# A Calculus of Circular Proofs and its Categorical Semantics*

Luigi Santocanale**

Department of Computer Science
University of Calgary
luigis@cpsc.ucalgary.ca

**Abstract.** We present a calculus of "circular proofs": the graph underlying a proof is not a finite tree but instead it is allowed to contain a certain amount of cycles. The main challenge in developing a theory for the calculus is to define the semantics of proofs, since the usual method by induction on the structure is not available. We solve this problem by associating to each proof a system of equations – defining relations among undetermined arrows of an arbitrary category with finite products and coproducts as well as constructible initial algebras and final coalgebras – and by proving that this system admits always a unique solution.

## 1 Introduction

In this paper we introduce a *calculus of proofs* for a simple fixed point logic. The proofs of the calculus are *circular* in that their underlying graph is not a tree but it is allowed to contain a certain amount of cycles. We present the semantics of the calculus and show how to interpret proof terms as arrows in categories. We also discuss a form of cut elimination theorem that holds for the calculus. Before discussing further our work, we relate it to two distinct topics in computer science.

**Fixed Points Logics**. The originating ground for the present work are fixed point logics [6, 13] and $\mu$-calculi [4]; as a particular $\mu$-calculus we count our work on free $\mu$-lattices [20, 21]. Roughly speaking, these frameworks are obtained from previously existing logical or algebraic frameworks by the addition of least and greatest fixed point operators. For example, the propositional modal $\mu$-calculus [15] arises in this way from modal logic. Usually cut free proofs in sequent calculi are inherently finite because premiss sequents are always strictly smaller than conclusions. However, in settings where the propositions themselves can be circular or infinite (as for fixed point propositions) there exists the possibility of having circular or infinite proofs as well. Remarkably these proofs happen

* Work developed at BRICS, Centre of the Danish National Research Foundation.
** Supported by Canada's NSERC and the Pacific Institute for the Mathematical Sciences.

to be the most useful in the theories so far developed. Examples from the literature are the refutations of the propositional $\mu$-calculus [26] and the proofs with guarded induction of type theory [9]. A major challenge when dealing with circular proofs is to prove their soundness, since the usual method by induction on the well founded structure of the proof tree is not available. Soundness is the main content of Walukiewicz's proof of the completeness of Kozen's axiomatization of the propositional $\mu$-calculus [26]: there the refutations are translated into more common tree like proofs characterized by the presence of a specific inference rule for fixed points.

We propose a categorical semantics of circular proofs and in this way we give a strong solution to the problem of soundness. It is our opinion that lifting the point of view from the theory of provability to proof theory – and from posets to categories – is of substantial help in clarifying the principles behind circular proofs. Recall that a recursively defined function is uniquely determined by its defining system of equations. In the spirit of categorical logic we analyze proofs as sort of recursively defined functions and obtain an immediate hint on the reasons for which proof terms should look like fixed point expressions.

**Semantics of Computation**. Often a programming language is given and one seeks for adequate algebraic models. If the language is typed, then the interesting models usually are structured categories. We follow an opposite direction as our aim is to extract a programming language from a given mathematical model. The present work is part of a more general investigation of categories with finite products, finite coproducts, "enough" initial algebras and final coalgebras; we call a category with these properties $\mu$-bicomplete, since it generalizes a posetal $\mu$-lattice to a categorical setting. Our primary interest are those categories that possess this structure in a canonical way, the free $\mu$-bicomplete categories. Syntactical constructions of free categories are always possible, however these constructions turn out to be useful only if the syntax has good proof theoretic properties like cut elimination or normalization. Thus our goal is to find a good syntax for a given semantic world. With respect to analogous logical and algebraic settings [8, 11, 12], with $\mu$-bicomplete categories the focus is on initial algebras and final coalgebras of functors. Initial algebras of functors, which naturally generalize least fixed points of order preserving functions, are a categorical formulation of induction and recursion and model inductive types [10]. On the other hand, final coalgebras – generalizing greatest fixed points – are a counterpart of coinduction and corecursion; they are related to bisimilarity in that they classify the observable behavior of systems [17, 18]. The use of coalgebraic methods is now a well established practice to deal with infinite objects by means of their defining equations [2].

As it is usually the case in proof theoretic contexts, it is possible to give a computational interpretation to proofs. The interpretation of circular proofs we shall propose stems from the game theoretical setting of free $\mu$-lattices [19, 20, 21] and the link we have established [23] between the theory of $\mu$-bicomplete categories and parity games [4]. The interpretation is consistent with the well known analogy proposed in [1] between games and winning strategies on the one hand, and systems' specifications and correct programs on the other. Given two $\mu$-lattice terms $S, T$ (the directed systems of section 2 are essentially $\mu$-lattice terms), the witnesses that a relation $S \vdash T$ holds are the winning strategies for one player in a game $S \multimap T$ with possibly infinite plays. A useful lemma allows to replace arbitrary winning strategies with bounded memory winning strategies; more explicitly, if we represent a winning strategy as an infinite tree, we can always assume that this tree is the unraveling of a finite graph. After we have translated our intuitions on games and strategies into a proof theoretic framework, we have rediscovered infinite and circular proofs: the first corresponding to infinite winning strategies, the latter corresponding to bounded memory winning strategies. Therefore the circular proofs presented here are meant to describe bounded memory deterministic strategies. The computational interpretation takes a game or a $\mu$-term into the description of a bidirectional synchronous communication channel. Given two $\mu$-terms $S$ and $T$, a circular proof witness of $S \vdash T$ can be understood as a protocol for letting the left user of the channel $S$ to communicate with the right user of $T$ in a constrained but asynchronous way.

**Our contribution**. The calculus of circular proofs would be uninteresting if not supported by good properties. As one of these properties, we account the existence of a canonical semantics of proof terms. The main purpose of this paper is that of illustrating this point. The semantics establishes equivalences between proofs and an obvious consequence of the way the semantics will be defined is that proofs in the form of tree with back edges can be partially unraveled to obtain equivalent proofs, and that "bisimilar" proofs are equivalent. To define the semantics we proceed as follows: once the propositions (the types, in the terminology of type theory) of the calculus are interpreted in the obvious way by means of products, coproducts, initial algebras and final coalgebras, it is then possible to associate to a circular proof a system of equations defining relations among undetermined arrows of an arbitrary $\mu$-bicomplete category. Theorem 3.7 states that the systems of equations arising from circular proofs admit always a unique solution. This is not an obvious result and depends strongly on the combinatorial condition by which we constrain cycles in circular proofs. To obtain this result, we need to improve the semantical tools that relate the theory of initial algebras to the theory of fixed points – known in type theory as Mendler's recursion [24] – in order to account for parameterized fixed points. This is the content of proposition 3.2.

A second property of the calculus, stated in 4.2, asserts that circular proofs are composable. This result is analogous to a cut elimination theorem in that it asserts the existence of an algorithm to produce a new cut free finite circular proof out of two given ones. This is an essential property of the calculus as it allows to consider circular proofs as concrete algorithms. To this end it would have been enough to observe that a lazy cut elimination holds (that is, a cut can indefinitely often be pushed up to a tree, producing an infinite tree). However our result is stronger, for example, under the given computational interpretation, it implies that there is a way of synthesizing a program without explicit substitution out of two programs with the same property. As far as we know, the most similar result concerns program transformation techniques [25]. The semantics allows to easily see that this sort of cut elimination is sound: two proofs can be composed into a proof the interpretation of which is the categorical composition of the interpretations of the two original proofs. Finally, we observe that the calculus is not powerful enough to describe all the arrows of a free $\mu$-bicomplete category. This reflects the fact that there are strategies that use an unbounded amount of memory, nonetheless, are computable. This observation suggests that some kind of step has to be done in order to describe free $\mu$-bicomplete categories; on the other hand, we expect that the ideas and tools presented in this paper will be helpful in future researches.

The paper is organized as follows. In section 2 we describe the syntactical part of the calculus, defining first the terms and then the proofs. In section 3 we state the main technical proposition which on the other hand is the key to define the semantics of proofs. The semantics is then implicitly defined by observing that the systems of equations associated to proofs admit unique solutions. In section 4, as concluding remarks, we state a cut elimination theorem, discuss the fact that the calculus is not enough expressive with respect to its intended models, and suggest a natural relation with automata theory. Full proofs of the statements presented here can be found in [22] and its extended version. The author is grateful to Robin Cockett for stimulating conversations on the subject.

**Notation.** With $\mathbb{S}\mathrm{et}$ we shall denote the category of sets and functions; for a function $f : A \longrightarrow B$ we shall use both the notations $f_a$ and $f(a)$ for the result of applying $f$ to $a$. With $[n]$ we shall denote the set $\{1, \ldots, n\}$. Composition in categories, say $A \xrightarrow{f} B \xrightarrow{g} C$, will be denoted in two different ways, that is, $g \circ f$ and $f \cdot g$. Sometimes we shall omit the symbol $\circ$ and write $gf$, but we always write the symbol $\cdot$ . We shall use $\mathtt{id}$ for identities, $\langle\rangle$ and $\mathtt{pr}$ for tuples and projections, $\{\}$ and $\mathtt{in}$ for cotuples and injections, for every kind of categorical products and coproducts. If $f : C \times A \longrightarrow C$ is a function (or a system of equations), we shall denote by $f^\dagger : A \longrightarrow C$ its unique parameterized fixed point (unique solution) whenever this exists. Our conventions on variables are as follows: each variable $x, y, z, \ldots$ can be in two states, either it is free or it is bound to some value. As a general rule, we shall use the usual style $x, y, z, \ldots$ for free variables and the overlined typewriter style $\overline{\mathtt{x}}, \overline{\mathtt{y}}, \overline{\mathtt{z}}, \ldots$ for bound variables.

## 2 The Calculus of Circular Proofs

Before we formally present the calculus, we shall point out its essential properties by inspecting the following "circular proof". We observe that:

- It is a proof in a sort of a Gentzen system: there are sequents $\Gamma \vdash \Delta$, where the expressions $\Gamma$ and $\Delta$ are simple formulas.
- The usual inference rules for disjunction and conjunction apply (true and false are treated as empty conjunction and disjunction respectively).
- There are inference rules (regenerations) allowing to replace variables with their values according to the set of equations on the left.

$$
\left\{\begin{array}{l} \overline{\mathtt{x}} =_\mu \overline{\mathtt{y}} \vee \overline{\mathtt{x}} \\ \overline{\mathtt{y}} =_\mu \top \vee \overline{\mathtt{y}} \end{array}\right\}
$$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{$\mathtt{R}\bigwedge_\emptyset$}
\UnaryInfC{$\top \vdash \top$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_l}$}
\UnaryInfC{$\top \vdash \top \vee \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{R}\overline{\mathtt{y}}_\mu$}
\UnaryInfC{$\top \vdash \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_l}$}
\UnaryInfC{$\top \vdash \overline{\mathtt{y}} \vee \overline{\mathtt{x}}$}
\RightLabel{$\mathtt{R}\overline{\mathtt{x}}_\mu$}
\UnaryInfC{$\top \vdash \overline{\mathtt{x}}$}
\AxiomC{}
\RightLabel{$\mathtt{R}\bigwedge_\emptyset$}
\UnaryInfC{$\top \vdash \top$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_l}$}
\UnaryInfC{$\top \vdash \top \vee \overline{\mathtt{y}}$}
\AxiomC{$\rangle \overline{\mathtt{y}} \vdash \overline{\mathtt{y}} \langle_{10}$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_r}$}
\UnaryInfC{$\overline{\mathtt{y}} \vdash \top \vee \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{L}\bigvee_{\{l,r\}}$}
\BinaryInfC{$\top \vee \overline{\mathtt{y}} \vdash \top \vee \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{R}\overline{\mathtt{y}}_\mu$}
\UnaryInfC{$\top \vee \overline{\mathtt{y}} \vdash \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{L}\mu\overline{\mathtt{y}}$}
\UnaryInfC{$\overline{\mathtt{y}} \vdash \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_r}$}
\UnaryInfC{$\overline{\mathtt{y}} \vdash \top \vee \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{R}\overline{\mathtt{y}}_\mu$}
\UnaryInfC{$\overline{\mathtt{y}} \vdash \overline{\mathtt{y}}$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_l}$}
\UnaryInfC{$\overline{\mathtt{y}} \vdash \overline{\mathtt{y}} \vee \overline{\mathtt{x}}$}
\AxiomC{$\rangle \overline{\mathtt{x}} \vdash \overline{\mathtt{x}} \langle_4$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_r}$}
\UnaryInfC{$\overline{\mathtt{x}} \vdash \overline{\mathtt{y}} \vee \overline{\mathtt{x}}$}
\RightLabel{$\mathtt{L}\bigvee_{\{l,r\}}$}
\BinaryInfC{$\overline{\mathtt{y}} \vee \overline{\mathtt{x}} \vdash \overline{\mathtt{y}} \vee \overline{\mathtt{x}}$}
\RightLabel{$\mathtt{R}\overline{\mathtt{x}}_\mu$}
\UnaryInfC{$\overline{\mathtt{y}} \vee \overline{\mathtt{x}} \vdash \overline{\mathtt{x}}$}
\RightLabel{$\mathtt{L}\mu\overline{\mathtt{x}}$}
\UnaryInfC{$\overline{\mathtt{x}} \vdash \overline{\mathtt{x}}$}
\RightLabel{$\mathtt{R}\bigvee_{\{l,r\}_r}$}
\UnaryInfC{$\overline{\mathtt{x}} \vdash \overline{\mathtt{y}} \vee \overline{\mathtt{x}}$}
\RightLabel{$\mathtt{R}\overline{\mathtt{x}}_\mu$}
\UnaryInfC{$\overline{\mathtt{x}} \vdash \overline{\mathtt{x}}$}
\RightLabel{$\mathtt{L}\bigvee_{\{l,r\}}$}
\BinaryInfC{$\top \vee \overline{\mathtt{x}} \vdash \overline{\mathtt{x}}$}
\end{prooftree}
$$

- Regeneration rules make it possible to construct infinite proof trees. We consider only regular trees and thus introduce the notation $\rangle \ldots \langle_n$ that you can see on some leaf. Its meaning is comparable to a `goto` command: "go back to the $n$-th node on the path from the root to this leaf, where you can find the same pair of formulas".

This circular proof has the following dynamic interpretation (which we have derived from the game theoretic setting): if $\top$ is read on the left, then no $\overline{\mathtt{x}}$ is produced on the right and then no new $\overline{\mathtt{y}}$ is produced on the right. If $\overline{\mathtt{x}}$ is read on the left, then $\overline{\mathtt{x}}$ is produced on the right and then as many $\overline{\mathtt{x}}$s are produced on the right as they are received from the left. After this cycle, a $\overline{\mathtt{y}}$ is produced on the right and then as many $\overline{\mathtt{y}}$s are produced on the right as they are received.

We shall abstract from regular infinite trees and consider simply properly labeled finite graphs. Not every such graph will be a circular proof. We observe in the above proof that on every cycle we can find a variable which is regenerated on the left side of the sequent symbol. We shall discuss this point in more details after the formal definition of the calculus.

### 2.1 Directed Systems of Labeled Equations

We fix a signature $\Omega$ and by writing $H \in \Omega_n$, $n \geq 0$, we mean that $H$ is a function symbol from $\Omega$ of arity $n$; we assume that the symbols $\bigwedge_I, \bigvee_I$ do not belong to $\Omega$, for each finite set $I$. We let $X$ be a countable set of variables, and let $\mathcal{C}$ be a category. We form terms as usual.

**Definition 2.1.** *The collection of terms* $\mathcal{T}(\mathbb{C})$ *and the free variables function* $\mathrm{fv} : \mathcal{T}(\mathbb{C}) \longrightarrow P(X)$ *are defined by induction by the following clauses:*

- *If* $x \in X$, *then* $x \in \mathcal{T}(\mathbb{C})$ *and* $\mathrm{fv}(x) = \{x\}$.
- *If* $c$ *is an object of* $\mathbb{C}$, *then* $c \in \mathcal{T}(\mathbb{C})$ *and* $\mathrm{fv}(c) = \emptyset$.
- *If* $I$ *is a finite set and* $s : I \longrightarrow \mathcal{T}(\mathbb{C})$ *is a function, then* $\bigwedge_I s \in \mathcal{T}(\mathbb{C})$ *and* $\bigvee_I s \in \mathcal{T}(\mathbb{C})$. *Moreover* $\mathrm{fv}(\bigwedge_I s) = \mathrm{fv}(\bigvee_I s) = \bigcup_{i \in I} \mathrm{fv}(s_i)$.
- *If* $H \in \Omega_n$ *and* $s : [n] \longrightarrow \mathcal{T}(\mathbb{C})$ *is a function, then* $Hs \in \mathcal{T}(\mathbb{C})$ *and* $\mathrm{fv}(Hs) = \bigcup_{i \in [n]} \mathrm{fv}(s_i)$.

If $Y \subseteq X$, we denote by $\mathcal{T}(\mathbb{C}, Y)$ the collection of terms $s \in \mathcal{T}(\mathbb{C})$ such that $\mathrm{fv}(s) \subseteq Y$. For a function $s : \{l, r\} \longrightarrow \mathcal{T}(\mathbb{C})$ we use the standard notation and write $s_l \wedge s_r, s_l \vee s_r$ for $\bigwedge_{\{l,r\}} s, \bigvee_{\{l,r\}} s$, respectively. Similarly, $\top$ stands for $\bigwedge_\emptyset$ and $\bot$ stands for $\bigvee_\emptyset$.

**Definition 2.2.** *A* polarized system of equations *over* $\mathbb{C}$ *is a tuple* $\langle \overline{\mathtt{X}}, q, \epsilon \rangle$ *where*

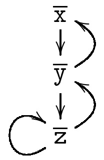
- $\overline{\mathtt{X}} \subseteq X$ *is a finite subset of* $X$, *the set of bound variables.*
- $q : \overline{\mathtt{X}} \longrightarrow \mathcal{T}(\mathbb{C})$ *is a function associating a value to each bound variable.*
- $\epsilon : \overline{\mathtt{X}} \longrightarrow \{\mu, \nu\}$ *is a labeling of bound variables.*

Given a polarized system of equations $\langle \overline{\mathtt{X}}, q, \epsilon \rangle$, the relation $\rightarrow$ on the set of variables $X$ is defined by saying that $\overline{\mathtt{x}} \rightarrow y$ if and only if $\overline{\mathtt{x}} \in \overline{\mathtt{X}}$ and $y \in \mathrm{fv}(q_{\overline{\mathtt{x}}})$.

**Definition 2.3.** *A tuple* $S = \langle \overline{\mathtt{X}}_S, q_S, \epsilon_S, \overline{\mathtt{X}}_{0,S} \rangle$ *is said to be a* directed system *over* $\mathbb{C}$ *if* $\langle \overline{\mathtt{X}}_S, q_S, \epsilon_S \rangle$ *is a polarized system of equations,* $\overline{\mathtt{X}}_{0,S} \subseteq \overline{\mathtt{X}}_S$ *and moreover for each* $\overline{\mathtt{x}} \in \overline{\mathtt{X}}_S$ *there exists a unique simple path in the graph* $\langle \overline{\mathtt{X}}_S, \rightarrow \rangle$ *from an element* $r(\overline{\mathtt{x}}) \in \overline{\mathtt{X}}_{0,S}$ *to* $\overline{\mathtt{x}}$. *For* $\overline{\mathtt{x}}, \overline{\mathtt{y}} \in \overline{\mathtt{X}}_S$, *we write* $\overline{\mathtt{x}} \leq_S \overline{\mathtt{y}}$ *if* $\overline{\mathtt{x}}$ *lies on the simple path from* $r(\overline{\mathtt{y}})$ *to* $\overline{\mathtt{y}}$; *we write* $\overline{\mathtt{x}} <_S \overline{\mathtt{y}}$ *if* $\overline{\mathtt{x}} \leq_S \overline{\mathtt{y}}$ *and* $\overline{\mathtt{x}} \neq \overline{\mathtt{y}}$. *We let* $\mathrm{fv}(S)$ *be the set* $(\bigcup_{\overline{\mathtt{x}} \in \overline{\mathtt{X}}_S} \mathrm{fv}(q_{\overline{\mathtt{x}}})) \setminus \overline{\mathtt{X}}_S$ *and by* $\mathrm{V}(S)$ *we denote the collection of finite subsets* $Y$ *of* $X$ *such that* $\mathrm{fv}(S) \subseteq Y$ *and* $Y \cap \overline{\mathtt{X}}_S = \emptyset$. *With* $\mathcal{S}(\mathbb{C})$ *we denote the collection of directed systems over* $\mathbb{C}$.

The notation $\{\overline{\mathtt{x}} =_{\epsilon_{\overline{\mathtt{x}}}} q_{\overline{\mathtt{x}}}\}_{\overline{\mathtt{x}} \in \overline{\mathtt{X}}}$ is used to represent a polarized system of equations $\langle \overline{\mathtt{X}}, q, \epsilon \rangle$. Roughly speaking, directed systems stand for $\mu$-terms, for example the $\mu$-term $\mu_x.\nu_y.(x \wedge \mu_z.(z \vee y))$ is translated into the directed system on the right which comes with the graph structure on bound variables; the induced order is $\overline{\mathtt{x}} < \overline{\mathtt{y}} < \overline{\mathtt{z}}$.

$$\left\langle \begin{Bmatrix} \overline{\mathtt{x}} =_\mu \overline{\mathtt{y}} \\ \overline{\mathtt{y}} =_\nu \overline{\mathtt{x}} \wedge \overline{\mathtt{z}} \\ \overline{\mathtt{z}} =_\mu \overline{\mathtt{z}} \vee \overline{\mathtt{y}} \end{Bmatrix}, \{\overline{\mathtt{x}}\} \right\rangle$$



Observe that the order does matter: the two directed systems on the right have the same underlying labeled system, however they represent the $\mu$-terms $\mu_x.\nu_y.(x \wedge y)$ and $\nu_y.((\mu_x.y) \wedge y)$, respectively.

$$\left\langle \begin{Bmatrix} \overline{\mathtt{x}} =_\mu \overline{\mathtt{y}} \\ \overline{\mathtt{y}} =_\nu \overline{\mathtt{x}} \wedge \overline{\mathtt{y}} \end{Bmatrix}, \{\overline{\mathtt{x}}\} \right\rangle \quad \left\langle \begin{Bmatrix} \overline{\mathtt{x}} =_\mu \overline{\mathtt{y}} \\ \overline{\mathtt{y}} =_\nu \overline{\mathtt{x}} \wedge \overline{\mathtt{y}} \end{Bmatrix}, \{\overline{\mathtt{y}}\} \right\rangle$$

In the category of sets, the interpretation of the first will be the empty set, where the interpretation of the second will be the set of unlabeled infinite binary trees, i.e. a singleton.

Let $S$ be a directed system, with $(\mathtt{x})_{\downarrow S}$ we denote the set of variables $\overline{\mathtt{y}}$ such that $\overline{\mathtt{y}} \leq_S \overline{\mathtt{x}}$. By $S_x$ we denote the system obtained from $S$ by freeing the variable $x$: we let $\overline{\mathtt{X}}_{S_x}$ be the set of variables $\overline{\mathtt{z}}$ such that $\overline{\mathtt{x}} <_S \overline{\mathtt{z}}$ and let $\overline{\mathtt{X}}_{0,S_x}, q_{S_x}$ and $\epsilon_{S_x}$ be the restrictions of $\overline{\mathtt{X}}_{0,S}, q_S$ and $\epsilon_S$ to $\overline{\mathtt{X}}_{S_x}$. It is easily verified that $\mathrm{fv}(S_x)$ is a subset of $\mathrm{fv}(S) \cup (\overline{\mathtt{x}})_{\downarrow S}$.

## 2.2 Circular Proofs

Let $S, T$ be two directed systems over $\mathcal{C}$. The collection $\mathcal{R}_{S,T}$ of *rule symbols* over $S, T$, with their arity set, is defined by means of table on the right.

| Rule | Range | Arity |
|---|---|---|
| $\mathtt{A}$ | | $[0]$ |
| $\mathtt{C}f$ | $f$ is an arrow of $\mathcal{C}$ | $[0]$ |
| $\mathtt{C}H$ | $H \in \Omega_n$ | $[n]$ |
| $\mathtt{L}\bigwedge_{I\,i}$ | $I$ is a finite set, $i \in I$ | $[1]$ |
| $\mathtt{R}\bigwedge_{I}$ | $I$ is a finite set | $I$ |
| $\mathtt{L}\bigvee_{I}$ | $I$ is a finite set | $I$ |
| $\mathtt{R}\bigvee_{I\,i}$ | $I$ is a finite set, $i \in I$ | $[1]$ |
| $\mathtt{L}\mu\overline{\mathtt{x}}$ | $\overline{\mathtt{x}} \in \overline{\mathtt{X}}_S, \epsilon_S(\overline{\mathtt{x}}) = \mu$ | $[1]$ |
| $\mathtt{R}\overline{\mathtt{y}}_\mu$ | $\overline{\mathtt{y}} \in \overline{\mathtt{X}}_T, \epsilon_T(\overline{\mathtt{y}}) = \mu$ | $[1]$ |
| $\mathtt{L}\overline{\mathtt{x}}_\nu$ | $\overline{\mathtt{x}} \in \overline{\mathtt{X}}_S, \epsilon_S(\overline{\mathtt{x}}) = \nu$ | $[1]$ |
| $\mathtt{R}\nu\overline{\mathtt{y}}$ | $\overline{\mathtt{y}} \in \overline{\mathtt{X}}_T, \epsilon_T(\overline{\mathtt{y}}) = \nu$ | $[1]$ |

**Definition 2.4.** *A tuple $\langle G_0, \lambda, \rho, \sigma \rangle$, where*

- *$G_0$ is a set of vertices,*
- *$\lambda : G_0 \longrightarrow \mathcal{T}(\mathcal{C}) \times \mathcal{T}(\mathcal{C})$ is a labeling of vertices by sequents,*
- *$\rho : G_0 \longrightarrow \mathcal{R}_{S,T}$ is a labeling of vertices by rule symbols over $S, T$,*
- *$\sigma_g : \mathrm{Arity}(\rho(g)) \longrightarrow G_0$ is a successor function associated to each $g \in G_0$,*

*is said to be* well typed *over $S, T$ if the typing constraints, defined in the following, hold.*

We present typing constraints on the right. A typing constraint has the form

$$\frac{\{s_i \vdash t_i\}_{i \in \mathrm{Arity}(R)}}{s \vdash t}\, R$$

and stands for the following implication: *for all $g \in G_0$, if $\rho(g) = R$, then $\lambda(g)$ has the form $s \vdash t$ and for each $i \in$* $\mathrm{Arity}(R)$ *$\lambda(\sigma_{g,i})$ has the form $s_i \vdash t_i$.*

$$\frac{}{s \vdash t}\,\mathtt{A}$$

$$\frac{}{\mathrm{dom}\, f \vdash \mathrm{cod}\, f}\,\mathtt{C}f \qquad \frac{\{s_i \vdash t_i\}_{i \in [n]}}{Hs \vdash Ht}\,\mathtt{C}H$$

$$\frac{s_i \vdash t}{\bigwedge_I s \vdash t}\,\mathtt{L}\textstyle\bigwedge_{I\,i} \qquad \frac{\{s \vdash t_i\}_{i \in I}}{s \vdash \bigwedge_I t}\,\mathtt{R}\textstyle\bigwedge_I$$

$$\frac{\{s_i \vdash t\}_{i \in I}}{\bigvee_I s \vdash t}\,\mathtt{L}\textstyle\bigvee_I \qquad \frac{s \vdash t_i}{s \vdash \bigvee_I t}\,\mathtt{R}\textstyle\bigvee_{I\,i}$$

$$\frac{q_{\overline{\mathtt{x}}} \vdash t}{\overline{\mathtt{x}} \vdash t}\,\mathtt{L}\mu\overline{\mathtt{x}} \qquad \frac{s \vdash q_{\overline{\mathtt{y}}}}{s \vdash \overline{\mathtt{y}}}\,\mathtt{R}\overline{\mathtt{y}}_\mu$$

$$\frac{q_{\overline{\mathtt{x}}} \vdash t}{\overline{\mathtt{x}} \vdash t}\,\mathtt{L}\overline{\mathtt{x}}_\nu \qquad \frac{s \vdash q_{\overline{\mathtt{y}}}}{s \vdash \overline{\mathtt{y}}}\,\mathtt{R}\nu\overline{\mathtt{y}}$$

Typing constraints are analogous to inference rules. For technical reasons we need the rule $\mathtt{A}$: a sequent justified by this rule has to be considered an assumption. Indeed, if $P = \langle G_0, \lambda, \rho, \sigma \rangle$ is a tuple well typed over $S, T$, we say that a vertex $g \in G_0$ is a *conclusion* if $\rho(g) \neq \mathtt{A}$ and that it is an *assumption* if $\rho(g) = \mathtt{A}$. We denote by $\mathcal{C}_P$ and $\mathcal{A}_P$ the set of conclusions and the set of assumptions of $P$, respectively. Not every well typed tuple is going to be a circular proof. To define this concept we need to analyze the graph underlying such a tuple.

**Definition 2.5.** *Let $P = \langle G_0, \lambda, \rho, \sigma \rangle$ be a tuple which is well typed over $S, T$. The graph $\mathcal{G}(P) = \langle G_0, \to \rangle$ has as vertices the elements of $G_0$, and $g \to g'$ iff $g' = \sigma_{g,i}$ for some $i \in \mathrm{Arity}(\rho(g))$. Let $\gamma_0 \to \gamma_1 \to \ldots \gamma_n = \gamma_0$, $n \geq 1$, be a proper cycle of $\mathcal{G}(P)$. We let*

$$\begin{aligned}
\gamma_S &= \{\, \mathtt{x} \in \overline{\mathtt{X}}_S \mid \exists i \in [n] \ s.t.\ \rho(\gamma_i) \in \{\mathtt{L}\mu\mathtt{x}, \mathtt{L}\mathtt{x}_\nu\}\,\}\,,\\
\gamma_T &= \{\, \mathtt{x} \in \overline{\mathtt{X}}_T \mid \exists i \in [n] \ s.t.\ \rho(\gamma_i) \in \{\mathtt{R}\mathtt{x}_\mu, \mathtt{R}\nu\mathtt{x}\}\,\}\,.
\end{aligned}$$

Observe that if $\gamma$ is a proper cycle of $\mathcal{G}(P)$, then either $\gamma_S \neq \emptyset$ or $\gamma_T \neq \emptyset$. If $\gamma_S \neq \emptyset$, then $\gamma_S$ is a strongly connected subgraph of the graph associated to $S$, hence we can find a minimum element with respect to the order $\leq_S$. A similar remark holds for $\gamma_T$.

**Definition 2.6.** *A tuple $\Pi$ well typed over $S, T$ is said to be a* circular proof *over $S, T$, if, for every proper cycle $\gamma$ of $\mathcal{G}(\Pi)$, either $\gamma_S \neq \emptyset$ and $\epsilon(\min \gamma_S) = \mu$, or $\gamma_T \neq \emptyset$ and $\epsilon(\min \gamma_T) = \nu$.*

We refer to the first statement as $\mathtt{L}(\gamma)$, and to the second as $\mathtt{R}(\gamma)$, so that a tuple $\Pi$, well typed over $S, T$, is a circular proof over $S, T$ if for every proper cycle $\gamma$ of $\mathcal{G}(\Pi)$ either $\mathtt{L}(\gamma)$ holds or $\mathtt{R}(\gamma)$ holds. The above condition can be understood as follows: the systems $S$ and $T$ are translations of games for free $\mu$-lattices, and a circular proof is meant to describe a bounded memory winning strategy in the compound game $S \multimap T$, which we described in [20, 21]. As in Blass' game semantics of Linear Logic [5] and in Joyal's games for communication [14], a chosen player has to win either on $S$ or on $T$. On the other hand, the games $S$ and $T$ are parity games, cf. [4]. Henceforth, the condition $\mathtt{L}(\gamma)$ can be understood as stating the fact that the chosen player of $S$ won't lose in this game by repeating infinitely often the instructions contained in the cycle $\gamma$ of his winning strategy.

In the examples we consider circular proofs coming with a base point, i.e. a chosen conclusion, such that the underlying pointed graph is a tree with back edges. It is our goal to remark the analogy with the usual model of a proof as a finite tree and use existing tools for drawing proofs. It is a consequence of the theory presented here that every circular proof with a chosen conclusion is equivalent to another one having the tree-with-back-edges shape. Hence, we draw trees with some of the leaves annotated by a number, as exemplified on the right. With this notation we mean that there is a transition in $\mathcal{G}(\Pi)$ from the vertex $g$ to the vertex that is at the $n$-th place on the path from the root to $g$.

$$\dfrac{\rangle s \vdash t\langle_n \quad \ldots}{\lambda(g)}\,\rho(g)$$
$$\vdots$$

In the data below, let $S$ be the the directed system on the left and observe that the associated order is $\mathtt{x} <_S \mathtt{y}$. If $T$ is the empty system of equations, then the two proof objects on the center and on the right below are both well typed over $S$ and $T$:

$$\langle \left\{ \begin{array}{l} \overline{\mathtt{x}} =_\nu \overline{\mathtt{y}} \\ \overline{\mathtt{y}} =_\mu \overline{\mathtt{x}} \wedge \overline{\mathtt{y}} \end{array} \right\} , \{\overline{\mathtt{x}}\} \rangle \qquad \dfrac{\dfrac{\dfrac{\rangle \overline{\mathtt{y}} \vdash \bot \langle_2}{\overline{\mathtt{x}} \wedge \overline{\mathtt{y}} \vdash \bot}\,\mathtt{L}\bigwedge_{\{l,r\}_r}}{\overline{\mathtt{y}} \vdash \bot}\,\mathtt{L}\mu\overline{\mathtt{y}}}{\overline{\mathtt{x}} \vdash \bot}\,\mathtt{L}\overline{\mathtt{x}}_\nu \qquad \dfrac{\dfrac{\dfrac{\rangle \overline{\mathtt{x}} \vdash \bot \langle_1}{\overline{\mathtt{x}} \wedge \overline{\mathtt{y}} \vdash \bot}\,\mathtt{L}\bigwedge_{\{l,r\}_l}}{\overline{\mathtt{y}} \vdash \bot}\,\mathtt{L}\mu\overline{\mathtt{y}}}{\overline{\mathtt{x}} \vdash \bot}\,\mathtt{L}\overline{\mathtt{x}}_\nu$$

The one on the center is a circular proof over $S, T$. The one on the right is not, since it does not satisfy condition of definition 2.6 on cycles. Indeed, let $\gamma$ be the only simple cycle on this graph. $\mathtt{R}(\gamma)$ does not hold, since $\gamma_T = \emptyset$. On the other hand $\mathtt{L}(\gamma)$ does not hold, since $\min \gamma_S = \overline{\mathtt{x}}$ and $\epsilon(\overline{\mathtt{x}}) = \nu$.

To end this section, we introduce some notation. Let $\Pi$ be a circular proof over the directed systems $S, T$. We write $s_g, t_g$ if $g$ is a vertex of $\Pi$ and $\lambda(g) = s_g \vdash t_g$. We let $\mathrm{fv}_l(\Pi)$ be the set $\mathrm{fv}(S) \cup (\bigcup_{g \in G_0} \mathrm{fv}(s_g)) \setminus \overline{\mathtt{X}}_S$ and let $\mathrm{fv}_r(\Pi)$ be the set $\mathrm{fv}(T) \cup (\bigcup_{g \in G_0} \mathrm{fv}(t_g)) \setminus \overline{\mathtt{X}}_T$. Observe that $\mathrm{fv}_l(\Pi) \in \mathrm{V}(S)$ and $\mathrm{fv}_r(\Pi) \in \mathrm{V}(T)$, and that, for $g \in G_0$, $s_g \in \mathcal{T}(\mathcal{C}, \overline{\mathtt{X}}_S \cup \mathrm{fv}_l(\Pi))$ and $t_g \in \mathcal{T}(\mathcal{C}, \overline{\mathtt{X}}_T \cup \mathrm{fv}_r(\Pi))$.

## 3 Semantics of the Calculus

The logical operators by which we have constructed terms and directed systems – that is, conjunction, disjunction, least prefixed point and greatest postfixed point – can be naturally interpreted in the category $\mathcal{C}$ provided $\mathcal{C}$ has finite products, finite coproducts and "enough" initial algebras and final coalgebras. We recall the definition of the latter two concepts and remind that these are categorical analogues of inductive and coinductive types.

**Definition 3.1.** *Let $S : \mathcal{C} \longrightarrow \mathcal{C}$ be an endofunctor, an $S$-*algebra *is a pair $(c, \gamma)$ where $c$ is an object of $\mathcal{C}$ and $\gamma : Sc \longrightarrow c$ is an arrow of $\mathcal{C}$. An $S$-algebra $(\overline{\mathtt{x}}, \chi)$ is* initial *if for each algebra $(c, \gamma)$ there exists a unique arrow $f : \overline{\mathtt{x}} \longrightarrow c$ such that $\chi \cdot f = Sf \cdot \gamma$. We define $S$-coalgebras in the dual way; an $S$-*coalgebra *$\theta : \overline{\mathtt{y}} \longrightarrow S\overline{\mathtt{y}}$ is* final *if for each coalgebra $\gamma : c \longrightarrow Sc$ there exists a unique arrow $f : c \longrightarrow \overline{\mathtt{y}}$ such that $f \cdot \theta = \gamma \cdot Sf$.*

It is known [16] that the arrow $\chi$ of an initial $S$-algebra $(\overline{\mathtt{x}}, \chi)$ is invertible. The universal property of the initial algebra states the existence and uniqueness of a solution of the equation $f = \chi^{-1} \cdot Sf \cdot \alpha$ for each algebra $\alpha : Sa \longrightarrow a$. This equation is rephrased in a more compact way as the fixed point equation

$$f = \chi^{-1} \cdot \alpha_{\overline{\mathtt{x}}}(f)\,,$$

where the transformation (natural in the variable $x$) $\alpha_x : \mathcal{C}(x, a) \longrightarrow \mathcal{C}(Sx, a)$ is defined by the formula $\alpha_x(f) = Sf \cdot \alpha$. Henceforth, we shall approach initial algebras and final coalgebras from the point of view of fixed point theory [6]. In order to obtain the full power of this theory we need a parameterized version of the universal property, which can be deduced if the category $\mathcal{C}$ has products.

**Proposition 3.2.** *Let $\mathcal{Z}, \mathcal{W}, \mathcal{C}$ be three categories, of which $\mathcal{C}$ has finite products, and let $S, T$ and $Q$ be functors such that $S : \mathcal{C} \times \mathcal{Z} \longrightarrow \mathcal{C}$, $T : \mathcal{W} \longrightarrow \mathcal{C}$, and $Q : \mathcal{C}^{op} \times \mathcal{Z}^{op} \times \mathcal{W} \longrightarrow \mathcal{S}\mathrm{et}$. Consider a natural transformation*

$$\alpha_{x,z,w} : \mathcal{C}(x, Tw) \times Q(x, z, w) \longrightarrow \mathcal{C}(S(x, z), Tw)$$

*and let $(\overline{\mathtt{x}}_z, \chi_z)$ be a parameterized initial algebra of the functor $S(x, z)$. For each object $z$ of $\mathcal{Z}$, $w$ of $\mathcal{W}$ and each $q \in Q(\overline{\mathtt{x}}_z, z, w)$, there exists a unique $f : \overline{\mathtt{x}}_z \longrightarrow Tw$ that is a solution of the equation*

$$f = \chi_z^{-1} \cdot \alpha_{\overline{\mathtt{x}}_z, z, w}(f, q)\,.$$

Unique solutions of the above equation make up a natural transformation

$$\beta_{z,w} : Q(\overline{\mathtt{x}}_z, z, w) \longrightarrow C(\overline{\mathtt{x}}_z, Tw)\,.$$

The above proposition leads to show that circular proofs, whenever interpreted as systems of equations, always admit a unique solution. The other tool needed is the Bekič lemma, cf. [6, §5.3.1.c], which can be stated in the form of a sufficient condition to determine whether a system admits a unique solution in terms of its subsystems. Before giving the formal semantics, we shall sketch our ideas with the circular proof of page 9. We can define the semantics of a directed system as for the $\mu$-term $\nu_x.\mu_y.(x \wedge y)$. We let

$$\begin{aligned}
\|x \wedge y\| &= \times : \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}\,.\\
\|\overline{\mathtt{y}}\| &= \text{The initial algebra of the above functor, parameterized in}\\
&\phantom{=}\ \text{the variable } x\text{. This makes up a functor:}\\
&\phantom{=}\ \mu_{\overline{\mathtt{y}}}.(x \times \overline{\mathtt{y}}) : \mathcal{C} \longrightarrow \mathcal{C}\,.\\
\|\overline{\mathtt{x}}\| &= \text{The final coalgebra of the above functor:}\\
&\phantom{=}\ \nu_{\overline{\mathtt{x}}}.\mu_{\overline{\mathtt{y}}}.(\overline{\mathtt{x}} \times \overline{\mathtt{y}}) : 1 \longrightarrow \mathcal{C}\,.
\end{aligned}$$

Observe that $\|\overline{\mathtt{x}}\|$, corresponding to a closed $\mu$-term, can be thought to be an object of $\mathcal{C}$. At this point, $\|\overline{\mathtt{y}}\|$ and $\|\overline{\mathtt{x}} \wedge \overline{\mathtt{y}}\|$ can be closed too, so that they also become objects of $\mathcal{C}$:

$$\begin{aligned}
\|\overline{\mathtt{y}}\| &= 1 \xrightarrow{\ \|\overline{\mathtt{x}}\|\ } \mathcal{C} \xrightarrow{\ \|\overline{\mathtt{y}}\|\ } \mathcal{C}\\
\|\overline{\mathtt{x}} \wedge \overline{\mathtt{y}}\| &= 1 \xrightarrow{\ \langle \|\overline{\mathtt{x}}\|, \|\overline{\mathtt{y}}\| \rangle\ } \mathcal{C} \times \mathcal{C} \xrightarrow{\ \times = \|x \wedge y\|\ } \mathcal{C}\,.
\end{aligned}$$

In order to interpret the circular proof of page 9 we associate to it a system of equations. Recall that we have

$$\begin{array}{rcl}
\|\overline{\mathtt{x}} \wedge \overline{\mathtt{y}}\| = \|\overline{\mathtt{x}}\| \times \|\overline{\mathtt{y}}\| & \xrightarrow{\ \mathtt{pr}_{\|\overline{\mathtt{y}}\|}\ } & \|\overline{\mathtt{y}}\| \\
 & & \text{product structure}\\
\|\overline{\mathtt{y}}\| = \|\overline{\mathtt{y}}\|(\,\|\overline{\mathtt{x}}\|\,) & \xleftarrow{\ \theta_{\|\overline{\mathtt{x}}\|}\ } & \|\overline{\mathtt{x}}\| \times \|\overline{\mathtt{y}}\|(\,\|\overline{\mathtt{x}}\|\,) = \|\overline{\mathtt{x}} \wedge \overline{\mathtt{y}}\| \\
 & & \text{initial algebra structure}\\
\|\overline{\mathtt{x}}\| & \xrightarrow{\ \chi\ } & \|\overline{\mathtt{y}}\|(\|\overline{\mathtt{x}}\|) = \|\overline{\mathtt{y}}\| \\
 & & \text{final coalgebra structure}\,.
\end{array}$$

Thus we can transform the circular proof into a system of equations:

$$
\dfrac{\dfrac{\dfrac{\rangle\overline{\mathtt{y}} \vdash \bot\langle_2}{\overline{\mathtt{x}} \wedge \overline{\mathtt{y}} \vdash \bot_3}\,\mathtt{L}\bigwedge_r}{\overline{\mathtt{y}} \vdash \bot_2}\,\mathtt{L}\mu\overline{\mathtt{y}}}{\overline{\mathtt{x}} \vdash \bot_1}\,\mathtt{L}\overline{\mathtt{x}}_\nu
\qquad \rightsquigarrow \qquad
\left\{\begin{array}{l} h_3 = \mathtt{pr}_{\|\overline{\mathtt{y}}\|} \cdot h_2 \\ h_2 = \theta^{-1}_{\|\overline{\mathtt{x}}\|} \cdot h_3 \\ h_1 = \chi \cdot h_2 \end{array}\right\}
$$

We shall see that this system admits a unique solution.

### 3.1 Semantics of Systems

In the following $\mathcal{C}$ will be a fixed category and $I, J$ will range over finite sets. A functor $S : \mathcal{C}^{\{x\}\cup J} \longrightarrow \mathcal{C}$ is said to *admit initial algebras* if, for each object $z$ of $\mathcal{C}^J$, an initial algebra of the functor $S(-, z)$ exists. Observe that if $R : \mathcal{C}^I \longrightarrow \mathcal{C}^J$ is a functor and $S : \mathcal{C}^{\{x\}\cup J} \longrightarrow \mathcal{C}$ admits initial algebras, then also the functor

$$S \circ (\mathtt{id}_{\mathcal{C}} \times R) : \mathcal{C}^{\{x\}\cup I} \longrightarrow \mathcal{C}$$

admits initial algebras. A *choice of initial algebras* is a correspondence $(\overline{\mathtt{x}}, \chi)$ that assigns to each pair $(S, z)$, where $S : \mathcal{C}^{\{x\}\cup J} \longrightarrow \mathcal{C}$ admits initial algebras and $z$ is an object of $\mathcal{C}^J$, an initial algebra $\chi_z : S(\overline{\mathtt{x}}_z, z) \longrightarrow \overline{\mathtt{x}}_z$. We shall require that a choice of initial algebras is stable under substitution, that is, if $\chi_z : S(\overline{\mathtt{x}}_z, z) \longrightarrow \overline{\mathtt{x}}_z$ is the initial algebra associated to the pair $(S, z)$, then $\chi_{Ru} : S(\overline{\mathtt{x}}_{Ru}, Ru) \longrightarrow \overline{\mathtt{x}}_{Ru}$ is the initial algebra associated to the pair $(S\circ(\mathtt{id}_{\mathcal{C}}\times R), u)$. A *choice of final coalgebras* is defined in a similar way.

**Definition 3.3.** *An $\Omega$-model is a pair $\langle \mathcal{C}, \mathcal{I}\rangle$ where $\mathcal{C}$ is a category with a given choice of finite products, finite coproducts, initial algebras and final coalgebras, and $\mathcal{I}$ is an interpretation of the signature, that is, a correspondence which assigns a functor $\mathcal{I}(H) : \mathcal{C}^n \longrightarrow \mathcal{C}$ to each symbol $H \in \Omega_n$, for each $n \geq 0$.*

We can avoid the use of choices if we allow uniqueness up to unique natural isomorphism in proposition 3.4. To ease the notation, we shall write simply $H : \mathcal{C}^n \longrightarrow \mathcal{C}$ for $\mathcal{I}(H) : \mathcal{C}^n \longrightarrow \mathcal{C}$ and say that $\mathcal{C}$ is an $\Omega$-model. To understand properly the next proposition, recall that if $\mathcal{C}$ has products (coproducts), then the functor category $\mathcal{C}^J$ has products (coproducts), which are calculated pointwise. Hence, a choice of products (coproducts) gives rise to a choice of products (coproducts) in the category $\mathcal{C}^J$. In a similar way, a choice of initial algebras (final coalgebras) determines, for each functor $S : \mathcal{C}^{\{x\}\cup J} \longrightarrow \mathcal{C}$ admitting initial algebras, a unique extension of the collection of objects $\{\overline{\mathtt{x}}_z\}_{z\in Obj(\mathcal{C}^J)}$ to a functor $\overline{\mathtt{x}} : \mathcal{C}^J \longrightarrow \mathcal{C}$ such that $\chi_z$ is a natural transformation from $S(\overline{\mathtt{x}}_z, z)$ to $\overline{\mathtt{x}}_z$.

**Proposition 3.4.** *Let $\mathcal{C}$ be an $\Omega$-model, let $S \in \mathcal{S}(\mathcal{C})$ and $Z \in \mathrm{V}(S)$. There exists at most one correspondence $\|-\|_S^Z$, defined on $\mathcal{T}(\mathcal{C}, \overline{\mathtt{X}}_S \cup Z)$, with the following properties:*

- *For each* $s \in \mathcal{T}(\mathcal{C}, \overline{\mathtt{X}}_S \cup Z)$, $\|s\|_S^Z$ *is a functor* $\mathcal{C}^Z \longrightarrow \mathcal{C}$.
- *For each* $z \in Z$, $\|z\|_S^Z$ *is the projection functor on the* $z$ *component.*
- *For each object* $c$ *of* $\mathcal{C}$, $\|c\|_S^Z = c$, *a constant functor.*
- *If* $s : I \longrightarrow \mathcal{T}(\mathcal{C}, \overline{\mathtt{X}}_S \cup Z)$, *then* $\|\bigwedge_I s\|_S^Z = \prod_{i \in I} \|s_i\|_S^Z$ *and* $\|\bigvee_I s\|_S^Z = \coprod_{i \in I} \|s_i\|_S^Z$.
- *If* $H \in \Omega_n$ *and* $s : [n] \longrightarrow \mathcal{T}(\mathcal{C}, \overline{\mathtt{X}}_S \cup Z)$, *then* $\|Hs\|_S^Z = H \circ \langle \|s_i\|_S^Z \rangle_{i \in [n]}$.
- *If the equation* $\overline{\mathtt{x}} =_\mu q_{\overline{\mathtt{x}}}$ *belongs to* $S$, *then* $\|\overline{\mathtt{x}}\|_S^Z$ *is the chosen initial algebra of the functor*

$$\|q_x\|_{S_x}^{(\overline{\mathtt{x}})_{\downarrow S} \cup Z} \circ (\mathtt{id}_{\mathcal{C}} \times \langle \|\overline{\mathtt{y}}\|_S^Z, \mathtt{id}_{\mathcal{C}^Z} \rangle_{\overline{\mathtt{y}} <_S \overline{\mathtt{x}}}) : \mathcal{C}^{\{x\} \cup Z} \longrightarrow \mathcal{C}\,.$$

- *If the equation* $\overline{\mathtt{x}} =_\nu q_{\overline{\mathtt{x}}}$ *belongs to* $S$, *then* $\|\overline{\mathtt{x}}\|_S^Z$ *is the chosen final coalgebra of the above functor.*

Observe that we need the relation $(\overline{\mathtt{x}})_{\downarrow S} \cup Z \in \mathrm{V}(S_x)$ to hold, however it is not difficult to derive it. We can now introduce the following definition.

**Definition 3.5.** *An* $\Omega$*-model* $\mathcal{C}$ *is said to be* $\mu$-bicomplete *if, for each directed system* $S \in \mathcal{S}(\mathcal{C})$ *and* $Z \in \mathrm{V}(S)$, *there exists exactly one correspondence* $\|-\|_S^Z$ *with the above properties.*

Every complete lattice $L$ with an interpretation of the signature $\Omega$ is a $\mu$-bicomplete $\Omega$-model. If $\Omega$ is the empty signature, then a lattice $L$ is $\mu$-bicomplete if and only if it is a $\mu$-lattice [20]. We have proved in [23] that a model $\langle \mathcal{C}, \mathcal{I} \rangle$ is $\mu$-bicomplete if (1) the interpretation of every function symbol is an accessible functor, and (2) the category $\mathcal{C}$ is locally presentable, cf. [3]. Assuming (1), it follows that a model is $\mu$-bicomplete if its underlying category is the category of sets and functions or is a variety or quasivariety of algebras. For example, the category of sets and partial functions is $\mu$-bicomplete, since this category is equivalent to the variety of pointed sets and functions that preserve the points.

### 3.2 Semantics of Circular Proofs

We shall suppose in the following that $\mathcal{C}$ is a $\mu$-bicomplete $\Omega$-model.

**Definition 3.6.** *Let* $\Pi = \langle G_0, \lambda, \rho, \sigma \rangle$ *be a circular proof over* $S, T \in \mathcal{S}(\mathcal{C})$. *If the equation* $\overline{\mathtt{x}} =_\mu q_{\overline{\mathtt{x}}}$ *is in* $S$ *(resp.* $T$*), let* $\chi$ *be the arrow part of the chosen initial algebras of the functor* $\|q_x\|_{S_x}^{(x)_{\downarrow S} \cup Z}$ *(resp.* $\|q_x\|_{T_x}^{(x)_{\downarrow T} \cup W}$*). Similarly, let* $\theta$ *be the arrow part of a chosen final coalgebra associated to an equation of the form* $\overline{\mathtt{y}} =_\nu q_{\overline{\mathtt{y}}}$ *and to the analogous functorial expression. The (natural) system of equations* $\|\Pi\|$ *in the variables* $\{h_g\}_{g \in G_0}$ *has the form*

$$\{\, h_g = \|\rho(g)\|(h_{\sigma_{g,i}})_{i \in \mathrm{Arity}(\rho(g))} \,\}_{g \in \mathcal{C}_\Pi}$$

*where*

$$
\begin{aligned}
\|\mathtt{C}f\| &= f & \|\mathtt{C}H\|(h_i)_{i\in[n]} &= H(h_1,\ldots,h_n)\\
\|\mathtt{L}{\textstyle\bigwedge}_{I\,i}\|(h) &= \mathtt{pr}_i \cdot h & \|\mathtt{R}{\textstyle\bigwedge}_I\|(h_i)_{i\in I} &= \langle h_i\rangle_{i\in I}\\
\|\mathtt{L}{\textstyle\bigvee}_I\|(h_i)_{i\in I} &= \{h_i\}_{i\in I} & \|\mathtt{R}{\textstyle\bigvee}_{I\,i}\|(h) &= h\cdot \mathtt{in}_i\\
\|\mathtt{L}\mu\overline{\mathtt{x}}\|(h) &= \chi^{-1}\cdot h & \|\mathtt{R}\overline{\mathtt{x}}_\mu\|(h) &= h\cdot\chi\\
\|\mathtt{L}\overline{\mathtt{y}}_\nu\|(h) &= \theta\cdot h & \|\mathtt{R}\nu\overline{\mathtt{y}}\|(h) &= h\cdot\theta^{-1}\quad .
\end{aligned}
$$

Let $Z = \mathrm{fv}_l(\Pi)$ and and $W = \mathrm{fv}_r(\Pi)$. This system of equation can be seen as a natural transformation

$$\|\Pi\| : \prod_{g\in\mathcal{C}_\Pi} \mathcal{C}_{S,T}(g) \times \prod_{g\in\mathcal{A}_\Pi} \mathcal{C}_{S,T}(g) \longrightarrow \prod_{g\in\mathcal{C}_\Pi} \mathcal{C}_{S,T}(g)\,,$$

where $\mathcal{C}_{S,T}(g)$ is the functor

$$\mathcal{C}(\|s_g\|_S^Z, \|t_g\|_T^W)\ : (\mathcal{C}^Z)^{op}\times\mathcal{C}^W \longrightarrow \mathcal{S}\mathrm{et}\,.$$

We can now state our main result.

**Theorem 3.7.** *The system $\|\Pi\|$ admits a unique (natural) solution*

$$\|\Pi\|^\dagger : \prod_{g\in\mathcal{A}_\Pi} \mathcal{C}_{S,T}(g) \longrightarrow \prod_{g\in\mathcal{C}_\Pi} \mathcal{C}_{S,T}(g)\,.$$

$$\{\,\overline{\mathtt{x}} =_\mu \overline{\mathtt{x}}\,\} \qquad \dfrac{\rangle\overline{\mathtt{x}}\vdash y\langle_1}{\overline{\mathtt{x}}\vdash y}\,\mathtt{L}\mu\overline{\mathtt{x}}$$

$$\{\,\overline{\mathtt{x}} =_\nu \overline{\mathtt{x}}\,\} \qquad \dfrac{\rangle\overline{\mathtt{x}}\vdash y\langle_1}{\overline{\mathtt{x}}\vdash y}\,\mathtt{L}\overline{\mathtt{x}}_\nu$$

Consider the circular proof on the right. From the fact that the associated system admits a unique solution it is easy to deduce that the interpretation of $\mu$-term $\mu_x.x$, corresponding to $\overline{\mathtt{x}}$, has to be an initial object. On the other hand, consideration of the second well typed tuple tells us that the condition on cycles is necessary. The interpretation of $\nu_x.x$ in the category of sets is any singleton set, which cannot be an initial object, i.e. the empty set.

## 4 Further Remarks and Future Work

The calculus presented in this paper satisfies a form of cut elimination, in a sound way. This is made precise in what follows.

Let $S,T$ be two directed systems, a *pointed circular proof* over $S,T$ is a pair $\langle\Pi, g_0\rangle$ where $\Pi = \langle G_0,\lambda,\rho,\sigma\rangle$ is a circular proof over $S,T$ and $g_0\in G_0$. We say that a pointed circular proof $\langle\Pi,g_0\rangle$ is *reachable* if the pointed graph $\langle\mathcal{G}(\Pi),g_0\rangle$ is reachable. A pair $(s,S)$, where $S\in\mathcal{S}(\mathcal{C})$ and $s\in\mathcal{T}(\mathcal{C})$, is closed if $\mathrm{fv}(S)=\emptyset$ and $\mathrm{fv}(s)\subseteq\overline{\mathtt{X}}_S$. By writing $\Pi_{g_0} : (s,S) \longrightarrow (t,T)$ we mean that $\Pi_{g_0} = \langle\Pi,g_0\rangle$ is a reachable pointed circular proof over $S,T$ such that $\lambda(g_0) = s\vdash t$, $\mathcal{A}_\Pi=\emptyset$ and moreover $(s,S),(t,T)$ are closed. We define the semantics of pointed reachable circular proofs in the obvious way.

**Definition 4.1.** *For* $\Pi_{g_0} : (s,S) \longrightarrow (t,T)$*, we let* $\|\Pi_{g_0}\|$ *be* $\|\Pi\|^{\dagger} \cdot \mathtt{pr}_{g_0}$.

If a pair $(s,S)$ is closed, then $\|s\|_S^{\emptyset} : \mathcal{C}^{\emptyset} \longrightarrow \mathcal{C}$ can be identified with an object of $\mathcal{C}$. Moreover, if $\Pi_{g_0} : (s,S) \longrightarrow (t,T)$, then $\mathcal{A}_{\Pi} = \emptyset$ and the domain of $\|\Pi_{g_0}\|$ is a singleton set. It follows that $\|\Pi_{g_0}\|$ can be identified with an arrow from the object $\|s\|_S^{\emptyset}$ to the object $\|t\|_T^{\emptyset}$.

**Theorem 4.2.** *Let* $\Pi_{g_0} : (s,S) \longrightarrow (t,T)$ *and* $\Gamma_{h_0} : (t,T) \longrightarrow (u,U)$ *be pointed circular proofs. There is an algorithm to construct a pointed circular proof* $\Pi_{g_0};\Gamma_{h_0} : (s,S) \longrightarrow (u,U)$ *with the property that* $\|\Pi_{g_0};\Gamma_{h_0}\| = \|\Pi_{g_0}\| \cdot \|\Gamma_{h_0}\|$.

Identities are also definable in the calculus so that, up to the equations induced by the semantics, the above construction can be extended to the construction of a category. This is a proper subcategory of a free $\mu$-bicomplete category, since the calculus is not powerful enough to describe all the arrows that are needed. The diagonal $\Delta : \mathbb{N} \longrightarrow \mathbb{N}^2$ arises as the unique algebra morphism from the initial one to the algebra $\langle\langle 0,0\rangle, s \times s\rangle : 1 + \mathbb{N}^2 \longrightarrow \mathbb{N}^2$, which is definable in the calculus being the interpretation of the circular proof of page 5 (here $s$ is the successor function on natural numbers). Let $S$ be the directed system to be found at the same page, so that $\|\overline{\mathtt{x}}\|_S^{\emptyset} = \mathbb{N}^2$ and $\|\overline{\mathtt{y}}\|_S^{\emptyset} = \mathbb{N}$.

**Proposition 4.3.** *There is no pointed reachable circular proof* $\Pi_g : (\overline{\mathtt{y}}, S) \longrightarrow (\overline{\mathtt{x}}, S)$ *such that* $\|\Pi_g\|$ *is the diagonal.*

The above result is analogous to the well known fact that the set of words $\{\, a^n b^n \mid n \geq 0 \,\}$ is not recognizable and indeed the computation which arises under the cut elimination is similar to computation with finite automata. The above result shows that the ideas presented in this paper and the syntax of the calculus have to be generalized in order to describe free $\mu$-bicomplete categories. However, it seems likely that the calculus presented here describes all the computations requiring bounded space and thus it seems interesting to understand the structure of the arising category of circular proofs, in particular to understand whether it has some kind of universal property. To this end we expect the comparison with [7] to be useful, since in this work analogous ideas are presented without a necessary reference to the notion of initial algebra.

## References


[1] S. Abramsky and R. Jagadeesan. Games and full completeness for multiplicative linear logic. *J. Symbolic Logic*, 59(2):543–574, 1994.

[2] P. Aczel. *Non-well-founded sets.* Stanford University Center for the Study of Language and Information, Stanford, CA, 1988.

[3] J. Adámek and J. Rosický. *Locally presentable and accessible categories.* Cambridge University Press, Cambridge, 1994.

[4] A. Arnold and D. Niwinski. *Rudiments of mu-calculus.* Number 146 in Studies in Logic and the Foundations of Mathematics. Elsevier (North-Holland), 2001.

[5] A. Blass. A game semantics for linear logic. *Ann. Pure Appl. Logic*, 56(1-3):183–220, 1992.

[6] S. L. Bloom and Z. Ésik. *Iteration theories*. Springer-Verlag, Berlin, 1993. The equational logic of iterative processes.

[7] S. L. Bloom, Z. Ésik, A. Labella, and E. G. Manes. Iteration 2-theories. *Appl. Categ. Structures*, 9(2):173–216, 2001.

[8] J.R.B. Cockett and R.A.G. Seely. Finite sum-product logic. *Theory and Applications of Categories*, 8:63–99, 2001.

[9] T. Coquand. Infinite objects in type theory. In *Types for proofs and programs (Nijmegen, 1993)*, pages 62–78. Springer, Berlin, 1994.

[10] T. Coquand and C. Paulin. Inductively defined types. In *COLOG-88 (Tallinn, 1988)*, pages 50–66. Springer, Berlin, 1990.

[11] J.-Y. Girard. Linear logic. *Theoret. Comput. Sci.*, 50(1):101, 1987.

[12] H. Hu and A. Joyal. Coherence completions of categories. *Theoret. Comput. Sci.*, 227(1-2):153–184, 1999. Linear logic, I (Tokyo, 1996).

[13] A. J. C. Hurkens, M. McArthur, Y. N. Moschovakis, L. S. Moss, and G. T. Whitney. The logic of recursive equations. *J. Symbolic Logic*, 63(2):451–478, 1998.

[14] A. Joyal. Free lattices, communication, and money games. In *Logic and scientific methods*, pages 29–68. Kluwer Academic Publishers, 1997.

[15] D. Kozen. Results on the propositional $\mu$-calculus. *Theoret. Comput. Sci.*, 27(3):333–354, 1983.

[16] J. Lambek. A fixpoint theorem for complete categories. *Math. Z.*, 103:151–161, 1968.

[17] M. Lenisa. A complete coinductive logical system for bisimulation equivalence on circular objects. In *Foundations of software science and computation structures (Amsterdam, 1999)*, pages 243–257. Springer, Berlin, 1999.

[18] J. J. M. M. Rutten. Universal coalgebra: a theory of systems. *Theoret. Comput. Sci.*, 249(1):3–80, 2000.

[19] L. Santocanale. The alternation hierarchy for the theory of $\mu$-lattices. Technical Report RS-00-29, BRICS, November 2000. To appear in *Theory and Applications of Categories*.

[20] L. Santocanale. Free $\mu$-lattices. Technical Report RS-00-28, BRICS, November 2000. To appear in *Journal of Pure and Applied Algebra*.

[21] L. Santocanale. *Sur les $\mu$-treillis libres*. PhD thesis, Université du Québec à Montréal, July 2000.

[22] L. Santocanale. A calculus of circular proofs and its categorical semantics. Technical Report RS-01-15, BRICS, May 2001. Extended version available from: `http://www.cpsc.ucalgary.ca/~luigis/`.

[23] L. Santocanale. Parity functors and $\mu$-bicomplete categories (extended abstract). In *Fixed Points in Computer Science 2001*, September 2001. Extended version submitted.

[24] T. Uustalu and V. Vene. Mendler-style inductive types, categorically. *Nordic J. Comput.*, 6(3):343–361, 1999. Programming theory (Turku, 1998).

[25] P. Wadler. Deforestation: transforming programs to eliminate trees. *Theoret. Comput. Sci.*, 73(2):231–248, 1990.

[26] I. Walukiewicz. Completeness of Kozen's axiomatisation of the propositional $\mu$-calculus. *Inform. and Comput.*, 157(1-2):142–182, 2000. LICS 1995 (San Diego, CA).