Cuts for circular proofs

Jérôme Fortier[1] and Luigi Santocanale[2]

[1] LIF, AMU, Marseille, France
LaCIM, UQAM, Montréal, Canada
jerome.fortier@lif.univ-mrs.fr
[2] LIF, AMU, Marseille, France
luigi.santocanale@lif.univ-mrs.fr

One of the authors introduced in [2] a calculus of circular proofs for studying the computability arising from the following categorical operations: finite products and coproducts, initial algebras, final coalgebras. The calculus of [2] is cut-free; yet, even if sound and complete for provability, it lacks an important property for the semantics of proofs, namely fullness w.r.t. the class of natural categorical models called μ-bicomplete category in [3].

We fix, with this work, this problem by adding the cut rule to the calculus. To this goal, we need to modify the syntactical constraints on the cycles of proofs so to ensure soundness of the calculus and at same time local termination of cut-elimination. The enhanced proof system fully represents arrows of the intended model, a free μ-bicomplete category. We also describe a cut-elimination procedure as a model of computation arising from the above mentioned categorical operations. The procedure constructs a cut-free proof-tree with infinite branches out of a finite circular proof with cuts.

The calculus of circular proofs. Terms are constructed from a fixed set of variables $\mathbb{V}$ using the binary function symbols $\times, +$ and the constants $1, 0$; the set of terms will be denoted by TERMS. A *directed system of equations* is a tuple $S = \langle X, \tau, \pi \rangle$, where $X = \mathsf{BD}(S)$ is a finite subset of $\mathbb{V}$, $\tau : X \to \mathsf{TERMS}$, and $\pi : X \to \mathbb{N}$. $\mathsf{FV}(S)$ shall denote the set of free variables of S, namely $\bigcup_{x \in X} \mathsf{VAR}(\tau(x)) \setminus \mathsf{BD}(S)$.

Intuitively, we think of the tuple S as the system of equations $\{\, x =_{\theta(\pi(x))} \tau(x) \mid x \in X \,\}$ where $\theta(n) = \mu$ (least solution) if n is odd and $\theta(n) = \nu$ (greatest solution) otherwise. The priority function π also specifies the order by which we solve this system of equations. Given $n \geq 0$ and a system S, let $X_n = \{\, x \in \mathsf{BD}(S) \mid \pi(x) \leq n \,\}$ and let S_n be the restriction of S to X_n, namely $S_n = \langle X_n, \tau_{\restriction X_n}, \pi_{\restriction X_n} \rangle$. In particular, if $M = \max\{\, \pi(x) \mid x \in \mathsf{BD}(S) \,\}$, then we define $\mathsf{MAX}(S) = \{\, x \in \mathsf{BD}(S) \mid \pi(x) = M \,\}$, $\mathsf{LOW}(S) = X_{M-1}$, and let $P(S)$, the *predecessor system*, be S_{M-1}.

A sequent is a pair (s, t) of terms, written as usual $s \vdash t$; SEQ shall denote the set of sequents. For a fixed directed system of equations S, the *inference rules* over S are (instances of) the formal expressions appearing in Figure 1. Let Σ denote the set of justifications appearing on the right of these formal expressions. For a deterministic transition system G over $\{\, 0, 1 \,\}$ and $v \in G$, $\varsigma_i v$ shall denote the unique successor of v labelled by i.

Definition 1. A *pre-proof* over S is a tuple $\Pi = \langle G, \rho, \sigma \rangle$ where G is a deterministic labelled digraph over the alphabet $\{0, 1\}$, $\rho : G \to \Sigma$, and $\sigma = (\sigma_{\mathtt{L}}, \sigma_{\mathtt{R}}) : G \to \mathsf{SEQ}$; moreover, for each $v \in G$, $\mathrm{outdeg}(v) \leq 2$ and

$$\frac{\sigma(\varsigma_0 v) \quad \ldots \quad \sigma(\varsigma_{\mathrm{outdeg}(v)-1} v)}{\sigma(v)}\,\rho(v)$$

is an inference rule over S.

Identity, cut, assumption	$\dfrac{}{t \vdash t}\ \mathtt{Id}$	$\dfrac{s \vdash u \quad u \vdash t}{s \vdash t}\ \mathtt{Cut}$	$\dfrac{}{s \vdash t}\ \mathtt{A}$
Products			$\dfrac{}{t \vdash 1}\ \mathtt{RAx}$
	$\dfrac{s_i \vdash t}{s_0 \times s_1 \vdash t}\ \mathtt{L}\times_i \ \ i = 0, 1$		$\dfrac{s \vdash t_0 \quad s \vdash t_1}{s \vdash t_0 \times t_1}\ \mathtt{R}\times$
Coproducts	$\dfrac{}{0 \vdash t}\ \mathtt{LAx}$		
	$\dfrac{s_0 \vdash t \quad s_1 \vdash t}{s_0 + s_1 \vdash t}\ \mathtt{L}+$		$\dfrac{s \vdash t_i}{s \vdash t_0 + t_1}\ \mathtt{R}+_i \ \ i = 0, 1$
Fixpoints	$\dfrac{\tau(x) \vdash t}{x \vdash t}\ \mathtt{L}\mu x$		$\dfrac{s \vdash \tau(x)}{s \vdash x}\ \mathtt{R}\mu x$
	$\dfrac{\tau(x) \vdash t}{x \vdash t}\ \mathtt{L}\nu x$		$\dfrac{s \vdash \tau(x)}{s \vdash x}\ \mathtt{R}\nu x$

Figure 1: Inference rules of the system

A path Γ of a pre-proof is *left-traceable* if, for all n, if $\rho(\Gamma(n)) = \mathtt{Cut}$, then $\Gamma(n+1) = \varsigma_0(\Gamma(n))$; it is *right-traceable* if, for all n, if $\rho(\Gamma(n)) = \mathtt{Cut}$, then $\Gamma(n+1) = \varsigma_1(\Gamma(n))$. Γ has a *left μ-trace* if Γ is left-traceable, it contains a left regeneration rule, and the highest priority of its left regeneration rules is odd; Γ has a *right ν-trace* if if Γ is right-traceable, it contains a right regeneration rule, and the highest priority of its right regeneration rules is even.

Definition 2. A *circular proof* is a pre-proof $\Pi = \langle G, \rho, \sigma \rangle$ such that every cycle in G either has a left μ-trace or a right ν-trace.

Given a circular proof Π, we set $A_\Pi := \{v \in G : \rho(v) = \mathtt{A}\}$ and $C_\Pi := G \setminus A_\Pi$; A_Π is the set of assumptions of Π, while C_Π is the set of its conclusions.

Semantics of the calculus. μ-bicomplete categories were defined in [3]. Let $\mathcal{M}$ be a μ-bicomplete category. Given $t \in \mathsf{TERMS}$ and a finite subset X with $\mathsf{VAR}(t) \subseteq X$, the *natural semantics of* t, denoted $|t|_X$, is a functor from $\mathcal{M}^X$ to $\mathcal{M}$. The formal definition of $|t|_X$ is by induction on the structure of t, as usual by interpreting the function symbols $1, \times, 0, +$ by means of the categorical structure. Given a directed system of equations S and a finite subset X such that $\mathsf{FV}(S) \subseteq X$ and $\mathsf{BD}(S) \cap X = \varnothing$, the *semantics of* S, noted by $[\![S]\!]_X$, is a functor from $\mathcal{M}^X$ to $\mathcal{M}^{\mathsf{BD}(S)}$. The definition is as follows:

Definition 3. If $\mathsf{BD}(S) = \varnothing$, then $\mathcal{M}^{\mathsf{BD}(S)}$ is the terminal category so that we let $[\![S]\!]_X$ be the unique functor from $\mathcal{M}^X$ to the terminal category. Otherwise, the predecessor system $P(S)$ is well-defined and its semantics is a functor from $\mathcal{M}^{X \cup \mathsf{MAX}(S)}$ to $\mathcal{M}^{\mathsf{BD}(P(S))}$. Let G and H be the functors so defined:

$$\begin{aligned}
&G := \langle |\tau(x)|_{[\mathsf{BD}(S) \cup X]} \mid x \in \mathsf{MAX}(S) \rangle : \mathcal{M}^{\mathsf{BD}(S) \cup X} \to \mathcal{M}^{\mathsf{MAX}(S)}\,,\\
&H := \langle\, G\,,\ \llbracket P(S) \rrbracket_{\mathsf{MAX}(S) \cup X} \circ \mathtt{pr}^{\mathsf{BD}(S) \cup X}_{\mathsf{MAX}(S) \cup X}\ \rangle :\\
&\quad \mathcal{M}^{\mathsf{BD}(S)} \times \mathcal{M}^{X} = \mathcal{M}^{\mathsf{BD}(S) \cup X} \longrightarrow \mathcal{M}^{\mathsf{MAX}(S)} \times \mathcal{M}^{\mathsf{BD}(P(S))} = \mathcal{M}^{\mathsf{BD}(S)}\,.
\end{aligned}$$

If $\pi(\mathsf{MAX}(S))$ is odd, then $\llbracket S \rrbracket_X$ is the parametrized initial algebra of H; if $\pi(\mathsf{MAX}(S))$ is even, then $\llbracket S \rrbracket_X$ is the parametrized final coalgebra of H.

Finally, given a system S, a term t, and a finite subset X with $\mathsf{FV}(S) \cup (\mathsf{VAR}(t) \setminus \mathsf{BD}(S)) \subseteq X$, the *value of* t *w.r.t.* S, denoted $\llbracket t \rrbracket^S_X$, is the functor defined by:

$$\llbracket t \rrbracket^S_X := \left(\mathcal{M}^X \xrightarrow{\langle \mathtt{id}, \llbracket S \rrbracket_X \rangle} \mathcal{M}^X \times \mathcal{M}^{\mathsf{BD}(S)} = \mathcal{M}^{X \cup \mathsf{BD}(S)} \xrightarrow{|t|_{X \cup \mathsf{BD}(S)}} \mathcal{M} \right).$$

We shall use a sloppy notation and write just $\llbracket t \rrbracket$ in place of $\llbracket t \rrbracket^S_X$.

Lemma 4. *For each $x \in \mathsf{BD}(S)$, if $\pi(x)$ is odd, then there exists a canonical invertible arrow $\zeta_x : \llbracket \tau(x) \rrbracket \to \llbracket x \rrbracket$; if $\pi(x)$ is even, then there exists a canonical invertible arrow $\xi_x : \llbracket x \rrbracket \to \llbracket \tau(x) \rrbracket$.*

With exception of `Id` and `Cut`, a rule `Rule` with assumptions $s_i \vdash t_i$ and conclusion $s \vdash t$ can be intertpreted as a natural transformation

$$[\mathtt{Rule}]_{X,X'} : \prod_{i=1,\ldots,n} \mathcal{M}(\llbracket s_i \rrbracket, \llbracket t_i \rrbracket) \to \mathcal{M}(\llbracket s \rrbracket, \llbracket t \rrbracket) : (\mathcal{M}^X)^{op} \times \mathcal{M}^X \to \mathrm{Set}\,.$$

(For the fixpoint rules, use the structure maps $\zeta_x, \zeta_x^{-1}, \xi_x, \xi_x^{-1}$). The above remark is almost true of `Cut`; if either we have a natural transformation $\beta : \llbracket u \rrbracket \to \llbracket t \rrbracket$, or a natural transformation $\gamma : \llbracket s \rrbracket \to \llbracket u \rrbracket$, then we have:

$$[\mathtt{Cut}, \beta] : \mathcal{M}(\llbracket s \rrbracket, \llbracket u \rrbracket) \to \mathcal{M}(\llbracket s \rrbracket, \llbracket t \rrbracket)\,, \qquad [\gamma, \mathtt{Cut}] : \mathcal{M}(\llbracket u \rrbracket, \llbracket t \rrbracket) \to \mathcal{M}(\llbracket s \rrbracket, \llbracket t \rrbracket)\,.$$

Definition 5. A circular proof Π is *homogeneous* if it does not contain the rule `Id` and, for each $v \in \Pi$ with $\rho(v) = \mathtt{Cut}$, exactly one among $\varsigma_0 v$ and $\varsigma_1 v$ is an assumption of Π.

For Π homogeneous, let $A^{\mathsf{c}}_\Pi = \{\, \varsigma_i v \in A_\Pi \mid \rho(v) = \mathtt{Cut} \,\}$ and $A^{\mathsf{s}}_\Pi = \{\, \varsigma_i v \in A_\Pi \mid \rho(v) \neq \mathtt{Cut} \,\}$; w.l.o.g., we shall assume that $A^{\mathsf{c}}_\Pi \cap A^{\mathsf{s}}_\Pi = \varnothing$. Given a collection of natural transformations $\beta = \{\, \beta^v : \llbracket \sigma_{\mathtt{L}}(v) \rrbracket \to \llbracket \sigma_{\mathtt{R}}(v) \rrbracket \mid v \in A^{\mathsf{c}}_\Pi \,\}$, the above rules give rise to a natural transformation

$$[\Pi_\beta] : \prod_{v \in C_\Pi} \mathcal{M}(\llbracket \sigma_{\mathtt{L}}(v) \rrbracket, \llbracket \sigma_{\mathtt{R}}(v) \rrbracket) \times \prod_{v \in A^{\mathsf{s}}_\Pi} \mathcal{M}(\llbracket \sigma_{\mathtt{L}}(v) \rrbracket, \llbracket \sigma_{\mathtt{R}}(v) \rrbracket) \to \prod_{v \in C_\Pi} \mathcal{M}(\llbracket \sigma_{\mathtt{L}}(v) \rrbracket, \llbracket \sigma_{\mathtt{R}}(v) \rrbracket)\,.$$

Theorem 6. *For each system S, each homogeneous circular proof Π over S, and each collection of natural transformations $\{\, \beta_v : \llbracket \sigma_{\mathtt{L}}(v) \rrbracket \to \llbracket \sigma_{\mathtt{R}}(v) \rrbracket \mid v \in A^{\mathsf{c}}_\Pi \,\}$, there exists a unique natural transformation*

$$[\Pi_\beta]_\dagger : \prod_{v \in A^{s}_\Pi} \mathcal{M}(\llbracket \sigma_{\mathtt{L}}(v) \rrbracket, \llbracket \sigma_{\mathtt{R}}(v) \rrbracket) \longrightarrow \prod_{v \in C_\Pi} \mathcal{M}(\llbracket \sigma_{\mathtt{L}}(v) \rrbracket, \llbracket \sigma_{\mathtt{R}}(v) \rrbracket)$$

satysfying the fixpoint equation $[\Pi_\beta]_\dagger = [\Pi_\beta] \circ \langle [\Pi_\beta]_\dagger, \mathtt{id} \rangle$.

A circular proof is *ground* if it does not contain an assumption rule. A *pointed circular proof* is a pair $\langle \Pi, v \rangle$ where Π is a ground circular proof and $v \in \Pi$. We can define $[\![\Pi, v]\!]$, the *interpretation* of $\langle \Pi, v \rangle$ with respect to the system S, by induction, almost as usual; the induction is now on the well-founded structure of maximal strongly connected components of the underlying graph of Π. To this goal the key observation is that if $\mathcal{C}$ is such a non trivial component of Π (i.e. if there exists $v, u \in \mathcal{C}$ and a non-null path from v to u), then the restriction of Π to $\mathcal{C}$ is homogeneous. Thus Theorem 6 allows to interpret $\mathcal{C}$ as a sort of generalized inference rule, whose assumptions belong to strictly lesser components.

The calculus is full in this sense: if a pointed circular proof $\langle \Pi, v \rangle$ is such that $\sigma(v) = s[t/x] \vdash t$, then it is possible to construct a pointed circular proof $\langle \Pi', v' \rangle$ whose semantics $[\![\Pi', v']\!]$ shall be the unique arrow f such that $f \circ \zeta_x = [\![\Pi, v]\!] \circ [\![s]\!](f)$. Of course, a dual property holds as well.

Cut elimination. We devise an algorithm that, given a pointed circular proof $\langle \Pi, v \rangle$, outputs a proof-tree which is cut-free, finitely branching but with possibly infinite branches. Just like in the classical case for Gentzen's system (see [1] for instance), the procedure consists in "pushing" every cut away from the root. Yet, this time, the output tree must be computed with a lazy (outermost) rather than eager (innermost) strategy. This is because not every path in Π leads to a leaf, so that we have to eliminate cuts by performing a breadth-first search of Π. A main problem, see Figure 2, is that with this strategy it might be the case that we need to permute a cut with another cut. We dismiss this problem by merging consecutive cuts together in a sort of n-ary cut. Such an n-ary cut becomes the internal data structure (that we call a *tape*) of an automaton that tries to build up a branch of the the proof-tree. When the proof-tree branches, the automaton forks into several automata so to construct all the branches. Equivalently, we can think that the automaton undeterministically chooses which branch to construct. The automaton grows up the branch by means of commutative cut reductions at the extremities of the tape; if all the cuts in the tape are principal, the automaton undeterministically chooses one and reduces it, without constructing a new node on the branch. *We can prove that the automaton does not perform "internal chatting". That is, the automaton eventually finds on its tape the oppurtunity to perfom a commutative cut reduction, thus growing the prefix of the proof-tree.*

$$\dfrac{\dfrac{t_0 \vdash t_1 \quad t_1 \vdash t_2}{t_0 \vdash t_2}\,\texttt{Cut} \qquad t_2 \vdash t_3 \cdots t_{n-1} \vdash t_n}{t_0 \vdash t_3}\,\texttt{Cut} \quad \Rightarrow \quad \dfrac{t_0 \vdash t_1 \quad t_1 \vdash t_2 \quad \cdots \quad t_{n-1} \vdash t_n}{t_0 \vdash t_n}\,\texttt{Cut}$$

Figure 2: Flattening cuts into a tape of cuts

References

[1] R. David, K. Nour, and C. Raffalli. *Introduction à la logique, Théorie de la démonstration.* Dunod, 2nd edition, 2004.

[2] Luigi Santocanale. A calculus of circular proofs and its categorical semantics. In Mogens Nielsen and Uffe Engberg, editors, *FoSSaCS*, volume 2303 of *Lecture Notes in Computer Science*, pages 357–371. Springer, 2002.

[3] Luigi Santocanale. μ-bicomplete categories and parity games. *Theoretical Informatics and Applications*, 36:195–227, September 2002.