



---

Basic Research in Computer Science

BRICS RS-01-15 L. Santocanale: A Calculus of Circular Proofs and its Categorical Semantics

## **A Calculus of Circular Proofs and its Categorical Semantics**

**Luigi Santocanale**

**BRICS Report Series**

**ISSN 0909-0878**

**RS-01-15**

**May 2001**

**Copyright © 2001,**

**Luigi Santocanale.**

**BRICS, Department of Computer Science  
University of Aarhus. All rights reserved.**

**Reproduction of all or part of this work  
is permitted for educational or research use  
on condition that this copyright notice is  
included in any copy.**

**See back inner page for a list of recent BRICS Report Series publications.  
Copies may be obtained by contacting:**

**BRICS  
Department of Computer Science  
University of Aarhus  
Ny Munkegade, building 540  
DK-8000 Aarhus C  
Denmark  
Telephone: +45 8942 3360  
Telefax: +45 8942 3255  
Internet: BRICS@brics.dk**

**BRICS publications are in general accessible through the World Wide  
Web and anonymous FTP through these URLs:**

`http://www.brics.dk`

`ftp://ftp.brics.dk`

**This document in subdirectory RS/01/15/**

# A calculus of circular proofs and its categorical semantics

Luigi Santocanale  
luigis@brics.dk

**BRICS\***

## **Abstract**

We present a calculus of proofs, the intended models of which are categories with finite products and coproducts, initial algebras and final coalgebras of functors that are recursively constructible out of these operations, that is,  $\mu$ -bicomplete categories. The calculus satisfies the cut elimination and its main characteristic is that the underlying graph of a proof is allowed to contain a certain amount of cycles. To each proof of the calculus we associate a system of equations which has a meaning in every  $\mu$ -bicomplete category. We prove that this system admits always a unique solution, and by means of this theorem we define the semantics of the calculus.

**Keywords:** Initial algebras, final coalgebras. Fixed point calculi,  $\mu$ -calculi. Bicompletion of categories. Models of interactive computation.

## **Introduction**

The goal of this paper is to present and discuss our first results on free  $\mu$ -bicomplete categories. A category is said to be  $\mu$ -bicomplete if every finite set of objects has a product as well as a coproduct, and moreover the initial algebra and the final coalgebra of every definable functor exist.

---

\*Basic Research in Computer Science,  
Centre of the Danish National Research Foundation.

A  $\mu$ -bicomplete category is said to be free over a set  $X$  if it contains  $X$  as a subset of objects, and moreover it is canonical<sup>1</sup> among the  $\mu$ -bicomplete categories having the same property.

Among the motivations to generalize to a categorical setting the results obtained by us on free  $\mu$ -lattices [San00a, San00b, San00c], is the capability of these algebraic objects to model simple computational situations. Indeed, these results were obtained through an explicit description of free  $\mu$ -lattices by means of games and strategies. Several authors [NYY92, AJ94, Joy97] have remarked the analogy between games and winning strategies on the one hand, and systems' specifications and correct programs on the other. Accordingly, we can think of games for free  $\mu$ -lattices as being bidirectional *synchronous* communication channels which are recursively constructed from a few primitives: left and right choices, similar to the internal and external choices of CSP [Hoa85], and left and right iterations. The challenging part of our work on free  $\mu$ -lattices has been the explicit characterization of the order relation: we declared that  $S \leq T$ ,  $S$  and  $T$  being games for a free  $\mu$ -lattice, if there exists a winning strategy in a compound game of communication  $\langle S, T \rangle$  for a player called the Mediator. If  $S$  and  $T$  are thought of as channels, then such a strategy can be understood as a mediating protocol for letting the left user of the channel  $S$  communicate with the right user of  $T$  in an *asynchronous* way. Figure (1) suggests that the games  $S$  and  $T$  could be sort of telephone lines and the mediating protocol  $M$  an answering machine or an operating system. The lattice theoretic point of view, which we have adopted until now, is interested only in the existence of such strategies. The analysis of different strategies is more in the spirit of proof theory [HS86, GTL89], categorical logic [LS88], and the semantics of programming languages [Win93]. We would like to classify all the possible asynchronous communications arising in the situation described above; this is usually achieved by giving an algebra of mediating protocols, that is, a programming language by which to construct them, together with a notion of equivalence between protocols. We suggest that *the desired algebra is the one of  $\mu$ -bicomplete categories*, and that two programs should be considered equivalent if they denote the same arrow in every  $\mu$ -bicomplete category.

Motivations behind research on bicompletion of categories [Joy95, Joy97,

---

<sup>1</sup>What it means to be canonical can be made precise by introducing morphisms and then stating a universal property analogous to the universal property of the free monoid.

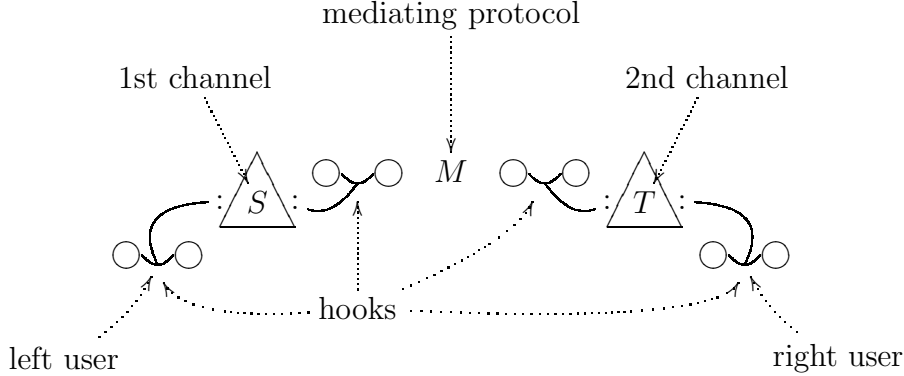


Figure 1: Games as channels, winning strategies as mediating protocols.

HJ99, CS01] are similar to those of Linear Logic [Gir87, Gir01] and related categorical models [Bar91, CS97]. With respect to these algebraic and logical settings, with  $\mu$ -bicomplete categories the focus is on initial algebras and final coalgebras of functors; from an operational perspective, the focus is on the modeling of possibly infinite computations. Initial algebras of functors are the categorical counterpart of induction and recursion, they model inductive types [CP90]; on the other hand, final coalgebras are a counterpart of coinduction and corecursion; they are related to bisimilarity, in that they classify the observable behavior of systems [Rut00]. The use of coalgebraic methods is now a well established practice to deal with infinite objects by means of their defining equations [Acz88, ML90].

In this paper we define a logical calculus to describe bounded memory deterministic strategies in a communication game of the form  $\langle S, T \rangle$ , that is, to describe the mediating protocols that use a finite amount of space. We skip here the exact description of the correspondence between the combinatorics of games and the algebra of  $\mu$ -lattices, and focus on the algebraic meaning of strategies; we remark only that if a communication strategy is translated into a proof, as usual in logics and games, then the result is a paradoxical infinite proof, or, in the case of a bounded memory strategy, a circular proof. Hence, the characteristic of our calculus is that the underlying graph of a proof is allowed to contain a certain amount of cycles. This is a common fact in fixed point theory, for example it appears in the proofs with guarded induction of type theory [Coq94] and in the refutations of the propositional  $\mu$ -calculus [Wal00]. In order

to define the semantics, we proceed as follows: once the type-terms of the calculus are interpreted in the obvious way by means of products, coproducts, initial algebras and final coalgebras, then the proof-terms are also interpreted in a natural way as systems of equations. The main achievement of this paper, theorem 4.11, states that such systems of equations admit always a unique solution. The semantics of a circular proof with a chosen conclusion is then defined to be the chosen projection of the vector solution.

The calculus does not contain an explicit cut rule, it satisfies the cut elimination: two proofs can be composed in a sound way, leading to a proof the interpretation of which is the composition of the interpretations of the two original proofs. However, the calculus is not powerful enough to describe all the arrows of a free  $\mu$ -bicomplete category, which 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.

We approach the theory of initial algebras and final coalgebras from fixed point theory [BÉ93] - the two theories are closely related, see for example [Fre91]. From [Lam68], it is known that, in an initial algebra  $\chi : S\mathbf{x} \longrightarrow \mathbf{x}$  of an endofunctor  $S : \mathcal{C} \longrightarrow \mathcal{C}$ , the arrow  $\chi$  is invertible, so that its universal property states the existence and uniqueness of a solution of the equation

$$f = \chi^{-1} \cdot Sf \cdot \alpha,$$

for each algebra  $\alpha : Sa \longrightarrow a$ . The above equation is rephrased in a more compact way as the fixed point equation

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

where the natural transformation

$$\alpha_x : \mathcal{C}(x, a) \longrightarrow \mathcal{C}(Sx, a)$$

is obtained from the previous  $\alpha$  under the Yoneda correspondence, that is,  $\alpha_a(\text{id}_a) = \alpha$ . The next step is to realize that also parameterized fixed points exist whenever the category  $\mathcal{C}$  has products. We prove that, for every natural transformation of the form

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

where  $S : \mathcal{C} \times \mathcal{Z} \longrightarrow \mathcal{C}$ ,  $T : \mathcal{W} \longrightarrow \mathcal{C}$  and  $Q$  is a parameterized set, covariant in  $w$ , contravariant in  $x$  and  $z$ , there exists a unique solution of the equation

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

for each choice of  $q \in Q(\mathbf{x}_z, z, w)$ . In this case

$$\chi_z : S(\mathbf{x}_z, z) \longrightarrow \mathbf{x}_z$$

is the initial algebra of the functor  $S(x, z)$ , parameterized in the variable  $z$ . The existence of parameterized unique fixed points leads to show that circular proofs, whenever interpreted as systems of equations, admit always a unique solution.

The paper is organized as follows: we introduce the notation and the key concepts of the theory in section 1. In section 2 we describe the syntactical part of the calculus, defining first the terms and then the proofs. In section 3 we prove the main theorem about the existence and uniqueness of certain parameterized fixed points. In section 4, we use this theorem to define the semantics of the calculus. In section 5, as concluding remarks, we discuss the fact that the calculus is not expressive enough with respect to its intended models and suggest a natural relation with automata theory.

## 1 Notation and preliminaries

### Notation.

With  $\mathbf{Set}$  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  $\{1, \dots, n\}$ . Composition in categories, say

$$A \xrightarrow{f} B \xrightarrow{g} C,$$

will be denoted in two different ways, that is,  $g \circ f$  and  $f \cdot g$ . Sometime we shall omit the symbol  $\circ$  and write  $gf$ , but we write always the symbol  $\cdot$ . We shall use  $\mathbf{id}$  for identities,  $\langle \rangle$  and  $\mathbf{pr}$  for tuples and projections,  $\{ \}$  and  $\mathbf{in}$  for cotuples and injections, for every kind of categorical products and coproducts.

### Initial algebras of a functor.

Let  $\mathcal{C}$  be a category and  $S : \mathcal{C} \longrightarrow \mathcal{C}$  be an endofunctor. A *S-algebra* is a pair  $(c, \gamma)$ , where  $c$  is an object of  $\mathcal{C}$  and  $\gamma : Sc \longrightarrow c$  is an arrow of  $\mathcal{C}$ . A morphism of *S-algebras*  $f : (c, \gamma) \longrightarrow (d, \delta)$  is an arrow  $f : c \longrightarrow d$  of  $\mathcal{C}$  such that  $\gamma \cdot f = Sf \cdot \delta$ . *S-algebras* and their morphisms form a category  $\mathcal{C}^S$ . A *T-algebra*  $(\mathbf{x}, \chi)$  is initial if for each algebra  $(c, \gamma)$  there exists a unique arrow  $! \gamma : \mathbf{x} \longrightarrow c$  such that  $\chi \cdot ! \gamma = S! \gamma \cdot \gamma$ . *S-coalgebras* and their morphisms are defined in the dual way and form a category  $\mathcal{C}_S$ . We recall that a coalgebra  $\zeta : \mathbf{y} \longrightarrow S\mathbf{y}$  is final if for each coalgebra  $\gamma : c \longrightarrow Sc$  there exists a unique arrow  $! \gamma : c \longrightarrow \mathbf{y}$  such that  $! \gamma \cdot \zeta = \gamma \cdot S! \gamma$ .

We explain our conventions concerning variables. Each variable  $x, y, z, \dots$  can be in two states: either it is free, in which case it denotes a projection functor, or it is bounded to some value. As a general rule, we shall use the usual style  $x, y, z, \dots$  for free variables and the typewriter style  $\mathbf{x}, \mathbf{y}, \mathbf{z}, \dots$  for bounded variables. For example, with an equation of the form

$$\mathbf{x} =_{\mu} S\mathbf{x}$$

we shall mean that the denotation of  $\mathbf{x}$  is the object part of a chosen initial *S-algebra*, in which case we shall use the corresponding Greek letter  $\chi$  to denote the arrow part of this *S-algebra*.

### Systems of equations.

**Definition 1.1** Let  $\alpha : C \times A \longrightarrow C$  be an arrow in the functor category  $\text{Set}^{\mathcal{D}}$ . We shall say that  $\alpha$  *admits a unique solution* if, for each object  $d$  of  $\mathcal{D}$  and each  $a \in A_d$ , there exists a unique  $c \in C_d$  such that  $\alpha_d(c, a) = a$ . If  $\alpha$  admits a unique solution we shall denote by  $\alpha_d^{\dagger}(a)$  such a  $c \in C_d$ . 1.1

**Lemma 1.2** If  $\alpha$  admits a unique solution, then the collection  $\{\alpha_d^{\dagger}\}_{d \in \text{Obj}(\mathcal{D})}$  is a natural transformation  $\alpha^{\dagger} : A \longrightarrow C$ .

**Lemma 1.3** Let  $\alpha : C \times A \longrightarrow C$  be an arrow of the functor category  $\text{Set}^{\mathcal{D}}$  and let  $F : \mathcal{C} \longrightarrow \mathcal{D}$  be a functor. If  $\alpha$  admits a unique solution, then  $\alpha_F$  – that is, the arrow  $\text{Set}^F(\alpha)$  of the category  $\text{Set}^{\mathcal{C}}$  – admits the unique solution  $(\alpha^{\dagger})_F$ .

**Definition 1.4** A *natural system of equations* is a tuple  $\langle I, C, F, \alpha, \beta \rangle$ , where



- $I$  is a finite indexing set, and for each  $i \in I$ ,  $F_i$  is a functor from  $\mathcal{D}$  to  $\text{Set}$ .
- $C \subseteq I$  is the set of bounded indexes.
- For each  $c \in C$ ,  $\beta_c \subseteq I$  and

$$\alpha_c : \prod_{k \in \beta_c} F_k \longrightarrow F_c$$

is a natural transformation.

We say that a natural system of equations admits a unique solution if the arrow

$$\prod_{c \in C} F_c \times \prod_{a \in I \setminus C} F_a \xrightarrow{\langle \alpha_c \circ \text{pr}_{\beta_c} \rangle_{c \in C}} \prod_{c \in C} F_c$$

admits a unique solution.

1.4

In the following “system” will be synonymous of natural system of equations. We shall represent systems with the usual notation:

$$\{ c = \alpha_c(\beta_c) \}_{c \in C} .$$

The Bekič property holds, we state it in the form of a sufficient condition to determine whether a system admits a unique solution.

**Proposition 1.5** If the system

$$\{ c = \alpha_c(c, \alpha_d(c, a), a) \}$$

admits a unique solution, then also the system

$$\left\{ \begin{array}{l} c = \alpha_c(c, d, a) \\ d = \alpha_d(c, a) \end{array} \right\}$$

admits a unique solution. If the systems

$$\left\{ \begin{array}{l} d = \alpha_d(d, c, a) \\ c = \alpha_c(c, d, a) \\ d = \alpha_d^\dagger(c, a) \end{array} \right\}$$

admit a unique solution, then also the system

$$\left\{ \begin{array}{l} c = \alpha_c(c, d, a) \\ d = \alpha_d(d, c, a) \end{array} \right\}$$

admits a unique solution.

## 2 The calculus of circular proofs

### 2.1 Directed systems of labeled equations

We shall fix a signature  $\Omega$  and by writing  $H \in \Omega_n$ , where  $n \geq 0$ , we shall 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  $\mathcal{T}(\mathcal{C})$  and the free variables function  $\text{fv} : \mathcal{T}(\mathcal{C}) \longrightarrow P(X)$  are defined by induction by the following clauses:

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

For  $Y \subseteq X$ , we let  $\mathcal{T}(\mathcal{C}, Y)$  be the collection of terms  $s \in \mathcal{T}(\mathcal{C})$  such that  $\text{fv}(s) \subseteq Y$ . 2.1

**Remark 2.2** Let  $s : \{l, r\} \longrightarrow \mathcal{T}(\mathcal{C})$  be a function. In the examples we shall informally use the standard notation  $s_l \wedge s_r, s_l \vee s_r$  for  $\bigwedge_{\{l, r\}} s, \bigvee_{\{l, r\}} s$ , respectively. Similarly,  $\top$  stands for  $\bigwedge_{\emptyset}$  and  $\perp$  stands for  $\bigvee_{\emptyset}$ . 2.2

**Definition 2.3** A *polarized system of equations* over  $\mathcal{C}$  is a tuple  $\langle \mathbf{X}, q, \epsilon \rangle$  where

- $\mathbf{X} \subseteq X$  is a finite subset of  $X$ , the set of bounded variables.
- $q : \mathbf{X} \longrightarrow \mathcal{T}(\mathcal{C})$  is a function which associates to each bounded variable its value.
- $\epsilon : \mathbf{X} \longrightarrow \{\mu, \nu\}$  is a labeling of equations.

2.3

We represent a polarized system of equations  $\langle X, q, \epsilon \rangle$  with the notation:

$$\left\{ x =_{\epsilon_x} q_x \right\}_{x \in X}.$$

**Definition 2.4** Let  $\langle X, q, \epsilon \rangle$  be a polarized system of equations over  $\mathcal{C}$ . The relation  $\rightarrow$  on the set of variables of  $X$  is defined as follows:

$$x \rightarrow y \text{ iff } x \in X_S \text{ and } y \in \text{fv}(q_x).$$

A tuple  $S = \langle X_S, q_S, \epsilon_S, X_{0,S} \rangle$  is said to be a *directed system* over  $\mathcal{C}$  if  $\langle X_S, q_S, \epsilon_S \rangle$  is a polarized system of equations and  $X_{0,S} \subseteq X_S$ ; moreover, for each  $x \in X_S$  there exists a unique simple path in the graph  $\langle X_S, \rightarrow \rangle$  from an element  $r(x) \in X_{0,S}$  to  $x$ . That is, the tuple  $\langle X_{0,S}, X_S, \rightarrow \rangle$  is a *forest with back edges*. If  $x, y \in X_S$ , we shall write  $x \leq_S y$  if  $x$  lies on the simple path from  $r(y)$  to  $y$ ; we shall write  $x <_S y$  if  $x \leq_S y$  and  $x \neq y$ . We let

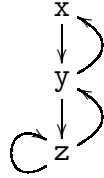
$$\text{fv}(S) = \left( \bigcup_{x \in X_S} \text{fv}(q_x) \right) \setminus X_S,$$

and by  $V(S)$  we shall denote the collection of finite subsets  $Y$  of  $X$  such that  $Y \cap X_S = \emptyset$  and  $\text{fv}(S) \subseteq Y$ . With  $\mathcal{S}(\mathcal{C})$  we shall denote the collection of directed systems over  $\mathcal{C}$ . 2.4

**Example 2.5** Directed systems are (roughly speaking) another representation of  $\mu$ -terms, they are analogous to the hierarchical systems of equations of [Sei96]. For example, the  $\mu$ -term  $\mu_x.\nu_y.(x \wedge \mu_z.(z \vee y))$  is translated into the directed system

$$\left\langle \left\{ \begin{array}{l} x =_{\mu} y \\ y =_{\nu} x \wedge z \\ z =_{\mu} z \vee y \end{array} \right\}, \{x\} \right\rangle.$$

The forest with back edges is in this case a tree with back edges, since  $X_0 = \{x\}$  is a singleton, and it is given in the following diagram:



The ordering is  $x < y < z$ . 2.5

**Definition 2.6** Let  $S$  be a directed system and let  $F \subseteq X_S$  be an order filter, that is, a subset of  $X_S$  with the property that if  $\mathbf{x} \in F$  and  $\mathbf{x} \leq_S \mathbf{y}$ , then  $\mathbf{y} \in F$ . We define the system  $S_F$  as follows:

- $X_{S_F} = F$ .
- $q_{S_F}$  and  $\epsilon_{S_F}$  are the restrictions of  $q_S$  and  $\epsilon_S$  to  $F$ , respectively.
- $X_{0,S_F} = \{ \mathbf{y} \in F \mid \mathbf{z} <_S \mathbf{y} \text{ implies } \mathbf{z} \notin F \}$ .

We shall write  $S_x$  for  $S_F$ , where  $F = \{ \mathbf{y} \mid \mathbf{x} <_S \mathbf{y} \}$ . 2.6

**Lemma 2.7** The inequality

$$\text{fv}(S_x) \subseteq \text{fv}(S) \cup (\mathbf{x})_{\downarrow_S}$$

holds, where  $(\mathbf{x})_{\downarrow_S} = \{ \mathbf{y} \in X_S \mid \mathbf{y} \leq_S \mathbf{x} \}$ .

## 2.2 Circular proofs

**Definition 2.8** 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 the following table:

Rule	Range	Arity
A		[0]
Cf	$f$ is an arrow of $\mathcal{C}$	[0]
CH	$H \in \Omega_n$	[ $n$ ]
$L\bigwedge_{Ii}$	$I$ is a finite set, $i \in I$	[1]
$R\bigwedge_I$	$I$ is a finite set	$I$
$L\bigvee_I$	$I$ is a finite set	$I$
$R\bigvee_{Ii}$	$I$ is a finite set, $i \in I$	[1]
$L\mu\mathbf{x}$	$\mathbf{x} \in X_S, \epsilon_{\mathbf{x}} = \mu$	[1]
$R\mathbf{y}\mu$	$\mathbf{y} \in X_T, \epsilon_{\mathbf{y}} = \mu$	[1]
$L\mathbf{x}\nu$	$\mathbf{x} \in X_S, \epsilon_{\mathbf{x}} = \nu$	[1]
$R\nu\mathbf{y}$	$\mathbf{y} \in X_T, \epsilon_{\mathbf{y}} = \nu$	[1]

2.8

**Definition 2.9** Let  $S, T$  be two directed systems over  $\mathcal{C}$ . A tuple  $\langle G_0, \lambda, \rho, \sigma \rangle$ , where

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

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

$$\begin{array}{c}
\frac{}{s \vdash t} \text{A} \\
\\
\frac{}{\text{dom } f \vdash \text{cod } f} \text{Cf} \\
\\
\frac{\{s_i \vdash t_i\}_{i \in [n]}}{Hs \vdash Ht} \text{CH} \\
\\
\frac{s_i \vdash t}{\bigwedge_I s \vdash t} \text{L}\bigwedge_{I_i} \qquad \frac{\{s \vdash t_i\}_{i \in I}}{s \vdash \bigwedge_I t} \text{R}\bigwedge_I \\
\\
\frac{\{s_i \vdash t\}_{i \in I}}{\bigvee_I s \vdash t} \text{L}\bigvee_I \qquad \frac{s \vdash t_i}{s \vdash \bigvee_I t} \text{R}\bigvee_{I_i} \\
\\
\frac{q_x \vdash t}{x \vdash t} \text{L}\mu_x \qquad \frac{s \vdash q_y}{s \vdash y} \text{R}\nu_\mu \\
\\
\frac{q_x \vdash t}{x \vdash t} \text{L}\nu_\nu \qquad \frac{s \vdash q_y}{s \vdash y} \text{R}\nu_y
\end{array}$$

Here a typing constraint of the form

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

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  $i \in \text{Arity}(R)$   $\lambda(\sigma_{g,i})$  has the form  $s_i \vdash t_i$ .* 2.9

**Definition 2.10** Let  $P = \langle G_0, \lambda, \rho, \sigma \rangle$  be a tuple which is well typed over  $S, T$ . The graph  $\mathcal{G}(P) = \langle G_0, \rightarrow \rangle$  has as vertexes the elements of  $G_0$ , and

$$g \rightarrow g' \quad \text{iff} \quad g' = \sigma_{g,i}.$$

for some  $i \in \text{Arity}(\rho(g))$ . 2.10

**Definition 2.11** Let  $P$  be a tuple well typed over  $S, T$ , and let  $\gamma_0 \rightarrow \gamma_1 \rightarrow \dots \gamma_n = \gamma_0$ ,  $n \geq 1$ , be a proper cycle of  $\mathcal{G}(P)$ . We let  $\gamma_S, \gamma_T$  be the sets

$$\begin{aligned} & \{ \mathbf{x} \in \mathbf{X}_S \mid \exists i \in [n] \text{ s.t. } \rho(\gamma_i) \in \{L\mu\mathbf{x}, L\mathbf{x}\nu\} \}, \\ & \{ \mathbf{x} \in \mathbf{X}_T \mid \exists i \in [n] \text{ s.t. } \rho(\gamma_i) \in \{R\mathbf{x}\mu, R\nu\mathbf{x}\} \}, \end{aligned}$$

respectively.

2.11

**Remark 2.12** 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 component 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  $\gamma_T$ .

2.12

**Definition 2.13** 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

$$\gamma_S \neq \emptyset \text{ and } \epsilon(\min \gamma_S) = \mu,$$

or

$$\gamma_T \neq \emptyset \text{ and } \epsilon(\min \gamma_T) = \nu.$$

2.13

**Remark 2.14** In the following we shall refer to the first statement as  $L(\gamma)$ , and to the second as  $R(\gamma)$ , 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  $L(\gamma)$  holds, or  $R(\gamma)$  holds. The above condition can be understood as follows: the systems  $S$  and  $T$  can be a translation of games for free  $\mu$ -lattices, and a circular proof is meant to describe a bounded memory winning strategy in the compound game  $\langle S, T \rangle$ , which we described in [San00c, San00a, San00b] and recalled in the introduction. As in Blass' game semantics of Linear Logic [Bla72, Bla92] and in Joyal's games for communication [Joy97], a player called Mediator has to win either on  $S$  or on  $T$ . On the other hand, the games  $S$  and  $T$  are parity games; these games have shown to be a useful tool in the study of Monadic Second Order Logic [GH82] and of Propositional  $\mu$ -Calculus, a general introduction to them can be found in [Zie98]. Henceforth, the condition  $L(\gamma)$  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 its winning strategy.

2.14

**Definition 2.15** Let  $\Pi = \langle G_0, \lambda, \rho, \sigma \rangle$  be a circular proof over  $S, T$ . We say that a vertex  $g \in G_0$  is a *conclusion* if  $\rho(g) \neq \mathbf{A}$  and that it is an *assumption* if  $\rho(g) = \mathbf{A}$ . We denote by  $\mathcal{C}_\Pi$  and  $\mathcal{A}_\Pi$  the set of conclusions and the set of assumptions of  $\Pi$ , respectively. 2.15

We shall use often the notation  $s_g$  if  $g$  is a vertex of a circular proof and  $\lambda(g) = s_g \vdash t$  for some  $t \in \mathcal{T}(\mathcal{C})$ . We shall also use a similar notation  $t_g$ .

**Definition 2.16** Let  $\Pi$  be a circular proof over the directed systems  $S, T$ , we define

$$\begin{aligned} \text{fv}_l(\Pi) &= \text{fv}(S) \cup \left( \bigcup_{g \in G_0} \text{fv}(s_g) \right) \setminus \mathbf{X}_S, \\ \text{fv}_r(\Pi) &= \text{fv}(T) \cup \left( \bigcup_{g \in G_0} \text{fv}(t_g) \right) \setminus \mathbf{X}_T. \end{aligned}$$

Observe that  $\text{fv}_l(\Pi) \in V(S)$  and  $\text{fv}_r(\Pi) \in V(T)$ , and that, for  $g \in G_0$ ,  $s_g \in \mathcal{T}(\mathcal{C}, \mathbf{X}_S \cup \text{fv}_l(\Pi))$  and  $t_g \in \mathcal{T}(\mathcal{C}, \mathbf{X}_T \cup \text{fv}_r(\Pi))$ . 2.16

**Definition 2.17** Let  $\Pi$  be a circular proof over  $S, T$ , its complexity  $\#\Pi$  is the pair of numbers  $(\text{card } \mathcal{C}_\Pi, \text{card } \mathbf{X}_S + \text{card } \mathbf{X}_T)$ . 2.17

**Remark 2.18** Observe that  $\#\Pi \in \mathbb{N}^2$ , and this set comes with the lexicographic order:  $(n, m) \leq (n', m')$  if and only if  $n \leq n'$  and  $n = n'$  implies  $m \leq m'$ . The strict order  $<$  arising from the lexicographic order is a well founded relation. Hence, we shall prove properties of circular proofs by induction on  $\#\Pi$ , by providing a base case if  $\text{card } \mathcal{C}_\Pi = 0$  and an induction step if  $\text{card } \mathcal{C}_\Pi > 0$ . 2.18

**Definition 2.19** A circular proof  $\Pi = \langle G_0, \lambda, \rho, \sigma \rangle$  is said to be *strongly connected* if, for each pair of conclusions  $g_1, g_2 \in \mathcal{C}_\Pi$ , we can find paths  $g_1 \rightarrow^* g_2$  and  $g_2 \rightarrow^* g_1$  in  $\mathcal{G}(\Pi)$ . 2.19

We draw examples of circular proofs with a given base point and such that their underlying graph is a tree with back edges. Indeed, we want to remark the analogy with the usual model of a proof as a finite tree and use existing tools for drawing proofs. Hence, we shall draw trees with some of the leaves annotated by a number. With the notation

$$\frac{\lambda(g) \quad \rho(g)}{\vdots} \quad \text{...} \quad \text{...}$$

we mean that there is a transition in  $\mathcal{G}(\Pi)$  from  $g$  to the  $n$ -th vertex  $g'$  on the path from the root to  $g$ .

**Example 2.20** Let  $S$  be the directed system

$$\left\langle \left\{ \begin{array}{l} \mathbf{x} =_{\nu} \mathbf{y} \\ \mathbf{y} =_{\mu} \mathbf{x} \wedge \mathbf{y} \end{array} \right\}, \{\mathbf{x}\} \right\rangle$$

so that the associated order is  $\mathbf{x} <_S \mathbf{y}$ . Let  $T$  be the empty system of equations, then

$$\frac{\frac{\frac{\mathbf{y} \vdash \perp \langle_2}{\mathbf{x} \wedge \mathbf{y} \vdash \perp} \text{L}\wedge_{\{l,r\}r}}{\mathbf{y} \vdash \perp} \text{L}\mu\mathbf{y}}{\mathbf{x} \vdash \perp} \text{L}\mathbf{x}_{\nu}}$$

is a circular proof over  $S, T$ . The following is not a circular proof, since it does not satisfy condition of definition 2.13 on cycles:

$$\frac{\frac{\frac{\frac{\mathbf{x} \vdash \perp \langle_1}{\mathbf{x} \wedge \mathbf{y} \vdash \perp} \text{L}\wedge_{\{l,r\}l}}{\mathbf{y} \vdash \perp} \text{L}\mu\mathbf{y}}{\mathbf{x} \vdash \perp} \text{L}\mathbf{x}_{\nu}}$$

Indeed, let  $\gamma$  be the only simple cycle on this graph.  $\mathbf{R}(\gamma)$  does not hold, since  $\gamma_T = \emptyset$ . On the other hand  $\mathbf{L}(\gamma)$  does not hold, since  $\min \gamma_S = \mathbf{x}$  and  $\epsilon(\mathbf{x}) = \nu$ . 2.20



**Example 2.21** A more complex example is the following:

$$\begin{array}{c}
\frac{}{\top \vdash \top} \text{R}\wedge_{\emptyset} \\
\frac{}{\top \vdash \top \vee x_1} \text{R}\vee_{\{l,r\}l} \quad \frac{\rangle x_1 \vdash x_1 \langle_{10}}{x_1 \vdash \top \vee x_1} \text{R}\vee_{\{l,r\}r} \\
\hline
\frac{}{\top \vee x_1 \vdash \top \vee x_1} \text{L}\vee_{\{l,r\}} \\
\frac{}{\top \vee x_1 \vdash x_1} \text{R}y_{\mu} \\
\frac{}{x_1 \vdash x_1} \text{L}\mu x_1 \\
\frac{}{x_1 \vdash \top \vee x_1} \text{R}\vee_{\{l,r\}r} \\
\frac{}{x_1 \vdash x_1} \text{R}x_{1\mu} \\
\frac{}{x_1 \vdash x_1 \vee x_2} \text{R}\vee_{\{l,r\}l} \quad \frac{\rangle x_2 \vdash x_2 \langle_4}{x_2 \vdash x_1 \vee x_2} \text{R}\vee_{\{l,r\}r} \\
\hline
\frac{}{\top \vdash \top} \text{R}\wedge_{\emptyset} \quad \frac{x_1 \vee x_2 \vdash x_1 \vee x_2}{x_1 \vee x_2 \vdash x_2} \text{R}x_{1\mu} \\
\frac{}{\top \vdash \top \vee x_1} \text{R}\vee_{\{l,r\}l} \quad \frac{x_1 \vee x_2 \vdash x_2}{x_2 \vdash x_2} \text{L}\mu x \\
\frac{}{\top \vdash x_1} \text{R}x_{1\mu} \quad \frac{}{x_1 \vdash x_2} \text{R}\vee_{\{l,r\}r} \\
\frac{}{\top \vdash x_1 \vee x_2} \text{R}\vee_{\{l,r\}l} \quad \frac{}{x_1 \vdash x_2 \vee x_2} \text{R}x_{\mu} \\
\frac{}{\top \vdash x_2} \text{R}x_{2\mu} \quad \frac{}{x_1 \vdash x_2} \text{L}\vee_{\{l,r\}} \\
\hline
\frac{}{\top \vee x_2 \vdash x_2}
\end{array}$$

This circular proof is over  $S_2, S_2$ , the directed system  $S_2$  being defined at page 26. 2.21

### 2.3 Operations on circular proofs

**Taking the reachable part.**

Let  $\Pi = \langle G_0, \lambda, \rho, \sigma \rangle$  be a circular proof and let  $C \subseteq G_0$ . We define  $\overline{\Pi}, \overline{C}$  to be the circular proof  $\langle H_0, \lambda', \rho', \sigma' \rangle$ , where  $H_0 \subseteq G_0$  and  $g \in H_0$  if and only if we can find  $c \in C$  and a path  $c \rightarrow^* g$  in  $\mathcal{G}(\Pi)$ ;  $\lambda', \rho', \sigma'$  are the restriction of the analogous functions to  $H_0$ .

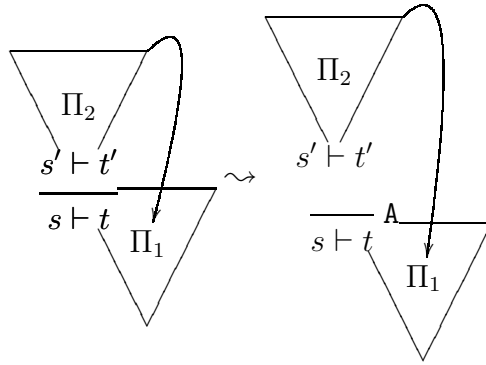
If  $C = \{g\}$ , then we shall write  $\overline{\Pi}, \overline{g}$  instead of  $\overline{\Pi}, \{g\}$ . By definition,  $\mathcal{G}(\overline{\Pi}, \overline{g})$  is a pointed reachable graph.

### Addition of new assumptions.

Let  $\Pi = \langle G_0, \lambda, \rho, \sigma \rangle$  be a circular proof and let  $A \subseteq G_0$ . We define  $\Pi^A$  to be the circular proof  $\langle G_0, \lambda, \rho', \sigma \rangle$ , where

$$\rho'(g) = \begin{cases} \rho(g), & g \in G_0 \setminus A, \\ A, & g \in A. \end{cases}$$

We draw this operation as follows:



## 3 A parameterized fixed point theorem

In this section we prove the theorem that enables us to define the semantics of the calculus.

**Theorem 3.1** 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 as follows:

$$\begin{aligned} S &: \mathcal{C} \times \mathcal{Z} \longrightarrow \mathcal{C} \\ T &: \mathcal{W} \longrightarrow \mathcal{C} \\ Q &: \mathcal{C}^{op} \times \mathcal{Z}^{op} \times \mathcal{W} \longrightarrow \text{Set}. \end{aligned}$$

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

$$\chi_z \cdot f = \alpha_{\mathbf{x}_z, z, w}(f, q).$$

Before proving the theorem, we observe that the condition that  $C$  has products is necessary. Consider the discrete poset  $\{a, b\}$  and the constant function  $Sx = a$ , so that  $a$ , being the unique fixed point, is the initial  $S$ -algebra. In  $\{a, b\}$ , the following implication holds:

$$x < b \Rightarrow Sx \leq b.$$

Let  $Q(x, b)$  be the statement  $b \not\leq x$ , then the above implication is

$$x \leq b \wedge Q(x, b) \Rightarrow Sx \leq b$$

and if the theorem were true also in this case, we would be allowed to deduce

$$Q(a, b) \Rightarrow a \leq b.$$

Since  $b \not\leq a$ , then we would deduce that  $a \leq b$ .

In the proof we shall use a bimodule notation, that is, for  $q \in Q(x, z, w)$ , we let

$$\begin{aligned} (f, g) \cdot q &= Q(f, g, \text{id}_w)(q) \\ q \cdot h &= Q(\text{id}_x, \text{id}_z, h)(q). \end{aligned}$$

Naturality in  $x$  of  $\alpha$  leads to the relation

$$\begin{aligned} \alpha_{x', z, w}(h \cdot f, (h, \text{id}_z) \cdot q) \\ = S(h, \text{id}_z) \cdot \alpha_{x, z, w}(f, q) \end{aligned}$$

for  $h : x' \longrightarrow x$ .

*Proof of theorem 3.1.* We show first that the above equation admits a solution. Let  $z$  be an object of  $\mathcal{Z}$ ,  $w$  be an object of  $\mathcal{W}$  and  $q \in Q(\mathbf{x}_z, z, w)$ . Consider the two projections  $\text{pr}_{\mathbf{x}_z}, \text{pr}_{Tw}$  from the product  $\mathbf{x}_z \times Tw$  and observe that  $(\text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot q \in Q(\mathbf{x}_z \times Tw, z, w)$ . It makes sense to consider the arrow

$$\alpha_{\mathbf{x}_z \times Tw, z, w}(\text{pr}_{Tw}, (\text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot q) : S(\mathbf{x}_z \times Tw, z) \longrightarrow Tw.$$

Pair this arrow with

$$S(\text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot \chi_z : S(\mathbf{x}_z \times Tw, z) \longrightarrow \mathbf{x}_z$$

to obtain a  $S(x, z)$ -algebra  $(\mathbf{x}_z \times Tw, \beta)$ . Let  $!\beta$  be the unique morphism of  $S(x, z)$ -algebras from the initial one to  $(\mathbf{x}_z \times Tw, \beta)$ , and observe that

$$!\beta \cdot \text{pr}_{\mathbf{x}_z} = \text{id}_{\mathbf{x}_z},$$

since  $\text{pr}_{\mathbf{x}_z}$  is a morphism of  $S(x, z)$ -algebras. Let

$$f = !\beta \cdot \text{pr}_{Tw} : \mathbf{x}_z \longrightarrow Tw,$$

then the relation  $\chi_z \cdot f = \alpha_{\mathbf{x}_z, z, w}(f, q)$  holds:

$$\begin{aligned} \chi_z \cdot f &= \chi_z \cdot !\beta \cdot \text{pr}_{Tw} \\ &= S(!\beta, \text{id}_z) \cdot \beta \cdot \text{pr}_{Tw} \\ &= S(!\beta, \text{id}_z) \cdot \alpha_{\mathbf{x}_z \times Tw, z, w}(\text{pr}_{Tw}, (\text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot q) \\ &= \alpha_{\mathbf{x}_z, z, w}(!\beta \cdot \text{pr}_{Tw}, (!\beta, \text{id}_z) \cdot (\text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot q) \\ &= \alpha_{\mathbf{x}_z, z, w}(f, (!\beta \cdot \text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot q) \\ &= \alpha_{\mathbf{x}_z, z, w}(f, q). \end{aligned}$$

On the other hand, suppose that  $\chi_z \cdot f = \alpha_{\mathbf{x}_z, z, w}(f, q)$ , and let

$$\gamma = \langle \text{id}_{\mathbf{x}_z}, f \rangle : \mathbf{x}_z \longrightarrow \mathbf{x}_z \times Tw.$$

We shall show that

$$\chi_z \cdot \gamma = S(\gamma, \text{id}_z) \cdot \beta,$$

and, as a consequence, we shall deduce that  $\gamma = !\beta$  and that  $f = \gamma \cdot \text{pr}_{Tw} = !\beta \cdot \text{pr}_{Tw}$ . Indeed, we have:

$$\begin{aligned} \chi_z \cdot \gamma \cdot \text{pr}_{\mathbf{x}_z} &= \chi_z \\ &= S(\gamma \cdot \text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot \chi_z \\ &= S(\gamma, \text{id}_z) \cdot S(\text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot \chi_z \\ &= S(\gamma, \text{id}_z) \cdot \beta \cdot \text{pr}_{\mathbf{x}_z}, \end{aligned}$$

and

$$\begin{aligned} \chi_z \cdot \gamma \cdot \text{pr}_{Tw} &= \chi_z \cdot f \\ &= \alpha_{\mathbf{x}_z, z, w}(f, q) \\ &= \alpha_{\mathbf{x}_z, z, w}(\gamma \cdot \text{pr}_{Tw}, (\gamma \cdot \text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot q) \\ &= S(\gamma, \text{id}_z) \cdot \alpha_{\mathbf{x}_z \times Tw, z, w}(\text{pr}_{Tw}, (\text{pr}_{\mathbf{x}_z}, \text{id}_z) \cdot q) \\ &= S(\gamma, \text{id}_z) \cdot \beta \cdot \text{pr}_{Tw}. \end{aligned}$$

□

As in 1.2, unique solutions of the above equation make up a natural transformation

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

A similar dual technique has been used in [AAV00, Mos00] to prove the universal property of iteration monads. The full dual statement, which we need to prove theorem 4.11, is as follows:

**Theorem 3.2** Let  $\mathcal{Z}, \mathcal{W}, \mathcal{C}$  be three categories, of which  $\mathcal{C}$  has finite co-products, and let  $S, T$  and  $Q$  be functors as follows:

$$\begin{aligned} S & : \mathcal{Z} \longrightarrow \mathcal{C} \\ T & : \mathcal{C} \times \mathcal{W} \longrightarrow \mathcal{C} \\ Q & : \mathcal{Z}^{op} \times \mathcal{C} \times \mathcal{W} \longrightarrow \text{Set} . \end{aligned}$$

Consider a natural transformation

$$\alpha_{z,y,w} : \mathcal{C}(Sz, y) \times Q(z, y, w) \longrightarrow \mathcal{C}(Sz, T(y, w))$$

and let  $(\mathbf{y}_w, \varsigma_w)$  be a parameterized final coalgebra of the functor  $T(y, w)$ . For each object  $z$  of  $\mathcal{Z}$ ,  $w$  of  $\mathcal{W}$  and each  $q \in Q(z, \mathbf{y}_w, w)$ , there exists a unique  $f : Sz \longrightarrow \mathbf{y}_w$  which is a solution of the equation

$$f \cdot \varsigma_w = \alpha_{z, \mathbf{y}_w, w}(f, q) .$$

## 4 Semantics of the calculus

### 4.1 Semantics of systems, $\mu$ -bicomplete categories

**Definition 4.1** Let  $\mathcal{C}$  be a category, 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  $S(x, z)$  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

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

admits initial algebras. A *choice of initial algebras* is a correspondence  $(\mathbf{x}, \chi)$  which 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  $\chi_z : S(\mathbf{x}_z, z) \longrightarrow \mathbf{x}_z$ . We shall require that a choice of initial algebras is stable under substitution, that is, if  $\chi_z : S(\mathbf{x}_z, z) \longrightarrow \mathbf{x}_z$  is the initial algebra associated to the pair  $(S, z)$ , then  $\chi_{Ru} : S(\mathbf{x}_{Ru}, Ru) \longrightarrow \mathbf{x}_{Ru}$  is the initial algebra associated to the pair  $(S \circ (\text{id}_{\mathcal{C}} \times R), u)$ . A *choice of final coalgebras* is defined in a similar way. 4.1

**Definition 4.2** 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  $n \geq 0$ . 4.2

**Remark 4.3** We can avoid the use of choices if we allow uniqueness up to unique natural isomorphism in proposition 4.4. 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. 4.3

To understand properly the next proposition, recall from [ML98, V.3] that if  $\mathcal{C}$  has products (coproducts), then a 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  $S : C^{\{x\} \cup J} \longrightarrow C$  admitting initial algebras, a unique extension of the collection of objects  $\{\mathbf{x}_z\}_{z \in \text{Obj}(C^J)}$  to a functor  $\mathbf{x} : C^J \longrightarrow C$  such that  $\chi_z$  is a natural transformation from  $S(\mathbf{x}_z, z)$  to  $\mathbf{x}_z$ .

**Proposition 4.4** Let  $\mathcal{C}$  be an  $\Omega$ -model, let  $S \in \mathcal{S}(\mathcal{C})$  and  $Z \in \text{V}(S)$ . There exists at most one correspondence  $\|-\|_S^Z$ , defined on  $\mathcal{T}(\mathcal{C}, \mathbf{x}_S \cup Z)$ , with the following properties:

- For each  $s \in \mathcal{T}(\mathcal{C}, \mathbf{x}_S \cup Z)$ ,  $\|s\|_S^Z$  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  $s : I \longrightarrow \mathcal{T}(\mathcal{C}, \mathbf{x}_S \cup Z)$ , 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  $s : [n] \longrightarrow \mathcal{T}(\mathcal{C}, \mathbf{x}_S \cup Z)$ , then  $\|Hs\|_S^Z = H \circ \langle \|s_i\|_S^Z \rangle_{i \in [n]}$ .
- If the equation  $\mathbf{x} =_\mu q_{\mathbf{x}}$  belongs to  $S$ , then  $\|\mathbf{x}\|_S^Z$  is the chosen initial algebra of the functor

$$\|q_{\mathbf{x}}\|_{S_{\mathbf{x}}}^{(\mathbf{x}) \downarrow_S \cup Z} [x, \|y\|_S^Z / y]_{y <_{S\mathbf{x}}}$$

where  $[x, \|\mathbf{y}\|_S^Z/y]_{y <_S \mathbf{x}}$  is the functor

$$\begin{aligned} \text{id}_{C^{\{x\}}} \times \langle \|\mathbf{y}\|_S^Z, \text{id}_{C^Z} \rangle_{y <_S \mathbf{x}} \\ : \mathcal{C}^{\{x\} \cup Z} \longrightarrow \mathcal{C}^{(\mathbf{x})_{\downarrow S} \cup Z}. \end{aligned}$$

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

Observe that the relation  $(\mathbf{x})_{\downarrow S} \cup Z \in V(S_x)$  follows from lemma 2.7. In the following lemma,  $(\mathbf{x})_{\uparrow S} \subseteq X$  is the principal order filter generated by  $\mathbf{x}$ .

**Lemma 4.5** Let  $\mathcal{C}$  be an  $\Omega$ -model, let  $S \in \mathcal{S}(\mathcal{C})$  and let  $Z \in V(S)$ . If a correspondence  $\|-\|_S^Z$  with the above properties exists, then

$$\|s\|_S^Z = \|s\|_{S_x}^{(\mathbf{x})_{\downarrow S} \cup Z} [\|\mathbf{y}\|_S^Z/y]_{y \leq_S \mathbf{x}}$$

holds, for every  $s \in \mathcal{T}(\mathcal{C})$  such that  $\text{fv}(s) \subseteq \text{fv}(S) \cup (\mathbf{x})_{\downarrow S} \cup (\mathbf{x})_{\uparrow S}$ . In particular  $\|q_{\mathbf{x}}\|_S^Z$  is equal to

$$\|q_{\mathbf{x}}\|_{S_x}^{(\mathbf{x})_{\downarrow S} \cup Z} [\|\mathbf{x}\|_S^Z/x, \|\mathbf{y}\|_S^Z/y, ]_{y <_S \mathbf{x}}.$$

The only obstacle to the existence of such a correspondence is that the desired initial algebras and final coalgebras could not exist. The following proposition gives an inductive method to verify whether we can find such a correspondence.

**Proposition 4.6** Let  $\mathcal{C}$  be an  $\Omega$ -model, let  $S \in \mathcal{S}(\mathcal{C})$  and  $Z \in V(S)$ . Suppose that for each variable  $\mathbf{x} \in \mathbf{X}_{0,S}$  the following conditions hold:

- A correspondence  $\|-\|_{S_x}^{\{x\} \cup Z}$  with the above properties exists.
- If the equation  $\mathbf{x} =_\mu q_{\mathbf{x}}$  belongs to  $S$ , then an initial algebra of the functor  $\|q_{\mathbf{x}}\|_{S_x}^{\{x\} \cup Z}$  exists.
- If the equation  $\mathbf{x} =_\nu q_{\mathbf{x}}$  belongs to  $S$ , then a final coalgebra of the functor  $\|q_{\mathbf{x}}\|_{S_x}^{\{x\} \cup Z}$  exists.

Then also a correspondence  $\|-\|_S^Z$  with the above properties exists.

This justifies the following definition.

**Definition 4.7** An  $\Omega$ -model  $\mathcal{C}$  is said to be  $\mu$ -bicomplete if, for each directed system  $S \in \mathcal{S}(\mathcal{C})$  and  $Z \in V(S)$ , there exists exactly one correspondence  $\|-\|_S^Z$  with the above properties. 4.7

**Example 4.8** 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 [San00b]. 4.8

**Example 4.9** Let  $\lambda > \omega$  be a regular cardinal and consider the space of  $\lambda$ -accessible functors of the form  $S : \text{Set}^J \longrightarrow \text{Set}$  for some finite set  $J$ ; that is, those functors that preserve  $\lambda$ -directed colimits, cf. [AR94]. This space contains constant functors and projections, and it is closed under substitution, finite products and coproducts. Parameterized initial algebras and final coalgebras exist, cf. [AK79, Bar93] and the respective induced functors are again  $\lambda$ -accessible. Therefore, if for each  $H \in \Omega_n$   $\mathcal{I}(H) : \text{Set}^n \longrightarrow \text{Set}$  is a  $\lambda$ -accessible functor, then  $\langle \text{Set}, \mathcal{I} \rangle$  is a  $\mu$ -bicomplete  $\Omega$ -model. The same arguments is still true, if we substitute  $\text{Set}$  with an arbitrary locally  $\lambda$ -presentable category. 4.9

## 4.2 Semantics of circular proofs

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

**Definition 4.10** Let  $\Pi = \langle G_0, \lambda, \rho, \sigma \rangle$  be a circular proof over  $S, T \in \mathcal{S}(\mathcal{C})$ , let  $Z = \text{fv}_l(\Pi)$  and  $W = \text{fv}_r(\Pi)$ . The natural system of equations  $\|\Pi\|$  is the tuple

$$\langle G_0, \mathcal{C}_\Pi, \mathcal{C}_{S,T}, \|\rho(-)\|, \beta \rangle,$$

where

- The indexing set is  $G_0$ , the set of vertexes of  $\Pi$ . The set of bounded indexes is  $\mathcal{C}_\Pi$ , i.e. those  $g \in G_0$  such that  $\rho(g) \neq \mathbf{A}$ .
- If  $\lambda(g) = s \vdash t$ , recall that  $\|s\|_S^Z : \mathcal{C}^Z \longrightarrow \mathcal{C}$  and  $\|t\|_T^W : \mathcal{C}^W \longrightarrow \mathcal{C}$ . Therefore we let  $\mathcal{C}_{S,T}(g)$  be the functor

$$\mathcal{C}(\|s\|_S^Z, \|t\|_T^W) : (\mathcal{C}^Z)^{op} \times \mathcal{C}^W \longrightarrow \text{Set}.$$

- If  $\rho(g) \neq \mathbf{A}$ , then we let

$$\beta_g = \{ \sigma_{g,i} \mid i \in \text{Arity}(\rho(g)) \},$$



- $\|\rho(-)\|$  has the form

$$\|\rho(g)\|(\sigma_{g,i})_{i \in \text{Arity}(\rho(g))},$$

where

$$\begin{aligned} \|\mathbf{C}f\| &= f \\ \|\mathbf{C}H\|(h_i)_{i \in [n]} &= H(h_1, \dots, h_n) \\ \|\mathbf{L}\bigwedge_{I_i}\|(h) &= \text{pr}_i \cdot h \\ \|\mathbf{R}\bigwedge_I\|(h_i)_{i \in I} &= \langle h_i \rangle_{i \in I} \\ \|\mathbf{L}\bigvee_I\|(h_i)_{i \in I} &= \{h_i\}_{i \in I} \\ \|\mathbf{R}\bigvee_{I_i}\|(h) &= h \cdot \text{in}_i \\ \|\mathbf{L}\mu\mathbf{x}\|(h) &= \chi^{-1} \cdot h \\ \|\mathbf{R}\mathbf{x}_\mu\|(h) &= h \cdot \chi \\ \|\mathbf{L}\mathbf{y}_\nu\|(h) &= \varsigma \cdot h \\ \|\mathbf{R}\nu\mathbf{y}\|(h) &= h \cdot \varsigma^{-1} \end{aligned}$$

Above,  $\chi$  is the arrow part of the choice of initial algebras of the functor  $\|q_x\|_{S_x}^{(x)\downarrow_S \cup Z}$ , respectively  $\|q_x\|_{T_x}^{(x)\downarrow_T \cup W}$ , and  $\varsigma$  is the arrow part of the chosen final coalgebra of the similar functorial expression. 4.10

We shall represent the system  $\|\Pi\|$  with the more compact notation

$$\mathcal{C}_\Pi = \|\Pi\|(\mathcal{C}_\Pi, \mathcal{A}_\Pi).$$

**Theorem 4.11** The system  $\|\Pi\|$  admits a unique (natural) solution

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

*Proof.* The proof is by induction on  $\#\Pi$ . To begin with, observe that if

$$\text{card } \mathcal{C}_\Pi = 0,$$

then the result is obviously true, and that if

$$\text{card } \mathcal{C}_\Pi > 0,$$

then a proof is either strongly connected or not. Therefore, if it is possible to argue as follows.

Suppose  $\Pi$  is not strongly connected: let  $\overline{g_1, g_2} \in \mathcal{C}_\Pi$  and suppose that there is no path from  $g_1$  to  $g_2$ . Let  $\Pi_1 = \overline{\Pi, g_1}$  and  $\Pi_2 = \Pi^{\mathcal{C}_{\Pi_1}}$ . Hence, we decompose  $\|\Pi\|$  as

$$\left\{ \begin{array}{l} \mathcal{C}_{\Pi_1} = \|\Pi_1\|(\mathcal{C}_{\Pi_1}, \mathcal{A}_{\Pi_1}) \\ \mathcal{C}_{\Pi_2} = \|\Pi_2\|(\mathcal{C}_{\Pi_2}, \mathcal{C}_{\Pi_1}, \mathcal{A}_\Pi) \end{array} \right\}$$

Since  $g_1$  is a conclusion of  $\Pi_1$ ,  $g_1$  is not a conclusion of  $\Pi_2$ , and therefore  $\text{card } \mathcal{C}_{\Pi_2} < \text{card } \mathcal{C}_\Pi$ ; and since  $g_2 \in \mathcal{C}_\Pi \setminus \mathcal{C}_{\Pi_1}$  we have  $\mathcal{C}_{\Pi_1} < \text{card } \mathcal{C}_\Pi$ . By the induction hypothesis  $\|\Pi_1\|, \|\Pi_2\|$  admit a unique solution in the proper categories of functors from  $(\mathcal{C}^{\text{fv}_l(\Pi_j)})^{\text{op}} \times \mathcal{C}^{\text{fv}_r(\Pi_j)}$  for  $j = 1, 2$ . Since  $\text{fv}_i(\Pi_j) \subseteq \text{fv}_i(\Pi)$  for  $i \in \{l, r\}$  and  $j = 1, 2$ , then we conclude that the above circular proofs admit also a unique solution in the category of functors from  $(\mathcal{C}^{\text{fv}_l(\Pi)})^{\text{op}} \times \mathcal{C}^{\text{fv}_r(\Pi)}$ , by 1.3. We conclude that also  $\|\Pi\|$  admits a unique solution, using the Bekić lemma.

We shall therefore assume that  $\Pi$  is strongly connected. In this case we can find a cycle  $\gamma$  which visits every  $g \in \mathcal{C}_\Pi$ . Suppose that this cycle satisfies  $\text{L}(\gamma)$  – a dual argument can be carried out if only the statement  $\text{R}(\gamma)$  is satisfied – and let  $\mathbf{x} = \min \gamma_S$ .

We can also suppose that each assumption of  $\Pi$  is reachable from an element  $g \in \mathcal{C}_\Pi$ , hence from any element of  $\mathcal{C}_\Pi$ , since the unique solution of this system depends only on the proof  $\overline{\Pi, \mathcal{C}_\Pi}$ . It follows that if  $\lambda(g) = s_g \vdash t_g$ , then  $\text{fv}(s_g) \subseteq \text{fv}(S) \cup (\mathbf{x})_{\downarrow S} \cup (\mathbf{x})_{\uparrow S}$ .

Let

$$\mathcal{A} = \{g \in G_0 \mid \rho(g) = \text{L}\mu\mathbf{x}\},$$

and  $\Pi_2 = \Pi^{\mathcal{A}}$ . Recall that, if  $g \in \mathcal{A}$ , then there exists a unique vertex  $g'$  such that  $g \rightarrow g'$  is a transition of  $\mathcal{G}(\Pi)$ ; we shall denote  $Sg$  such vertex, and let  $t_g \in \mathcal{T}(\mathcal{C})$  be such that  $\lambda(g) = \mathbf{x} \vdash t_g$  and  $\lambda(Sg) = q_{\mathbf{x}} \vdash t_g$ . If we let  $\|\text{L}\mu\mathbf{x}\|$  be the system

$$\{g = \|\text{L}\mu\mathbf{x}\|(Sg)\}_{g \in \mathcal{A}},$$

we obtain a decomposition of  $\|\Pi\|$  as

$$\left\{ \begin{array}{l} \mathcal{A} = \|\text{L}\mu\mathbf{x}\|(\mathcal{C}_{\Pi_2}, \mathcal{A}, \mathcal{A}_\Pi) \\ \mathcal{C}_{\Pi_2} = \|\Pi_2\|(\mathcal{C}_{\Pi_2}, \mathcal{A}, \mathcal{A}_\Pi) \end{array} \right\}.$$

By construction, in  $\Pi_2$  there are no rules of the form  $\text{L}\mu\mathbf{x}$ , hence we can free all bounded variables  $y \leq_S \mathbf{x}$  from  $S$  and let the circular proof  $\Pi_2$

be over the directed systems  $S_x$  and  $T$ . Since  $\text{card } \mathbf{X}_{S_x} < \text{card } \mathbf{X}_S$ , by the induction hypothesis the system  $\|\Pi_2\|$  admits a unique natural solution  $\|\Pi_2\|_x^\dagger$  over  $S_x, T$ ; if we apply back the substitution functor  $[\|\mathbf{y}\|_S^Z/y]_{y \leq Sx}$ , we see that  $\|\Pi_2\|$  admits the unique solution  $\|\Pi_2\|_{[\|\mathbf{y}\|_S^Z/y]_{y \leq Sx}}^\dagger$  over  $S, T$ , by the remark 1.3 and lemma 4.5. Thus, we have reduced existence and uniqueness of a solution of  $\|\Pi\|$ , to existence and uniqueness of a solution of

$$\mathcal{A} = \|\mathbf{L}\mu\mathbf{x}\|(\mathcal{A}, \|\Pi_2\|_{[\|\mathbf{y}\|_S^Z/y]_{y \leq Sx}}^\dagger(\mathcal{A}, \mathcal{A}_\Pi), \mathcal{A}_\Pi),$$

as usual, from the Bekič lemma. This system has the form

$$\left\{ g = \chi_{\vec{z}}^{-1} \cdot \alpha_{\|\mathbf{x}\|_{S_x}^Z, \vec{z}, \vec{w}}^g(\mathcal{A}, \mathcal{A}_\Pi) \right\}_{g \in \mathcal{A}}$$

where for each  $g \in G$

$$\alpha^g = \begin{cases} \|\Pi_2\|_{[x, \|\mathbf{y}\|_S^Z/y]_{y < Sx}}^\dagger \cdot \text{pr}_{Sg}, & Sg \in \mathcal{C}_{\Pi_2} \\ \text{pr}_{Sg}, & \text{otherwise.} \end{cases}$$

Let

$$\begin{aligned} S(x, \vec{z}) &= \|q_x\|_{S_x}^{(x)_1 S \cup Z} [x, \|\mathbf{y}\|_S^Z/y]_{y < Sx} \\ &: \mathcal{C} \times \mathcal{C}^Z \longrightarrow \mathcal{C}, \\ T\vec{w} &= \prod_{g \in \mathcal{A}} \|t_g\|_T^W : \mathcal{C}^W \longrightarrow \mathcal{C}, \end{aligned}$$

and let  $Q(x, \vec{z}, \vec{w})$  be

$$\begin{aligned} &\prod_{a \in \mathcal{A}_\Pi} \mathcal{C}(\|s_a\|_{S_x}^{(x)_1 S \cup Z} [x, \|\mathbf{y}\|_S^Z/y]_{y < Sx}, \|t_a\|_T^W) \\ &: \mathcal{C}^{op} \times (\mathcal{C}^Z)^{op} \times \mathcal{C}^W \longrightarrow \text{Set}. \end{aligned}$$

Observe that for  $g \in \mathcal{A}$  the domain of  $\alpha^g$  is

$$\prod_{a \in \mathcal{A}} \mathcal{C}(x, \|t_a\|_T^W) \times Q(x, \vec{z}, \vec{w}),$$

since  $\|x\|_{S_x}^{(x)_1 S \cup Z} [x, \|\mathbf{y}\|_S^Z/y]_{y < Sx}$  is equal to the projection functor on  $x$ , where its codomain is  $\mathcal{C}(S(x, \vec{z}), \|t_g\|_T^W)$ . If we let  $\alpha_x = \langle \alpha_x^g \rangle_{g \in \mathcal{A}}$ , under natural isomorphism, we have

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

and therefore, the existence and uniqueness of a solution of the previous system follows from 3.1.  $\square$

## 5 Conclusions and future work

The calculus presented in this paper satisfies the cut elimination, in a sound way. This can be made precise as follows.

**Definition 5.1** A *pointed circular proof* is a pair  $\langle \Pi, g_0 \rangle$ , where  $\Pi = \langle G, \lambda, \rho, \sigma \rangle$  is a circular proof and  $g_0 \in G_0$ . We call  $g_0$  the conclusion of  $\langle \Pi, g_0 \rangle$  and say that this pair is a proof of  $s \vdash t$  if  $\lambda(g_0) = s \vdash t$ . 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. 5.1

A pair  $(s, S)$ , where  $S \in \mathcal{S}(\mathcal{C})$  and  $s \in \mathcal{T}(\mathcal{C})$ , is said to be closed if  $\text{fv}(S) = \emptyset$  and  $\text{fv}(s) \subseteq \mathbf{x}_S$ . 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  $\lambda(g_0) = s \vdash t$  and moreover that  $\mathcal{A}_\Pi = \emptyset$  and  $(s, S), (t, T)$  are closed pairs. If  $\text{fv}(S) = \emptyset$  and  $\text{fv}(s) \subseteq \mathbf{x}_S$ , then  $\|s\|_S^\emptyset : \mathcal{C}^\emptyset \longrightarrow \mathcal{C}$  can be identified with an object of  $\mathcal{C}$ . Hence, if  $\Pi_{g_0} : (s, S) \longrightarrow (t, T)$ , then

$$\|\Pi_{g_0}\| : \prod_{g \in \emptyset} \mathcal{C}_{S,T}(g) \longrightarrow \mathcal{C}(\|s\|_S^\emptyset, \|t\|_T^\emptyset)$$

can be identified with an arrow from  $\|s\|_S^\emptyset$  to  $\|t\|_T^\emptyset$ .

**Definition 5.2** For  $\Pi_{g_0} : (s, S) \longrightarrow (t, T)$ , we let  $\|\Pi_{g_0}\|$  be  $\|\Pi\|^\dagger \cdot \text{pr}_{g_0}$ . 5.2

**Proposition 5.3** 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 proofs  $\Pi_{g_0}; \Gamma_{h_0} : (s, S) \longrightarrow (u, U)$  with the property that  $\|\Pi_{g_0}; \Gamma_{h_0}\| = \|\Pi_{g_0}\|; \|\Gamma_{h_0}\|$ .

The construction is analogous to the usual cut elimination procedure and allows to consider circular proofs as algorithms. For example, let  $S_n$  be the system

$$\left\langle \left\{ \begin{array}{l} \mathbf{x}_n =_\mu \mathbf{x}_{n-1} \vee \mathbf{x}_n \\ \vdots \\ \mathbf{x}_1 =_\mu \top \vee \mathbf{x}_1 \end{array} \right\}, \{\mathbf{x}_n\} \right\rangle.$$

The interpretation  $\|\mathbf{x}_n\|_{S_n}^\emptyset$  in the category  $\mathbf{Set}$  is  $\mathbb{N}^n$ , the  $n$ -power of the set of natural numbers; moreover every tuple of natural numbers  $(k_n, \dots, k_1)$  can be coded as a pointed reachable circular proof from  $(\top, \emptyset)$  to  $(\mathbf{x}_n, S_n)$ . If  $\Pi_g$  is a circular proof from  $(\mathbf{x}_n, S_n)$  to  $(\mathbf{x}_m, S_m)$ , it is possible to apply the cut elimination procedure, to calculate the result of  $\|\Pi_g\|$ .

The proposed calculus is not complete enough to describe all the arrows in a free  $\mu$ -bicomplete category. Indeed 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 proof of example 2.21 (here  $s$  is the successor function).

**Proposition 5.4** There is no pointed reachable circular proof  $\Pi_g : (\mathbf{x}_1, S_1) \longrightarrow (\mathbf{x}_2, S_2)$  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 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.

## References

- [AAV00] P. Aczel, J. Adámek, and J. Velebil. Iteration monads. Preprint, available at <http://math.feld.cvut.cz/velebil/>, November 2000.
- [Acz88] P. Aczel. *Non-well-founded sets*. Stanford University Center for the Study of Language and Information, Stanford, CA, 1988.
- [AJ94] S. Abramsky and R. Jagadeesan. Games and full completeness for multiplicative linear logic. *J. Symbolic Logic*, 59(2):543–574, 1994.
- [AK79] J. Adámek and V. Koubek. Least fixed point of a functor. *J. Comput. System Sci.*, 19(2):163–178, 1979.
- [AR94] J. Adámek and J. Rosický. *Locally presentable and accessible categories*. Cambridge University Press, Cambridge, 1994.

- [Bar91] M. Barr. \*-autonomous categories and linear logic. *Math. Structures Comput. Sci.*, 1(2):159–178, 1991.
- [Bar93] M. Barr. Terminal coalgebras in well-founded set theory. *Theoret. Comput. Sci.*, 114(2):299–315, 1993.
- [BÉ93] S. L. Bloom and Z. Ésik. *Iteration theories*. Springer-Verlag, Berlin, 1993. The equational logic of iterative processes.
- [Bla72] A. Blass. Degrees of indeterminacy of games. *Fund. Math.*, 77(2):151–166, 1972.
- [Bla92] A. Blass. A game semantics for linear logic. *Ann. Pure Appl. Logic*, 56(1-3):183–220, 1992.
- [Coq94] T. Coquand. Infinite objects in type theory. In *Types for proofs and programs (Nijmegen, 1993)*, pages 62–78. Springer, Berlin, 1994.
- [CP90] T. Coquand and C. Paulin. Inductively defined types. In *COLOG-88 (Tallinn, 1988)*, pages 50–66. Springer, Berlin, 1990.
- [CS97] J.R.B. Cockett and R.A.G. Seely. Weakly distributive categories. *J. Pure Appl. Algebra*, 114(2):133–173, 1997.
- [CS01] J.R.B. Cockett and R.A.G. Seely. Finite sum-product logic. *Theory and Applications of Categories*, 8:63–99, 2001.
- [Fre91] P. Freyd. Algebraically complete categories. In *Category theory (Como, 1990)*, pages 95–104. Springer, Berlin, 1991.
- [GH82] Y. Gurevich and L. Harrington. Trees, automata, and games. In *Proc. 14th ACM Symp. on the Theory of Computation*, pages 60–65, 1982.
- [Gir87] J.-Y. Girard. Linear logic. *Theoret. Comput. Sci.*, 50(1):101, 1987.
- [Gir01] J.-Y. Girard. Locus solum. To appear in *Math. Struct. in Comp. Science*, january 2001.
- [GTL89] J.-Y. Girard, P. Taylor, and Y. Lafont. *Proofs and types*. Cambridge University Press, Cambridge, 1989.

- [HJ99] H. Hu and A. Joyal. Coherence completions of categories. *Theoret. Comput. Sci.*, 227(1-2):153–184, 1999. Linear logic, I (Tokyo, 1996).
- [Hoa85] C.A.R. Hoare. *Communicating sequential processes*. Prentice-Hall International, Englewood Cliffs, NJ, 1985. With a foreword by Edsger W. Dijkstra.
- [HS86] J.R. Hindley and J.P. Seldin. *Introduction to combinators and  $\lambda$ -calculus*. Cambridge University Press, Cambridge, 1986.
- [Joy95] A. Joyal. Free bicomplete categories. *C. R. Math. Rep. Acad. Sci. Canada*, 17(5):219–224, 1995.
- [Joy97] A. Joyal. Free lattices, communication, and money games. In *Logic and scientific methods*, pages 29–68, 1997. Proceedings of the 10th international congress of logic, methodology and philosophy of science, Florence, Italy, August 19–25, 1995.
- [Lam68] J. Lambek. A fixpoint theorem for complete categories. *Math. Z.*, 103:151–161, 1968.
- [LS88] J. Lambek and P. J. Scott. *Introduction to higher order categorical logic*. Cambridge University Press, Cambridge, 1988. Reprint of the 1986 original.
- [ML90] P. Martin-Löf. Mathematics of infinity. In *COLOG-88 (Tallinn, 1988)*, pages 146–197. Springer, Berlin, 1990.
- [ML98] S. Mac Lane. *Categories for the working mathematician*. Springer-Verlag, New York, second edition, 1998.
- [Mos00] L. S. Moss. Parametric corecursion. Preprint, available at <http://math.indiana.edu/home/moss/>, 2000.
- [NYY92] A. Nerode, A. Yakhnis, and V. Yakhnis. Concurrent programs as strategies in games. In *Logic from computer science (Berkeley, CA, 1989)*, pages 405–479. Springer, New York, 1992.
- [Rut00] J. J. M. M. Rutten. Universal coalgebra: a theory of systems. *Theoret. Comput. Sci.*, 249(1):3–80, 2000. Modern algebra and its applications (Nashville, TN, 1996).

- [San00a] L. Santocanale. The alternation hierarchy for the theory of  $\mu$ -lattices. Technical report, BRICS, November 2000. Submitted for a special issue of *Theory and Applications of Categories*, in occasion of CT2000.
- [San00b] L. Santocanale. Free  $\mu$ -lattices. Technical report, BRICS, November 2000. To appear in a special issue of the *Journal of Pure and Applied Algebra*, in occasion of Category Theory 99.
- [San00c] L. Santocanale. *Sur les  $\mu$ -treillis libres*. PhD thesis, Université du Québec à Montréal, July 2000.
- [Sei96] H. Seidl. Fast and simple nested fixpoints. *Inform. Process. Lett.*, 59(6):303–308, 1996.
- [Wal00] 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).
- [Win93] G. Winskel. *The formal semantics of programming languages*. MIT Press, Cambridge, MA, 1993. An introduction.
- [Zie98] W. Zielonka. Infinite games on finitely coloured graphs with applications to automata on infinite trees. *Theoret. Comput. Sci.*, 200(1-2):135–183, 1998.



## Recent BRICS Report Series Publications

- RS-01-15 Luigi Santocanale. *A Calculus of Circular Proofs and its Categorical Semantics*. May 2001. 30 pp.
- RS-01-14 Ulrich Kohlenbach and Paulo B. Oliva. *Effective Bounds on Strong Unicity in  $L_1$ -Approximation*. May 2001.
- RS-01-13 Federico Crazzolaro and Glynn Winskel. *Events in Security Protocols*. April 2001.
- RS-01-12 Torben Amtoft, Charles Consel, Olivier Danvy, and Karoline Malmkjær. *The Abstraction and Instantiation of String-Matching Programs*. April 2001.
- RS-01-11 Alexandre David and M. Oliver Möller. *From Hierarchical Timed Automata to UPPAAL*. March 2001.
- RS-01-10 Daniel Fridlender and Mia Indrika. *Do we Need Dependent Types?* March 2001. 6 pp. Appears in *Journal of Functional Programming*, 10(4):409–415, 2000. Superseeds BRICS Report RS-98-38.
- RS-01-9 Claus Brabrand, Anders Møller, and Michael I. Schwartzbach. *Static Validation of Dynamically Generated HTML*. February 2001. 18 pp.
- RS-01-8 Ulrik Frendrup and Jesper Nyholm Jensen. *Checking for Open Bisimilarity in the  $\pi$ -Calculus*. February 2001. 61 pp.
- RS-01-7 Gregory Gutin, Khee Meng Koh, Eng Guan Tay, and Anders Yeo. *On the Number of Quasi-Kernels in Digraphs*. January 2001. 11 pp.
- RS-01-6 Gregory Gutin, Anders Yeo, and Alexey Zverovich. *Traveling Salesman Should not be Greedy: Domination Analysis of Greedy-Type Heuristics for the TSP*. January 2001. 7 pp.
- RS-01-5 Thomas S. Hune, Judi Romijn, Mariëlle Stoelinga, and Frits W. Vaandrager. *Linear Parametric Model Checking of Timed Automata*. January 2001. 44 pp. To appear in Margaria and Yi, editors, *Tools and Algorithms for The Construction and Analysis of Systems: 7th International Conference, TACAS '01 Proceedings*, LNCS, 2001.