The Structure of First-Order Causality

Samuel Mimram

The Structure of First-Order Causality

Samuel Mimram
CNRS – Université Paris Diderot
samuel.mimram@pps.jussieu.fr

Abstract

Game semantics describe the interactive behavior of proofs by interpreting formulas as games on which proofs induce strategies. Such a semantics is introduced here for capturing dependencies induced by quantifications in first-order propositional logic. One of the main difficulties that has to be faced during the elaboration of this kind of semantics is to characterize definable strategies, that is strategies which actually behave like a proof. This is usually done by restricting the model to strategies satisfying subtle combinatorial conditions, whose preservation under composition is often difficult to show. Here, we present an original methodology to achieve this task, which requires to combine advanced tools from game semantics, rewriting theory and categorical algebra. We introduce a diagrammatic presentation of the monoidal category of definable strategies of our model, by the means of generators and relations: those strategies can be generated from a finite set of atomic strategies and the equality between strategies admits a finite axiomatization, this equational structure corresponding to a polarized variation of the notion of bialgebra. This work thus bridges algebra and denotational semantics in order to reveal the structure of dependencies induced by first-order quantifiers, and lays the foundations for a mechanized analysis of causality in programming languages.

Denotational semantics were introduced to provide useful abstract invariants of proofs and programs modulo cut-elimination or reduction. In particular, game semantics, introduced in the nineties, have been very successful in capturing precisely the interactive behavior of programs. In these semantics, every type is interpreted as a *game* (that is as a set of *moves* that can be played during the game) together with the rules of the game (formalized by a partial order on the moves of the game indicating the dependencies between them). Every move is to be played by one of the two players, called *Proponent* and *Opponent*, who should be thought respectively as the program and its environment. A program is characterized by the sequences of moves that it can exchange with its environment during an execution and thus defines a *strategy* reflecting the interactive behavior of the program inside the game specified by the type of the program.

The notion of *pointer game*, introduced by Hyland and Ong [3], gave one of the first fully abstract models of PCF (a simply-typed λ-calculus extended with recursion, conditional branching and arithmetical constants). It has revealed that PCF programs generate strategies with partial memory, called *innocent* because they react to Opponent moves according to their own *view* of the play. Innocence is in this setting the main ingredient to characterize *definable* strategies, that is strategies which are the interpretation of a PCF term, because it describes the behavior of the purely functional core of the language (i.e. λ-terms), which also corresponds to proofs in propositional logic. This seminal work has lead to an extremely successful series of semantics: by relaxing in various ways the innocence constraint on strategies, it became suddenly possible to generalize this characterization to PCF programs extended with imperative features such as references, control, non-determinism, etc.

Unfortunately, these constraints are quite specific to game semantics and remain difficult to link with other areas of computer science or algebra. They are moreover very subtle and combinatorial and thus sometimes difficult to work with. This work is an attempt to find new ways to describe the behavior of proofs.

Generating instead of restricting. In this paper, we introduce a game semantics capturing dependencies induced by quantifiers in first-order propositional logic, forming a strict monoidal category called $\mathbf{Games}$. Instead of characterizing definable strategies of the model by restricting to strategies satisfying particular conditions, we show here that we can equivalently use here a kind of converse approach. We show how to *generate* definable strategies by giving a *presentation* of those strategies: a finite set of definable strategies can be used to generate all definable strategies by composition and tensoring, and the equality between strategies obtained this way can be finitely axiomatized.

What we mean precisely by a presentation is a generalization of the usual notion of presentation of a monoid to monoidal categories. For example, consider the additive monoid $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$. It admits the presentation $\langle\, p, q \mid qp = pq \,\rangle$, where p and q are two *generators* and $qp = pq$ is a relation between two elements of the free monoid M on $\{p, q\}$. This means that $\mathbb{N}^2$ is isomorphic to the free monoid M on the two generators, quotiented by the smallest congruence $\equiv$ (wrt multiplication) such that $qp \equiv pq$. More generally, a (strict) monoidal category $\mathcal{C}$ (such as $\mathbf{Games}$) can be presented by a *polygraph*, consisting of typed generators in dimension 1 and 2 and relations in dimension 3, such that the category $\mathcal{C}$ is monoidally equivalent to the free monoidal category on the generators, quotiented by the congruence generated by the relations.

Reasoning locally. The usefulness of our construction is both theoretic and practical. It reveals that the essential algebraic structure of dependencies induced by quantifiers is a polarized variation of the well-known structure of bialgebra, thus bridging game semantics and algebra. It also proves very useful from a technical point of view: this presentation allows us to reason locally about strategies. In particular, it enables us to deduce a posteriori that the strategies of the category $\mathbf{Games}$ are definable (one only needs to check that generators are definable) and that these strategies actually compose, which is not trivial. Finally, the presentation gives a finite description of the category, that we can hope to manipulate with a computer, paving the way for a series of new tools to automate the study of semantics of programming languages.

A game semantics capturing first-order causality. Game semantics has revealed that proofs in logic describe particular strategies to explore formulas. Namely, a formula A is a syntactic tree expressing in which order its connectives must be introduced in cut-free proofs of A. In this sense, it can be seen as the rules of a game whose moves correspond to connectives. For instance, consider a formula of the form

$$\forall x.P \quad \Rightarrow \quad \forall y.\exists z.Q \tag{1}$$

where P and Q are propositional formulas which may contain free variables. When searching for a proof of (1), the $\forall y$ quantification must be introduced before the $\exists z$ quantification, and the $\forall x$ quantification can be introduced independently. Here, introducing an existential quantification should be thought as playing a Proponent move (the strategy gives a witness for which the formula holds) and introducing an universal quantification as playing an Opponent move (the strategy receives a term from its environment, for which it has to show that the formula holds). So, the game associated to the formula (1) will be the partial order on the first-order quantifications appearing in the formula, depicted below (to be read from the top to the bottom):

$$\begin{array}{cc} \forall x & \forall y \\ & | \\ & \exists z \end{array}$$

To understand exactly which dependencies induced by proofs are interesting, we shall examine proofs of the formula $\exists x.P \Rightarrow \exists y.Q$, which induces the following game:

$$\exists x \qquad \exists y$$

By permuting the order of introduction rules, the proof of this formula on the left-hand side of

$$\dfrac{\dfrac{\dfrac{\pi}{P \vdash Q[t/y]}}{P \vdash \exists y.Q}}{\exists x.P \vdash \exists y.Q} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\pi}{P \vdash Q[t/y]}}{\exists x.P \vdash Q[t/y]}}{\exists x.P \vdash \exists y.Q}$$

might be reorganized as the proof on the right-hand side if and only if the term t used in the introduction rule of the $\exists y$ connective does not have x as free variable. If the variable x is free in t then the rule introducing $\exists y$ can only be used after the rule introducing the $\exists x$ connective. In this case, it will be reflected by a causal dependency in the strategy corresponding to the proof, depicted by an oriented wire:

$$\exists x \longrightarrow \exists y$$

and we sometimes say that the move $\exists x$ *justifies* the move $\exists y$. A simple further study of permutability of introduction rules of first-order quantifiers shows that this is the only kind of relevant dependencies. These permutations of rules where the motivation for the introduction of non-alternating asynchronous game semantics [12]. However, we focus here on causality and define strategies by the dependencies they induce on moves.

We thus build a strict monoidal category whose objects are games and whose morphisms are strategies, in which we can interpret formulas and proofs in first-order propositional logic, and write $\mathbf{Games}$ for the subcategory of definable strategies. This paper is devoted to the construction of a presentation for this category. We introduce formally the notion of presentation of a monoidal category in Section 1 and recall some useful classical algebraic structures in Section 2. Then, we give a presentation of the category of relations in Section 3 and extend this presentation to the category $\mathbf{Games}$, that we define formally in Section 4.

1 Presentations of monoidal categories

For the lack of space, we don't recall here the basic definitions in category theory, such as the definition of monoidal categories. The interested reader can find a presentation of these concepts in MacLane's reference book [11].

Monoidal theories. A *monoidal theory* $\mathbb{T}$ is a strict monoidal category whose objects are the natural integers, such that the tensor product on objects is the addition of integers. By an integer $\underline{n}$, we mean here the finite ordinal $\underline{n} = \{0, 1, \ldots, n-1\}$ and the addition is given by $\underline{m} + \underline{n} = \underline{m+n}$. An *algebra* F of a monoidal theory $\mathbb{T}$

in a strict monoidal category $\mathcal{C}$ is a strict monoidal functor from $\mathbb{T}$ to $\mathcal{C}$; we write $\mathbf{Alg}_{\mathbb{T}}^{\mathcal{C}}$ for the category of algebras from $\mathbb{T}$ to $\mathcal{C}$ and monoidal natural transformations between them. Monoidal theories are sometimes called PRO, this terminology was introduced by Mac Lane in [10] as an abbreviation for "category with products". They generalize equational theories (or Lawere theories [9]) in the sense that operations are typed and can moreover have multiple outputs as well as multiple inputs, and are not necessarily cartesian but only monoidal.

Presentations of monoidal categories. We now recall the notion of *presentation* of a monoidal category by the means of typed 1- and 2-dimensional generators and relations.

Suppose that we are given a set E_1 whose elements are called *atomic types*. We write E_1^* for the free monoid on the set E_1 and $i_1 : E_1 \to E_1^*$ for the corresponding injection; the product of this monoid is written $\otimes$. The elements of E_1^* are called *types*. Suppose moreover that we are given a set E_2, whose elements are called *generators*, together with two functions $s_1, t_1 : E_2 \to E_1^*$, which to every generator associate a type called respectively its *source* and *target*. We call a *signature* such a 4-uple (E_1, s_1, t_1, E_2):

$$\begin{tikzcd} E_1 \arrow[r, "i_1"] & E_1^* & E_2 \arrow[l, shift right, "s_1"'] \arrow[l, shift left, "t_1"] \end{tikzcd}$$

Every such signature (E_1, s_1, t_1, E_2) generates a free strict monoidal category $\mathcal{E}$, whose objects are the elements of E_1^* and whose morphisms are formal composite and tensor products of elements of E_2, quotiented by suitable laws imposing associativity of composition and tensor and compatibility of composition with tensor, see [2]. If we write E_2^* for the morphisms of this category and $i_2 : E_2 \to E_2^*$ for the injection of the generators into this category, we get a diagram

$$\begin{tikzcd} E_1 \arrow[d, "i_1"'] & E_2 \arrow[dl, shift right, "s_1"'] \arrow[dl, shift left, "t_1"] \arrow[d, "i_2"] \\ E_1^* & E_2^* \arrow[l, shift right, "\overline{s_1}"'] \arrow[l, shift left, "\overline{t_1}"] \end{tikzcd}$$

in $\mathbf{Set}$ together with a structure of monoidal category $\mathcal{E}$ on the graph

$$\begin{tikzcd} E_1^* & E_2^* \arrow[l, shift right, "\overline{s_1}"'] \arrow[l, shift left, "\overline{t_1}"] \end{tikzcd}$$

where the morphisms $\overline{s_1}, \overline{t_1} : E_2^* \to E_1^*$ are the morphisms (unique by universality of E_2^*) such that $s_1 = \overline{s_1} \circ i_2$ and $t_1 = \overline{t_1} \circ i_2$. The *size* $|f|$ of a morphism $f : A \to B$ in E_2^* is defined inductively by

$$\begin{array}{ll} |\mathrm{id}| = 0 & |f| = 1 \quad \text{if } f \text{ is a generator} \\ |f_1 \otimes f_2| = |f_1| + |f_2| & |f_2 \circ f_1| = |f_1| + |f_2| \end{array}$$

In particular, a morphism is of size 0 if and only if it is an identity.

Our constructions are a particular case of Burroni's polygraphs [2] (and Street's 2-computads [15]) who made precise the sense in which the generated monoidal category is free on the signature. In particular, the following notion of equational theory is a specialization of the definition of a 3-polygraph to the case where there is only one 0-cell.

Definition 1. *A **monoidal equational theory** is a 7-uple*

$$\mathfrak{E} = (E_1, s_1, t_1, E_2, s_2, t_2, E_3)$$

where (E_1, s_1, t_1, E_2) is a signature together with a set E_3 of relations *and two morphisms $s_2, t_2 : E_3 \to E_2^*$, as pictured in the diagram*

$$\begin{tikzcd} E_1 \arrow[d, "i_1"'] & E_2 \arrow[dl, shift right, "s_1"'] \arrow[dl, shift left, "t_1"] \arrow[d, "i_2"] & E_3 \arrow[dl, shift right, "s_2"'] \arrow[dl, shift left, "t_2"] \\ E_1^* & E_2^* \arrow[l, shift right, "\overline{s_1}"'] \arrow[l, shift left, "\overline{t_1}"] & \end{tikzcd}$$

such that $\overline{s_1} \circ s_2 = \overline{s_1} \circ t_2$ and $\overline{t_1} \circ s_2 = \overline{t_1} \circ t_2$.

Every equational theory defines a monoidal category $\mathbb{E} = \mathcal{E}/\equiv$ obtained from the monoidal category $\mathcal{E}$ generated by the signature (E_1, s_1, t_1, E_2) by quotienting the morphisms by the congruence $\equiv$ generated by the relations of the equational theory $\mathfrak{E}$: it is the smallest congruence (wrt both composition and tensoring) such that $s_2(e) \equiv t_2(e)$ for every element e of E_3. We say that a monoidal equational theory $\mathfrak{E}$ is a *presentation* of a strict monoidal category $\mathcal{M}$ when $\mathcal{M}$ is monoidally equivalent to the category $\mathbb{E}$ generated by $\mathfrak{E}$.

We sometimes informally say that an equational theory has a *generator* $f : A \to B$ to mean that f is an element of E_2 such that $s_1(f) = A$ and $t_1(f) = B$. We also say that the equational theory has a *relation* $f = g$ to mean that there exists an element e of E_3 such that $s_2(e) = f$ and $t_2(e) = g$.

It is remarkable that every monoidal equational theory $(E_1, s_1, t_1, E_2, s_2, t_2, E_3)$ where the set E_1 is reduced to only one object $\{1\}$ generates a monoidal category which is a monoidal theory ($\mathbb{N}$ is the free monoid on one object), thus giving a notion of presentation of those categories.

Presented categories as models. Suppose that a strict monoidal category $\mathcal{M}$ is presented by an equational theory $\mathfrak{E}$, generating a category $\mathbb{E} = \mathcal{E}/\equiv$. The proof that $\mathfrak{E}$ presents $\mathcal{M}$ can generally be decomposed in two parts:

1. *$\mathcal{M}$ is a model of the equational theory* $\mathfrak{E}$: there exists a functor $\widetilde{-}$ from the category $\mathbb{E}$ to $\mathcal{M}$. This amounts to checking that there exists a functor $F : \mathcal{E} \to \mathcal{M}$ such that for all morphisms $f, g : A \to B$ in $\mathcal{E}$, $f \equiv g$ implies $Ff = Fg$.

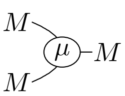
2. *$\mathcal{M}$ is a fully-complete model of the equational theory* $\mathfrak{E}$: the functor $\widetilde{-}$ is full and faithful.

We say that a morphism $f : A \to B$ of $\mathbb{E}$ *represents* the morphism $\widetilde{f} : \widetilde{A} \to \widetilde{B}$ of $\mathcal{M}$.

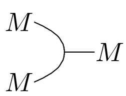
Usually, the first point is a straightforward verification. Proving that the functor $\widetilde{-}$ is full and faithful often requires more work. In this paper, we use the methodology introduced by Burroni [2] and refined by Lafont [8]. We first define *canonical forms* which are canonical representatives of the equivalence classes of morphisms of $\mathcal{E}$ under the congruence $\equiv$ generated by the relations of $\mathfrak{E}$. Proving that every morphism is equal to a canonical form can be done by induction on the size of the morphisms. Then, we show that the functor $\widetilde{-}$ is full and faithful by showing that the canonical forms are in bijection with the morphisms of $\mathcal{M}$.

It should be noted that this is not the only technique to prove that an equational theory presents a monoidal category. In particular, Joyal and Street have used topological methods [5] by giving a geometrical construction of the category generated by a signature, in which morphisms are equivalence classes under continuous deformation of progressive plane diagrams (we give some more details about those diagrams, also called string diagrams, later on). Their work is for example extended by Baez and Langford in [1] to give a presentation of the 2-category of 2-tangles in 4 dimensions. The other general methodology the author is aware of, is given by Lack in [6], by constructing elaborate monoidal theories from simpler monoidal theories. Namely, a monoidal theory can be seen as a monad in a particular span bicategory, and monoidal theories can therefore be "composed" given a distributive law between their corresponding monads. We chose not to use those methods because, even though they can be very helpful to build intuitions, they are difficult to formalize and even more to mechanize.

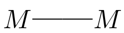
String diagrams. *String diagrams* provide a convenient way to represent and manipulate the morphisms in the category generated by a presentation. Given an object M in a strict monoidal category $\mathcal{C}$, a morphism $\mu : M \otimes M \to M$ can be drawn graphically as a device with two inputs and one output of type M as follows:



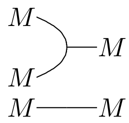
or simply as



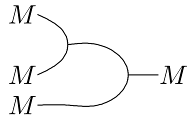
when it is clear from the context which morphism of type $M \otimes M \to M$ we are picturing (we sometimes even omit the source and target of the morphisms). Similarly, the identity $\mathrm{id}_M : M \to M$ (which we sometimes simply write M) can be pictured as a wire



The tensor $f \otimes g$ of two morphisms $f : A \to B$ and $g : C \to D$ is obtained by putting the diagram corresponding to f above the diagram corresponding to g. So, for instance, the morphism $\mu \otimes M$ can be drawn diagrammatically as



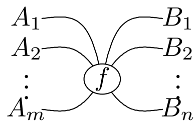
Finally, the composite $g \circ f : A \to C$ of two morphisms $f : A \to B$ and $g : B \to C$ can be drawn diagrammatically by putting the diagram corresponding to g at the right of the diagram corresponding to f and "linking the wires". The diagram corresponding to the morphism $\mu \circ (\mu \otimes M)$ is thus



Suppose that (E_1, s_1, t_1, E_2) is a signature. Every element f of E_2 such that

$$s_1(f) = A_1 \otimes \cdots \otimes A_m \quad \text{and} \quad t_1(f) = B_1 \otimes \cdots \otimes B_n$$

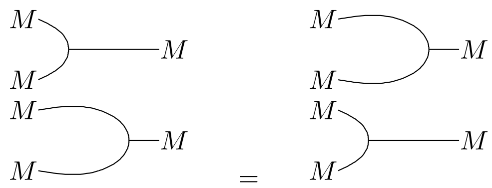
where the A_i and B_i are elements of E_1, can be similarly represented by a diagram



Bigger diagrams can be constructed from these diagrams by composing and tensoring them, as explained above. Joyal and Street have shown in details in [5] that the category of those diagrams, modulo continuous deformations, is precisely the free category generated by a signature (which they call a "tensor scheme"). For example, the equality

$$(M \otimes \mu) \circ (\mu \otimes M \otimes M) \quad = \quad (\mu \otimes M) \circ (M \otimes M \otimes \mu)$$

in the category $\mathcal{C}$ of the above example, which holds because of the axioms satisfied in any monoidal category, can be shown by continuously deforming the diagram on the left-hand side below into the diagram on the right-hand side:



All the equalities satisfied in any monoidal category generated by a signature have a similar geometrical interpretation. And conversely, any deformation of diagrams corresponds to an equality of morphisms in monoidal categories.

2 Algebraic structures

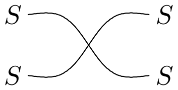
In this section, we recall the categorical formulation of some well-known algebraic structures. We give those definitions in the setting of a *strict* monoidal category which is *not* required to be symmetric. We suppose that $(\mathcal{C}, \otimes, I)$

is a strict monoidal category, fixed throughout the section. For the lack of space, we will only give graphical representations of axioms, but they can always be reformulated as commutative diagrams.

Symmetric objects. A *symmetric object* of $\mathcal{C}$ is an object S together with a morphism

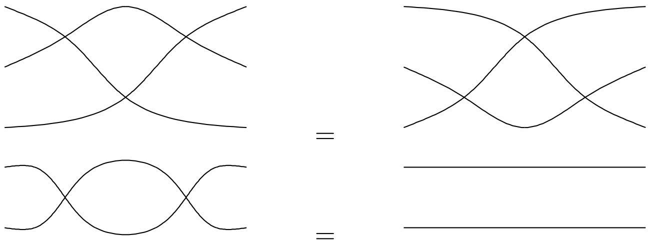
$$\gamma : S \otimes S \to S \otimes S$$

called *symmetry* and pictured as



(2)

such that the two equalities

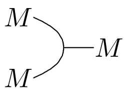


hold (the first equation is sometimes called the Yang-Baxter equation for braids). In particular, in a symmetric monoidal category, every object is canonically equipped with a structure of symmetric object.

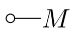
Monoids. A *monoid* (M, μ, η) in $\mathcal{C}$ is an object M together with two morphisms

$$\mu : M \otimes M \to M \quad \text{and} \quad \eta : I \to M$$

called respectively *multiplication* and *unit* and pictured respectively as

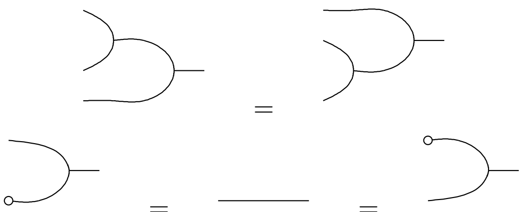


and



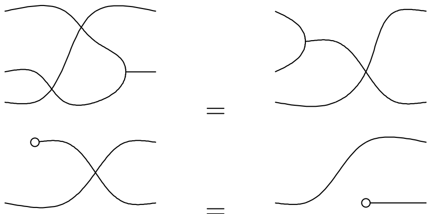
(3)

satisfying the three equations



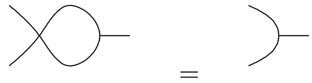
(4)

A *symmetric monoid* is a monoid which admits a symmetry $\gamma : M \otimes M \to M \otimes M$ which is compatible with the operations of the monoid in the sense that the equalities



(5)

are satisfied, as well as the equations obtained by turning the diagrams upside-down. A *commutative monoid* is a symmetric monoid such that the equality

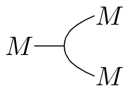


is satisfied. In particular, a commutative monoid in a symmetric monoidal category is a commutative monoid whose symmetry corresponds to the symmetry of the category: $\gamma = \gamma_{M,M}$. In this case, the equations (5) can always be deduced from the naturality of the symmetry of the monoidal category.

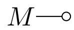
A *comonoid* (M, δ, ε) in $\mathcal{C}$ is an object M together with two morphisms

$$\delta : M \to M \otimes M \quad \text{and} \quad \varepsilon : M \to I$$

respectively drawn as



and



(6)

satisfying dual coherence diagrams. Similarly, the notions symmetric comonoid and cocommutative comonoid can be defined by duality.

The definition of a monoid can be reformulated internally, in the language of equational theories:

Definition 2. *The* equational theory of monoids $\mathfrak{M}$ *has one object* 1 *and two generators* $\mu : 2 \to 1$ *and* $\eta : 0 \to 1$ *subject to the three relations*

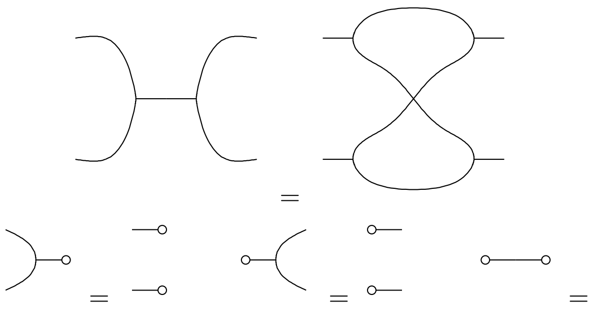
$$\begin{array}{rcccl} \mu \circ (\mu \otimes \mathrm{id}_1) & = & \mu \circ (\mathrm{id}_1 \otimes \mu) & & \\ \mu \circ (\eta \otimes \mathrm{id}_1) & = & \mathrm{id}_1 & = & \mu \circ (\mathrm{id}_1 \otimes \eta) \end{array} \tag{7}$$

The equations (7) are the algebraic formulation of the equations (4). If we write $\mathbb{M}$ for the monoidal category generated by the equational theory $\mathfrak{M}$, the algebras of $\mathbb{M}$ in a strict monoidal category $\mathcal{C}$ are precisely its monoids: the category $\mathbf{Alg}_{\mathbb{M}}^{\mathcal{C}}$ of algebras of the monoidal theory $\mathbb{M}$ in $\mathcal{C}$ is monoidally equivalent to the category of monoids in $\mathcal{C}$. Similarly, all the algebraic structures introduced in this section can be defined using algebraic theories.

Bialgebras. A *bialgebra* $(B, \mu, \eta, \delta, \varepsilon, \gamma)$ in $\mathcal{C}$ is an object B together with four morphisms

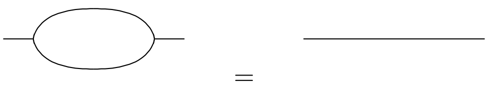
$$\begin{array}{ll} \mu : B \otimes B \to B & \eta : I \to B \\ \delta : B \to B \otimes B & \varepsilon : B \to I \end{array} \quad \text{and } \gamma : B \otimes B \to B \otimes B$$

such that $\gamma : B \otimes B \to B \otimes B$ is a symmetry for B, (B, μ, η, γ) is a symmetric monoid and $(B, \delta, \varepsilon, \gamma)$ is a symmetric comonoid. The morphism γ is thus pictured as in (2), μ and η as in (3), and δ and ε as in (6). Those two structures should be coherent, in the sense that the four equalities



should be satisfied.

A bialgebra is *commutative* (resp. *cocommutative*) when the induced symmetric monoid (B, μ, η, γ) (resp. symmetric comonoid $(B, \delta, \varepsilon, \gamma)$) is commutative (resp. cocommutative), and *bicommutative* when it is both commutative and cocommutative. A bialgebra is *qualitative* when the following equality holds:

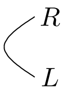


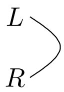
We write $\mathfrak{B}$ for the equational theory of bicommutative bialgebras and $\mathfrak{R}$ for the equational theory of qualitative bicommutative bialgebras.

Dual objects. An object L of $\mathcal{C}$ is said to be *left dual* to an object R when there exists two morphisms

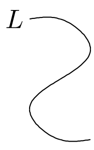
$$\eta : I \to R \otimes L \quad \text{and} \quad \varepsilon : L \otimes R \to I$$

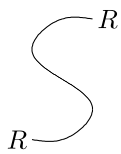
called respectively the *unit* and the *counit* of the duality and respectively pictured as



and


such that the two morphisms



and


are equal to the identities on L and R respectively. We write $\mathfrak{D}$ for the equational theory associated to dual objects.

3 Presenting the category of relations

We now introduce a presentation of the category $\mathbf{Rel}$ of finite ordinals and relations, by refining presentations of simpler categories. This result is mentioned in Examples 6 and 7 of [4] and is proved in three different ways in [7], [14] and [6]. The methodology adopted here to build this presentation has the advantage of being simple to check (although very repetitive) and can be extended to give the presentation of the category of games and strategies described in Section 4. For the lack of space, most of the proofs have been omitted or only sketched; detailed proofs can be found in the author's PhD thesis [13].

The simplicial category. The simplicial category Δ is the monoidal theory whose morphisms $f : \underline{m} \to \underline{n}$ are the monotone functions from $\underline{m}$ to $\underline{n}$. It has been known for a long time that this category is closely related to the notion of monoid, see [11] or [8] for example. This result can be formulated as follows:

Property 3. *The monoidal category Δ is presented by the equational theory of monoids $\mathfrak{M}$.*

In this sense, the simplicial category Δ impersonates the notion of monoid. We extend here this result to more complex categories.

Multirelations. A *multirelation* R between two finite sets A and B is a function $R : A \times B \to \mathbb{N}$. It can be equivalently be seen as a multiset whose elements are in $A \times B$ or as a matrix over $\mathbb{N}$ (or as a span in the category of finite sets). If $R_1 : A \to B$ and $R_2 : B \to C$ are two multirelations, their composition is defined by

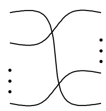
$$R_2 \circ R_1(a, c) \quad = \quad \sum_{b \in B} R_1(a, b) \times R_2(b, c).$$

(this corresponds to the usual composition of matrices if we see R_1 and R_2 as matrices over $\mathbb{N}$). The cardinal $|R|$ of a multirelation $R : A \to B$ is the sum of its coefficients. We write $\mathbf{MRel}$ for the monoidal theory of multirelations: its objects are finite ordinals and morphisms are multirelations between them. It is a strict symmetric monoidal category with the tensor product $\otimes$ defined on objects and morphisms by disjoint union, and thus a monoidal theory. In this category, the object $\underline{1}$ can be equipped with the obvious bicommutative bialgebra structure $(1, R^\mu, R^\eta, R^\delta, R^\varepsilon)$. For example, $R^\mu : \underline{2} \to \underline{1}$ is the multirelation defined by $R^\mu(i, 0) = 1$ for $i = 0$ or $i = 1$. We now show that the category of multirelations is presented by the equational theory $\mathfrak{B}$ of bicommutative bialgebras. We write $\mathcal{B}/\!\equiv$ for the monoidal category generated by $\mathfrak{B}$.

For every morphism $\phi : m \to n$ in $\mathcal{B}$, where $m > 0$, we define a morphism $S\phi : m + 1 \to n$ by

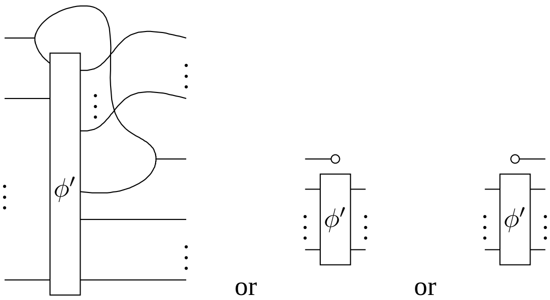
$$S\phi \quad = \quad \phi \circ (\gamma \otimes \mathrm{id}_{m-1}) \tag{8}$$

The *stairs* morphisms are defined inductively as either id_1 or $S\phi'$ where ϕ' is a stair, and are represented graphically as



The *length* of a stairs is defined as 0 if it is an identity, or as the length of the stairs ϕ' plus one if it is of the form $S\phi'$.

Morphisms ϕ which are *precanonical forms* are defined inductively: ϕ is either empty or



where ϕ' is a precanonical form. In this case, we write respectively ϕ as Z (the identity morphism $\mathrm{id}_{\underline{0}}$), as $W_i\phi'$ (where i is the length of the stairs in the morphism), as $E\phi'$ or as $H\phi'$. Precanonical forms ϕ are thus the well formed morphisms (where compositions respect types) generated by the following grammar:

$$\phi \quad ::= \quad Z \quad | \quad W_i\phi \quad | \quad E\phi \quad | \quad H\phi \tag{9}$$

It is easy to see that every non-identity morphism ϕ of a category generated by a monoidal equational theory (such as $\mathfrak{B}$) can be written as $\phi = \phi' \circ (\underline{m} \otimes \pi \otimes \underline{n})$, where π is a generator, thus allowing us to reason inductively about morphisms, by case analysis on the integer $\underline{m}$ and on the generator π. Using this technique, we can prove that

Lemma 4. *Every morphism ϕ of $\mathcal{B}$ is equivalent (wrt the relation $\equiv$) to a precanonical form.*

The *canonical forms* are precanonical forms which are normal wrt the following rewriting system:

$$\begin{array}{rcll} HW_i & \Longrightarrow & W_{i+1}H & \\ HE & \Longrightarrow & EH & \\ W_iW_j & \Longrightarrow & W_jW_i & \text{when } i < j \end{array} \tag{10}$$

when considered as words generated by the grammar (9). This rewriting system can easily be shown to be terminating and confluent, and moreover two morphisms ϕ and ψ such that $\phi \Longrightarrow \psi$ can be shown to be equivalent. By Lemma 4, every morphism of $\mathcal{B}$ is therefore equivalent to an unique canonical form.

Lemma 5. *Every multirelation $R : m \to n$ is represented by an unique canonical form.*

Proof. We prove by induction on m and on the cardinal $|R|$ of R that R is represented by a precanonical form.

1. If $m = 0$ then R is represented by the canonical form $H \ldots HZ$ (with n occurrences of H).

2. If $m > 0$ and for every $j < n$, $R(0, j) = 0$ then R is of the form $R = R^{\varepsilon} \otimes R'$ and R is necessarily represented by a precanonical form $E\phi'$ where ϕ' is a precanonical form representing $R' : (m-1) \to n$, obtained by induction hypothesis.

3. Otherwise, R is necessarily represented by a precanonical form of the form $W_k\phi'$, where k is the greatest index such that $R(0, k) > 0$ and ϕ' is a precanonical form, obtained by induction, representing the relation $R' : m \to n$ defined by
$$R'(i,j) = \begin{cases} R(i,j) - 1 & \text{if } i = 0 \text{ and } j = k, \\ R(i,j) & \text{otherwise.} \end{cases}$$

It can be moreover shown that every precanonical form representing R corresponds to such an enumeration of the coefficients of R, that the precanonical form constructed by the proof above is canonical, and that it is the only way to obtain a precanonical form representing R. ☐

Finally, we can deduce that

Theorem 6. *The category* $\mathbf{MRel}$ *of multirelations is presented by the equational theory $\mathfrak{B}$ of bicommutative bialgebras.*

Relations. The monoidal category $\mathbf{Rel}$ has finite ordinals as objects and relations as morphisms. This category can be obtained from $\mathbf{MRel}$ by quotienting the morphisms by the equivalence relation $\sim$ on multirelations such that two multirelations $R_1, R_2 : m \to n$ are equivalent when they have the same null coefficients. We can therefore easily adapt the previous presentation to show that

Theorem 7. *The category* $\mathbf{Rel}$ *of relations is presented by the equational theory $\mathfrak{R}$ of* qualitative *bicommutative bialgebras.*

In particular, precanonical forms are the same and canonical forms are defined by adding the rule $W_iW_i \Longrightarrow W_i$ to the rewriting system (10).

4 A game semantics for first-order causality

Suppose that we are given a fixed first-order language $\mathcal{L}$, that is a set of proposition symbols $P, Q, \ldots$ with given arities, a set of function symbols $f, g, \ldots$ with given arities and a set of first-order variables $x, y, \ldots$. *Terms* t and *formulas* A are respectively generated by the following grammars:

$$\begin{array}{rcl} t & ::= & x \quad | \quad f(t, \ldots, t) \\ A & ::= & P(t, \ldots, t) \quad | \quad \forall x.A \quad | \quad \exists x.A \end{array}$$

(we only consider formulas without connectives here). We suppose that application of propositions and functions always respect arities. Formulas are considered modulo renaming of bound variables and substitution $A[t/x]$ of a free variable x by a term t in a formula A is defined as usual, avoiding capture of variables. In the following, we sometimes omit the arguments of propositions when they are clear from the context. We also suppose given a set *Ax* of *axioms*, that is pairs of propositions, which is reflexive, transitive and closed under substitution. The logic associated to these formulas has the following inference rules:

$$\frac{A[t/x] \vdash B}{\forall x.A \vdash B}(\forall\text{-L}) \qquad \frac{A \vdash B}{A \vdash \forall x.B}(\forall\text{-R})$$
(with x not free in A)

$$\frac{A \vdash B}{\exists x.A \vdash B}(\exists\text{-L}) \qquad \frac{A \vdash B[t/x]}{A \vdash \exists x.B}(\exists\text{-R})$$
(with x not free in B)

$$\frac{(P,Q) \in \mathit{Ax}}{P \vdash Q}(\text{Ax}) \qquad \frac{A \vdash B \qquad B \vdash C}{A \vdash C}(\text{Cut})$$

Games and strategies. Games are defined as follows.

Definition 8. *A* game $A = (M_A, \lambda_A, \leq_A)$ *consists of a set of moves* M_A*, a polarization function* λ_A *from* M_A *to* $\{-1, +1\}$ *which to every move* m *associates its* polarity*, and a well-founded partial order* $\leq_A$ *on moves, called* causality *or* justification*. A move* m *is said to be a Proponent move when* $\lambda_A(m) = +1$ *and an Opponent move otherwise.*

If A and B are two games, their tensor product $A \otimes B$ is defined by disjoint union on moves, polarities and causality, the opposite game A^* of the game A is obtained from A by inverting polarities and the arrow game $A \multimap B$ is defined by $A \multimap B = A^* \otimes B$. A game A is *filiform* when the associated partial order is total (we are mostly interested in such games in the following).

Definition 9. *A* strategy σ *on a game* A *is a partial order* $\leq_\sigma$ *on the moves of* A *which satisfies the two following properties:*

1. polarity*: for every pair of moves* $m, n \in M_A$ *such that* $m <_\sigma n$*, we have* $\lambda_A(m) = -1$ *and* $\lambda_A(n) = +1$.
2. acyclicity*: the partial order* $\leq_\sigma$ *is compatible with the partial order of the game, in the sense that the transitive closure of their union is still a partial order (i.e. is acyclic).*

The *size* $|A|$ of a game A is the cardinal of M_A and the *size* $|\sigma|$ of a strategy $\sigma : A$ is the cardinal of the relation $\leq_\sigma$. If $\sigma : A \multimap B$ and $\tau : B \multimap C$ are two strategies, their composite $\tau \circ \sigma : A \multimap C$ is the partial order $\leq_{\tau\circ\sigma}$ on the moves of $A \multimap C$, defined as the restriction of the transitive closure of the union $\leq_\sigma \cup \leq_\tau$ of the partial orders $\leq_\sigma$ and $\leq_\tau$ (considered as relations). The identity strategy $\mathrm{id}_A : A \multimap A$ on a game A is the strategy such that for every move m of A we have $m_L \leq_{\mathrm{id}_A} m_R$ if $\lambda_A(m) = -1$ and $m_R \leq_{\mathrm{id}_A} m_L$ if $\lambda_A(m) = +1$, where m_L (resp. m_R) is the instance of a move m in the left-hand side (resp. right-hand side) copy of A.

Since composition of strategies is defined in the category of relations, we still have to check that the composite of two strategies σ and τ is actually a strategy. The preservation by composition of the polarity condition is immediate. However, proving that the relation $\leq_{\tau\circ\sigma}$ corresponding to the composite strategy is acyclic is more difficult: a direct proof of this property is combinatorial, lengthy and requires global reasoning about strategies. For now, we define the category $\mathbf{Games}$ as the category whose objects are finite filiform games, and whose sets of morphisms are the smallest sets containing the strategies on the game $A \multimap B$ as morphisms between two objects A and B and are moreover closed under composition. We will deduce at the end of the section, from its presentation, that strategies are in fact the only morphisms of this category.

If A and B are two games, the game $A \oslash B$ (to be read A *before* B) is the game defined as $A \otimes B$ on moves and polarities and $\leq_{A \oslash B}$ is the transitive closure of the relation

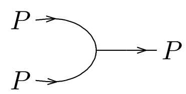
$$\leq_{A\otimes B} \cup \{\ (a,b) \quad | \quad a \in M_A \text{ and } b \in M_B\ \}$$

This operation is extended as a bifunctor on strategies as follows. If $\sigma : A \to B$ and $\tau : C \to D$ are two strategies, the strategy $\sigma \oslash \tau : A \oslash C \to B \oslash D$ is defined as the relation $\leq_{\sigma\oslash\tau} = \leq_\sigma \uplus \leq_\tau$. This bifunctor induces a monoidal structure $(\mathbf{Games}, \oslash, I)$ on the category $\mathbf{Games}$, where I denotes the empty game.

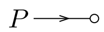
We write O for a game with only one Opponent move and P for a game with only one Proponent move. It can be easily remarked that finite filiform games A are generated by the following grammar

$$A \quad ::= \quad I \quad | \quad O \oslash A \quad | \quad P \oslash A$$

A strategy $\sigma : A \to B$ is represented graphically by drawing a line from a move m to a move n whenever $m \leq_\sigma n$. For example, the strategy $\mu^P : P \oslash P \to P$



is the strategy on the game $(O \oslash O) \otimes P$ in which both Opponent move of the left-hand game justify the Proponent move of the right-hand game. When a move does not justify (or is not justified by) any other move, we draw a line ended by a small circle. For example, the strategy $\varepsilon^P : P \to I$, drawn as



is the unique strategy from P to the terminal object I. With these conventions, we introduce notations for some morphisms which are depicted in Figure 1.

$$
\begin{array}{rcl rcl}
\mu^O & : & O \otimes O \to O & \mu^P & : & P \otimes P \to P \\
\eta^O & : & I \to O & \eta^P & : & I \to P \\
\delta^O & : & O \to O \otimes O & \delta^P & : & P \to P \otimes P \\
\varepsilon^O & : & O \to I & \varepsilon^P & : & P \to I \\
\gamma^O & : & O \otimes O \to O \otimes O & \gamma^P & : & P \otimes P \to P \otimes P \\
\eta^{OP} & : & I \to O \otimes P & \varepsilon^{OP} & : & P \otimes O \to I
\end{array}
$$

$$\gamma^{OP} \quad : \quad P \otimes O \to O \otimes P$$

respectively drawn as

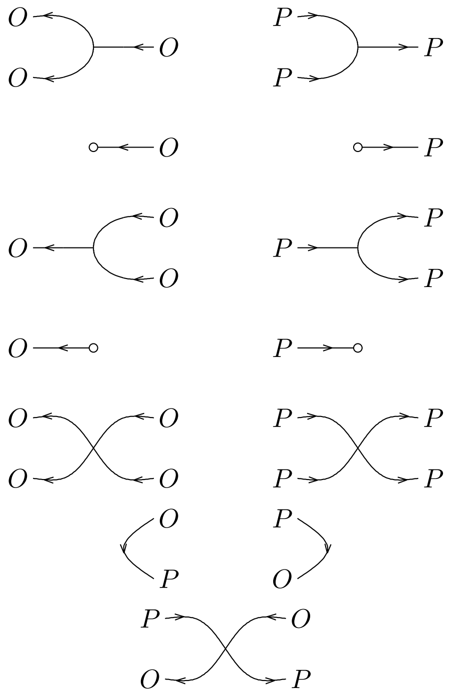


Figure 1. Generators of the strategies.

A game semantics. A formula A is interpreted as a filiform game $[\![A]\!]$ by

$$[\![P]\!] = I \qquad [\![\forall x.A]\!] = O \otimes [\![A]\!] \qquad [\![\exists x.A]\!] = P \otimes [\![A]\!]$$

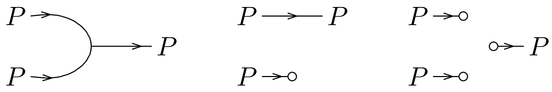
A cut-free proof $\pi : A \vdash B$ is interpreted as a strategy $\sigma : [\![A]\!] \multimap [\![B]\!]$ whose causality partial order $\leq_\sigma$ is defined as follows. For every Proponent move P interpreting a quantifier introduced by a rule which is either

$$\frac{A[t/x] \vdash B}{\forall x.A \vdash B}(\forall\text{-L}) \qquad \text{or} \qquad \frac{A \vdash B[t/x]}{A \vdash \exists x.B}(\exists\text{-R})$$

every Opponent move O interpreting an universal quantification $\forall x$ on the right-hand side of a sequent, or an existential quantification $\exists x$ on the left-hand side of a sequent, is such that $O \leq_\sigma P$ whenever the variable x is free in the term t. For example, a proof

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \vdash Q[t/z]}(\text{Ax})}{P \vdash \exists z.Q}(\exists\text{-R})}{\exists y.P \vdash \exists z.Q}(\exists\text{-L})}{\exists x.\exists y.P \vdash \exists z.Q}(\exists\text{-L})$$

is interpreted respectively by the strategies



(11)

when the free variables of t are $\{x, y\}$, $\{x\}$ or $\emptyset$.

An equational theory of strategies. We can now introduce the equational theory which will be shown to present the category $\mathbf{Games}$.

Definition 10. *The* equational theory of strategies *is the equational theory $\mathfrak{G}$ with two atomic types O and P and thirteen generators depicted in Figure 1 such that*

- *the Opponent structure*
$$(O, \mu^O, \eta^O, \delta^O, \varepsilon^O, \gamma^O) \tag{12}$$
is a bicommutative qualitative bialgebra,
- *the Proponent structure $(P, \mu^P, \eta^P, \delta^P, \varepsilon^P, \gamma^P)$, as well as the morphism γ^{OP}, are deduced from the Opponent structure* (12) *by composition with the duality morphisms η^{OP} and ε^{OP} (for example $\eta^P = (\varepsilon^O \otimes \mathrm{id}_P) \circ \eta^{OP}$).*

We write $\mathcal{G}/\!\equiv$ for the monoidal category generated by $\mathfrak{G}$. It can be noticed that the generators μ^P, η^P, δ^P, ε^P, γ^P and γ^{OP} are superfluous in this presentation (since they can be deduced from the Opponent structure and duality). However, removing them would seriously complicate the proofs.

We can now proceed as in Section 3 to show that the theory $\mathfrak{G}$ introduced in Definition 10 presents the category $\mathbf{Games}$. First, in the category $\mathbf{Games}$ with the monoidal structure induced by $\otimes$, the objects O and P can be canonically equipped with thirteen morphisms as shown in Figure 1 in order to form a model of the theory $\mathfrak{G}$.

Conversely, we need to introduce a notion of canonical form for the morphisms of $\mathcal{G}$. *Stairs* are defined similarly as before, but are now constructed from the three kinds of polarized crossings γ^O, γ^P and γ^{OP} instead of simply γ in (8). The notion of *precanonical form* ϕ is now defined inductively as shown in Figure 2, where the object X is either O or P and ϕ' is a precanonical form. These cases correspond respectively to the productions of the following grammar

$$\phi \quad ::= \quad Z \;\mid\; A_i\phi \;\mid\; B_i\phi \;\mid\; W_i^X\phi \;\mid\; E^X\phi \;\mid\; H^X\phi$$

By induction on the size of morphisms, it can be shown that every morphism of $\mathcal{G}$ is equivalent to a precanonical form and a notion of canonical form can be defined by adapting the rewriting system (10) into a normalizing rewriting system for precanonical forms. Finally, a reasoning similar to Lemma 5 shows that canonical forms are in bijection with morphisms of the category $\mathbf{Games}$.

Theorem 11. *The monoidal category $\mathbf{Games}$ (with the $\otimes$ tensor product) is presented by the equational theory $\mathfrak{G}$.*

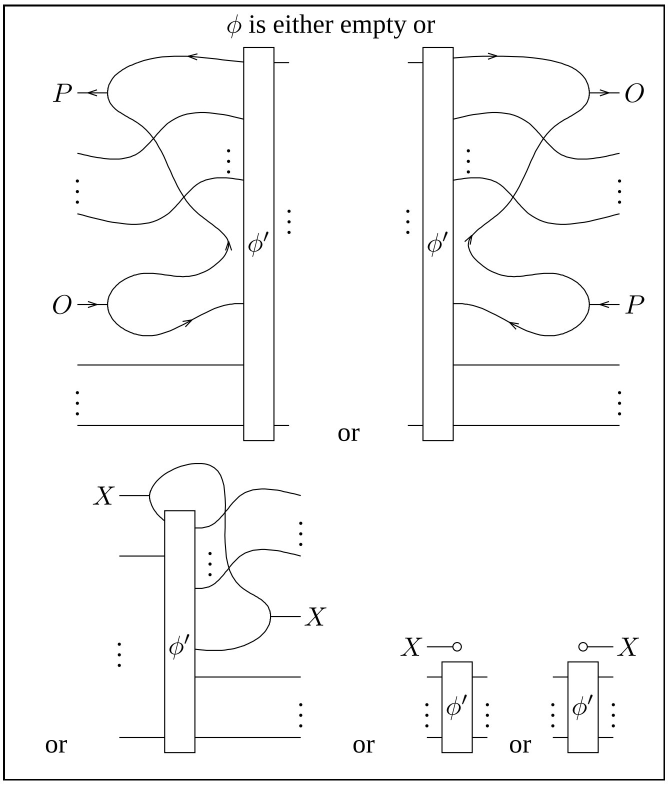


Figure 2. Precanonical forms for strategies.

As a direct consequence of this Theorem, we deduce that

1. the composite of two strategies, in the sense of Definition 9, is itself a strategy (in particular, the acyclicity property is preserved by composition),
2. the strategies of $\mathbf{Games}$ are definable (when the set *Ax* of axioms is reasonable enough): it is enough to check that generators are definable – for example, the first case of (11) shows that μ^P is definable.

5 Conclusion

We have constructed a game semantics for first-order propositional logic and given a presentation of the category $\mathbf{Games}$ of games and definable strategies. This has revealed the essential structure of causality induced by quantifiers as well as provided technical tools to show definability and composition of strategies.

We consider this work much more as a starting point to bridge semantics and algebra than as a final result. The methodology presented here seems to be very general and many tracks remain to be explored. First, we would like to extend the presentation to a game semantics for richer logic systems, containing connectives (such as conjunction or disjunction). Whilst we do not expect essential technical complications, this case is much more difficult to grasp and manipulate, since a presentation of such a semantics would have generators up to dimension 3 (one dimension is added since games would be trees instead of lines) and corresponding diagrams would now live in a 3-dimensional space. It would also be interesting to know whether it is possible to orient the equalities in the presentations in order to obtain strongly normalizing rewriting systems for the algebraic structures described in the paper. Such rewriting systems are given in [8] – for monoids and commutative monoids for example – but finding a strongly normalizing rewriting system presenting the theory of bialgebras is a difficult problem [13]. Finally, some of the proofs (such as the proof of Lemma 4) are very repetitive and we believe that they could be mechanically checked or automated. However, finding a good representation of morphisms, in order for a program to be able to manipulate them, is a difficult task that we should address in subsequent works.

Acknowledgements. I would like to thank my PhD supervisor Paul-André Melliès as well as John Baez, Albert Burroni, Yves Guiraud, Martin Hyland, Yves Lafont and François Métayer for the lively discussion we had, during which I learned so much.

References

[1] J. Baez and L. Langford. Higher-dimensional algebra IV: 2-tangles. *Advances in Mathematics*, 180(2):705–764, 2003.
[2] A. Burroni. Higher-dimensional word problems with applications to equational logic. *TCS*, 115(1):43–62, 1993.
[3] M. Hyland and L. Ong. On Full Abstraction for PCF: I, II, III. *Information and Computation*, 163(2):285–408, 2000.
[4] M. Hyland and J. Power. Symmetric Monoidal Sketches. In *Proceedings of PPDP'00*, pages 280–288, 2000.
[5] A. Joyal and R. Street. The Geometry of Tensor Calculus, I. *Advances in Mathematics*, 88:55–113, 1991.
[6] S. Lack. Composing PROPs. *Theory and Applications of Categories*, 13(9):147–163, 2004.
[7] Y. Lafont. Equational Reasoning with 2-Dimensional Diagrams. *Term Rewriting*, pages 170–195, 1995.
[8] Y. Lafont. Towards an Algebraic Theory of Boolean Circuits. *J. Pure Appl. Algebra*, 184(2-3):257–310, 2003.
[9] F. W. Lawvere. *Functorial Semantics of Algebraic Theories and Some Algebraic Problems in the context of Functorial Semantics of Algebraic Theories*. PhD thesis, 1963.
[10] S. MacLane. Categorical Algebra. *Bulletin of the American Mathematical Society*, 71:40–106, 1965.
[11] S. MacLane. *Categories for the Working Mathematician*. Graduate Texts in Mathematics. Springer Verlag, 1971.
[12] P.-A. Melliès and S. Mimram. Asynchronous Games: Innocence without Alternation. In *Proceedings of CONCUR'05*, volume 4703 of *LNCS*, pages 395–411. Springer, 2007.
[13] S. Mimram. *Sémantique des jeux asynchrones et réécriture 2-dimensionnelle*. PhD thesis, 2008.
[14] T. Pirashvili. On the PROP Corresponding to Bialgebras. *Cah. Top. Géom. Diff. Cat.*, 43(3):221–239, 2002.
[15] R. Street. Limits indexed by category-valued 2-functors. *J. Pure Appl. Algebra*, 8(2):149–181, 1976.