downarrow}\,\dfrac{(A\,\beta\,E)\,\nu\,(C\,\beta\,E)}{(A\,\nu\,C)\,\beta\,\boxed{c{\downarrow}\,\dfrac{E\,\nu\,E}{E}}}}\;\alpha\;\boxed{\beta' c{\downarrow}\,\dfrac{(B\,\beta'\,F)\,\nu\,(D\,\beta'\,F)}{(B\,\nu\,D)\,\beta'\,\boxed{c{\downarrow}\,\dfrac{F\,\nu\,F}{F}}}}}
$$

Splitting

- Generalisation of a common technique employed for cut-elimination in deep inference systems [9, 12, 14, 3].
- We break down the proof in different pieces, and put them back together in such a way that we avoid the cut.
- This type of argument has been used to prove the admissibility of rules other than the atomic cut.

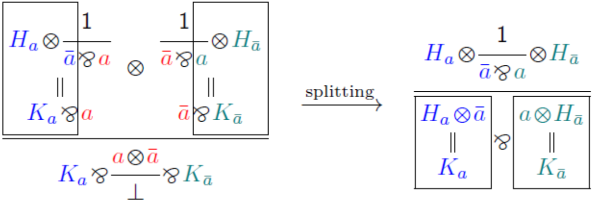
Splitting

- We show that cut-elimination via splitting works for all systems without contractions where the rules introduce dualities [2].



Splitting

- We show that cut-elimination via splitting works for all systems without contractions where the rules introduce dualities [2].



Conclusion

- We observe a mysterious phenomenon: only one rule shape is enough to describe many different systems.
- We characterise the systems that enjoy splitting+decomposition.
- In this way, we disentangle two phenomena gaining understanding and control.
- We can use it to design systems.

References

[1] A. Aler Tubella.
A Study of Normalisation Through Subatomic Logic.
PhD thesis, University of Bath, 2016.

[2] A. Aler Tubella and A. Guglielmi.
Subatomic proof systems: Splittable systems.
Submitted for publication. https://arxiv.org/abs/1703.10258.

[3] K. Brünnler.
Cut elimination inside a deep inference system for classical predicate logic.
Studia Logica, 82(1):51–71, 2006.

[4] K. Brünnler.
Nested sequents.
Habilitation Thesis, 2010.

[5] 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.

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

[7] A. Das.
On the proof complexity of cut-free bounded deep inference.
In K. Brünnler and G. Metcalfe, editors, *Automated Reasoning with Analytic Tableaux and Related Methods (Tableaux)*, volume 6793 of *Lecture Notes in Artificial Intelligence*, pages 134–148. Springer-Verlag, 2011.

[8] A. Guglielmi.
Deep inference.
Web site at http://alessio.guglielmi.name/res/cos.

References (cont.)

[9] A. Guglielmi.
A system of interaction and structure.
ACM Transactions on Computational Logic, 8(1):1:1–64, 2007.

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

[11] 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.

[12] A. Guglielmi and L. Straßburger.
A system of interaction and structure V: The exponentials and splitting.
Mathematical Structures in Computer Science, 21(3):563–584, 2011.

[13] T. Gundersen.
A General View of Normalisation Through Atomic Flows.
PhD thesis, University of Bath, 2009.

[14] L. Straßburger.
Linear Logic and Noncommutativity in the Calculus of Structures.
PhD thesis, Technische Universität Dresden, 2003.

[15] L. Straßburger.
From deep inference to proof nets via cut elimination.
Journal of Logic and Computation, 21(4):589–624, 2011.

[16] A. Tiu.
A system of interaction and structure II: The need for deep inference.
Logical Methods in Computer Science, 2(2):4:1–24, 2006.