

The Structure of First-Order Causality (extended version)

Samuel Mimram

► **To cite this version:**

Samuel Mimram. The Structure of First-Order Causality (extended version). Mathematical Structures in Computer Science, Cambridge University Press (CUP), 2011, 21 (01), pp.65-110. <http://journals.cambridge.org/article_S0960129510000459>. <10.1017/S0960129510000459>. <inria-00559240>

HAL Id: inria-00559240

<https://hal.inria.fr/inria-00559240>

Submitted on 25 Jan 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The Structure of First-Order Causality

Samuel Mimram*

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. The interactions between these two players are sequences of moves respecting the partial order of the game, called *plays*. In this setting, a program is characterized by the set of plays 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 [HO00], 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

*This work has been supported by the CHOCO (“Curry Howard pour la Concurrency”, ANR-07-BLAN-0324) French ANR project.

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 led 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 **Games**. Instead of characterizing definable strategies of the model by restricting to strategies satisfying particular conditions, we show here that we can equivalently use 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 **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 these strategies actually *compose*, which is not trivial, and it also enables us to deduce that the strategies of the category **Games** are *definable* (one only needs to check that generators are definable). 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,

or more generally sequents. Namely, a formula (or a sequent) is a syntactic tree expressing in which order its connectives must be introduced in cut-free proofs. In this sense, it can be seen as the rules of a game whose moves correspond to connectives. For instance, consider a sequent of the form

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

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 on the right of a sequent 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); introducing a quantification on the left of a sequent is similar but with polarities inverted since it is the same as introducing the dual quantification on the right of the sequent. 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):

$$\begin{array}{c} \forall x \quad \forall y \\ | \\ \exists z \end{array} \tag{2}$$

This partial order is sometimes called the *syntactic partial order* generated by the sequent. Possible proofs of sequent (1) in first-order propositional logic are of one of the three following shapes:

$$\begin{array}{c} \vdots \\ \hline P[t/x] \vdash Q[t'/z] \\ \hline P[t/x] \vdash \exists z.Q \\ \hline P[t/x] \vdash \forall y.\exists z.Q \\ \hline \forall x.P \vdash \forall y.\exists z.Q \end{array} \quad \begin{array}{c} \vdots \\ \hline P[t/x] \vdash Q[t'/z] \\ \hline P[t/x] \vdash \exists z.Q \\ \hline \forall x.P \vdash \exists z.Q \\ \hline \forall x.P \vdash \forall y.\exists z.Q \end{array} \quad \begin{array}{c} \vdots \\ \hline P[t/x] \vdash Q[t'/z] \\ \hline \forall x.P \vdash Q[t'/z] \\ \hline \forall x.P \vdash \exists z.Q \\ \hline \forall x.P \vdash \forall y.\exists z.Q \end{array}$$

where $P[t/x]$ denotes the formula P where every occurrence of the free variable x has been replaced by the term t . These proofs introduce the connectives in the orders depicted respectively below

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

which are all total orders extending the partial order of the game (2): these correspond to the plays in the strategies interpreting the proofs in the game semantics. In this sense, they have more dependencies between moves: proofs add causal dependencies between connectives.

Some sequentializations induced by proofs are not really relevant. For example consider a proof of the form

$$\frac{\frac{\frac{\pi}{P \vdash Q}}{P \vdash \forall y.Q}}{\exists x.P \vdash \forall y.Q}}$$

The order in which the introduction rules of the universal and existential quantifications are introduced is not really significant here since this proof might always be reorganized into the proof

$$\frac{\frac{\frac{\pi}{P \vdash Q}}{\exists x.P \vdash Q}}{\exists x.P \vdash \forall y.Q}}$$

by “permuting” the introduction rules. Similarly, the following permutations of rules are always possible:

$$\frac{\frac{\frac{\pi}{P[t/x] \vdash Q[u/y]}}{P[t/x] \vdash \exists y.Q}}{\forall x.P \vdash \exists y.Q} \rightsquigarrow \frac{\frac{\frac{\pi}{P[t/x] \vdash Q[u/y]}}{\forall x.P \vdash Q[u/y]}}{\forall x.P \vdash \exists y.Q} \quad \text{and} \quad \frac{\frac{\frac{\pi}{P[t/x] \vdash Q}}{P[t/x] \vdash \forall y.Q}}{\forall x.P \vdash \forall y.Q} \rightsquigarrow \frac{\frac{\frac{\pi}{P[t/x] \vdash Q}}{\forall x.P \vdash Q}}{\forall x.P \vdash \forall y.Q}$$

Interestingly, the permutation

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

is only possible 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. Now, the sequent $\exists x.P \vdash \exists y.Q$ will be interpreted by the following game

$$\exists x \quad \exists y$$

Whenever the $\exists y$ connective depends on the $\exists x$ connective (i.e. whenever x is free in the witness term t provided for y), the strategy corresponding to the proof will contain a causal dependency, which will be 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 [MM07], where plays are considered modulo certain permutations of

consecutive moves. However, we focus here on causality and define strategies by the dependencies they induce on moves (a precise description of the relation between these two points of view was investigated in [Mim08]). They are also very closely related to the motivations for the introduction of Hintikka’s games and independence friendly logic [HS97].

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 the connective-free fragment of first-order propositional logic, and write **Games** for the subcategory of definable strategies. One should thus keep in mind the following correspondences while reading this paper:

category	logic	game semantics	combinatorial objects
object	formula	game	syntactic order
morphism	proof	strategy	justification order

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 **Games**, that we define formally in Section 4.

1 Presentations of monoidal categories

We recall here briefly some basic definitions in category theory. The interested reader can find a more detailed presentation of these concepts in MacLane’s reference book [Mac71].

Monoidal categories. A *monoidal category* $(\mathcal{C}, \otimes, I)$ is a category \mathcal{C} together with a functor

$$\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$$

and natural isomorphisms

$$\alpha_{A,B,C} : (A \otimes B) \otimes C \rightarrow A \otimes (B \otimes C), \quad \lambda_A : I \otimes A \rightarrow A \quad \text{and} \quad \rho_A : A \otimes I \rightarrow A$$

satisfying coherence axioms [Mac71]. A symmetric monoidal category \mathcal{C} is a monoidal category \mathcal{C} together with a natural isomorphism

$$\gamma_{A,B} : A \otimes B \rightarrow B \otimes A$$

satisfying coherence axioms and such that $\gamma_{B,A} \circ \gamma_{A,B} = \text{id}_{A \otimes B}$. A monoidal category \mathcal{C} is *strictly* monoidal when the natural isomorphisms α , λ and ρ are identities. For the sake of simplicity, in the rest of this paper we only consider strict monoidal categories. Formally, it can be shown that it is not restrictive, using MacLane’s coherence theorem [Mac71]: every monoidal category is monoidally equivalent to a strict one.

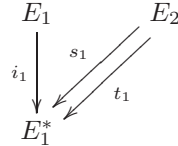
A (strict) *monoidal functor* $F : \mathcal{C} \rightarrow \mathcal{D}$ between two strict monoidal categories \mathcal{C} and \mathcal{D} is a functor F between the underlying categories such that $F(A \otimes B) = F(A) \otimes F(B)$ for every objects A and B of \mathcal{C} , and $F(I) = I$. A *monoidal natural transformation* $\theta : F \rightarrow G$ between two monoidal functors $F, G : \mathcal{C} \rightarrow \mathcal{D}$ is a natural transformation between the underlying functors F

and G such that $\theta_{A \otimes B} = \theta_A \otimes \theta_B$ for every objects A and B of \mathcal{C} , and $\theta_I = \text{id}_I$. Two monoidal categories \mathcal{C} and \mathcal{D} are *monoidally equivalent* when there exists a pair of monoidal functors $F : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$ and two invertible monoidal natural transformations $\eta : \text{Id}_{\mathcal{C}} \rightarrow GF$ and $\varepsilon : FG \rightarrow \text{Id}_{\mathcal{D}}$.

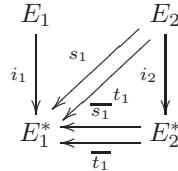
Monoidal theories. A *monoidal theory* \mathbb{T} is a strict monoidal category whose objects are the natural integers, such that the tensor product on objects is the addition of integers. By an integer \underline{n} , we mean here the finite ordinal $\underline{n} = \{0, 1, \dots, n-1\}$ and the addition is given by $\underline{m} + \underline{n} = \underline{m+n}$ (we will simply write n instead of \underline{n} in the following). 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 MacLane in [Mac65] as an abbreviation for “category with products”. They generalize equational theories – or Lawvere theories [Law63] – 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* or *generators for objects*. We write E_1^* for the free monoid on the set E_1 and $i_1 : E_1 \rightarrow E_1^*$ 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 (for morphisms)*, together with two functions $s_1, t_1 : E_2 \rightarrow E_1^*$, 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) :



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 formal tensor products of elements of E_2 , quotiented by suitable laws imposing associativity of composition and tensor and compatibility of composition with tensor, see [Bur93]. If we write E_2^* for the morphisms of this category and $i_2 : E_2 \rightarrow E_2^*$ for the injection of the generators into this category, we get a diagram



$t_1(f) = B$. 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 $t_2(e) = g$.

We say that two equational theories are *equivalent* when they generate monoidally equivalent categories. A generator f in an equational theory \mathfrak{E} is *superfluous* when the equational theory \mathfrak{E}' obtained from \mathfrak{E} by removing the generator f and all equations involving f , is equivalent to \mathfrak{E} . Similarly, an equation e is *superfluous* when the equational theory \mathfrak{E}' obtained from \mathfrak{E} by removing the equation e is equivalent to \mathfrak{E} . An equational theory is *minimal* when it does not contain any superfluous generator or equation.

Notice 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 $M : \mathbb{E} \rightarrow \mathcal{M}$. This amounts to checking that there exists a functor $M' : \mathcal{E} \rightarrow \mathcal{M}$ such that for all morphisms $f, g : A \rightarrow B$ in \mathcal{E} , $f \equiv g$ implies $M'f = M'g$.
2. \mathcal{M} is a fully-complete model of the equational theory \mathfrak{E} : the functor M is full and faithful.

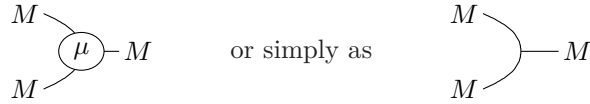
We sometimes say that a morphism $f : A \rightarrow B$ of \mathbb{E} *represents* the morphism $Mf : MA \rightarrow MB$ of \mathcal{M} .

Usually, the first point is a straightforward verification. Proving that the functor M is full and faithful often requires more work. In this paper, we use the methodology introduced by Burroni [Bur93] and refined by Lafont [Laf03]. 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 M 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 [JS91] 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 [BL03] 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 [Lac04], 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: we believe indeed that some of the tedious proofs given

in this paper could be somewhat automated, a first step in this direction was given in [Mim10] where we describe an algorithm to compute critical pairs in polygraphic rewriting systems of dimension 2.

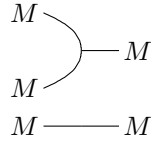
String diagrams. *String diagrams* provide a convenient way to represent and manipulate the morphisms in the category generated by a presentation. Given an object M in a strict monoidal category \mathcal{C} , a morphism $\mu : M \otimes M \rightarrow M$ can be drawn graphically as a device with two inputs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



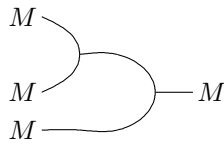
when it is clear from the context which morphism of type $M \otimes M \rightarrow M$ we are picturing (we sometimes even omit the source and target of the morphisms). Similarly, the identity $\text{id}_M : M \rightarrow M$ (which we sometimes simply write M) can be pictured as a wire



The tensor $f \otimes g$ of two morphisms $f : A \rightarrow B$ and $g : C \rightarrow D$ 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



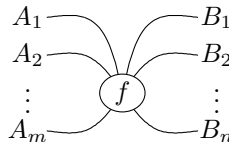
Finally, the composite $g \circ f : A \rightarrow C$ of two morphisms $f : A \rightarrow B$ and $g : B \rightarrow C$ can be drawn diagrammatically by putting the diagram corresponding to g at the right of the diagram corresponding to f and “linking the wires”. The diagram corresponding to the morphism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

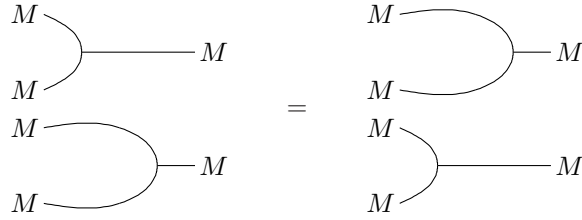


where wires correspond to generators for objects and circled points to generators for morphisms. Bigger diagrams can be constructed from these diagrams by

composing and tensoring them, as explained above. Joyal and Street have shown in details in [JS91] 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

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

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, the most fundamental in this work being maybe the notion of *bialgebra*. 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.

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

$$\gamma : S \otimes S \rightarrow S \otimes S$$

called *symmetry* and pictured as

$$\begin{array}{ccc} S & \text{---} & S \\ & \text{---} & \\ S & \text{---} & S \end{array} \quad (3)$$

such that the diagrams

$$\begin{array}{ccccc} S \otimes S \otimes S & \xrightarrow{\gamma \otimes S} & S \otimes S \otimes S & \xrightarrow{S \otimes \gamma} & S \otimes S \otimes S \\ \downarrow S \otimes \gamma & & & & \downarrow \gamma \otimes S \\ S \otimes S \otimes S & \xrightarrow{\gamma \otimes S} & S \otimes S \otimes S & \xrightarrow{S \otimes \gamma} & S \otimes S \otimes S \end{array}$$

and

$$\begin{array}{ccc}
 & S \otimes S & \\
 \gamma \nearrow & & \searrow \gamma \\
 S \otimes S & \xrightarrow{s \otimes s} & S \otimes S
 \end{array}$$

commute. Graphically,

$$\begin{array}{ccc}
 \text{[Diagram 1]} & = & \text{[Diagram 2]} \\
 \text{[Diagram 3]} & = & \text{[Diagram 4]}
 \end{array} \tag{4}$$

(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

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

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

$$\begin{array}{ccc}
 \begin{array}{c} M \\ \text{---} \\ M \end{array} \text{---} M & \text{and} & \circ \text{---} M
 \end{array} \tag{5}$$

such that the diagrams

$$\begin{array}{ccc}
 M \otimes M \otimes M & \xrightarrow{\mu \otimes M} & M \otimes M \\
 \downarrow M \otimes \mu & & \downarrow \mu \\
 M \otimes M & \xrightarrow{\mu} & M
 \end{array}
 \quad \text{and} \quad
 \begin{array}{ccc}
 I \otimes M & \xrightarrow{\eta \otimes M} & M \otimes M & \xleftarrow{M \otimes \eta} & M \otimes I \\
 \searrow M & & \downarrow \mu & & \swarrow M \\
 & & M & &
 \end{array}$$

commute. Graphically,

$$\begin{array}{ccc}
 \text{[Diagram 1]} & = & \text{[Diagram 2]} \\
 \text{[Diagram 3]} & = & \text{[Diagram 4]} = \text{[Diagram 5]}
 \end{array} \tag{6}$$

A *symmetric monoid* is a monoid equipped with a symmetry morphism $\gamma : M \otimes M \rightarrow M \otimes M$ which is compatible with the operations of the monoid in the sense that it makes the diagrams

$$\begin{array}{ccc}
 M \otimes M \otimes M & \xrightarrow{M \otimes \gamma} & M \otimes M \otimes M & \xrightarrow{\gamma \otimes M} & M \otimes M \otimes M \\
 \mu \otimes M \downarrow & & & & \downarrow M \otimes \mu \\
 M \otimes M & \xrightarrow{\gamma} & M \otimes M & & M \otimes M \\
 \\
 M \otimes M \otimes M & \xrightarrow{\gamma \otimes M} & M \otimes M \otimes M & \xrightarrow{M \otimes \gamma} & M \otimes M \otimes M \\
 M \otimes \mu \downarrow & & & & \downarrow \mu \otimes M \\
 M \otimes M & \xrightarrow{\gamma} & M \otimes M & & M \otimes M \\
 \\
 M & \xrightarrow{\eta \otimes M} & M \otimes M & \xrightarrow{\gamma} & M \otimes M \\
 \eta \otimes M \nearrow & & & & \searrow \gamma \\
 & & M \otimes M & & \\
 \\
 M & \xrightarrow{\eta \otimes M} & M \otimes M & \xrightarrow{\gamma} & M \otimes M \\
 \eta \otimes M \nearrow & & & & \searrow \gamma \\
 & & M \otimes M & & \\
 \\
 M & \xrightarrow{M \otimes \eta} & M \otimes M & \xrightarrow{\gamma} & M \otimes M \\
 M \otimes \eta \nearrow & & & & \searrow \gamma \\
 & & M \otimes M & & \\
 \\
 M & \xrightarrow{M \otimes \eta} & M \otimes M & \xrightarrow{\gamma} & M \otimes M \\
 M \otimes \eta \nearrow & & & & \searrow \gamma \\
 & & M \otimes M & &
 \end{array}$$

commute. Graphically,

$$\begin{array}{ccc}
 \text{Diagram 1} & = & \text{Diagram 2} \\
 \text{Diagram 3} & = & \text{Diagram 4}
 \end{array} \tag{7}$$

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

$$\begin{array}{ccc}
 & M \otimes M & \\
 \gamma \nearrow & & \searrow \mu \\
 M \otimes M & \xrightarrow{\mu} & M
 \end{array}$$

commutes. Graphically,

$$\text{Diagram 5} = \text{Diagram 6} \tag{8}$$

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 (7) 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

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

respectively drawn as

$$\begin{array}{c} M \\ \text{---} \left(\begin{array}{l} \text{---} M \\ \text{---} M \end{array} \right. \end{array} \quad \text{and} \quad M \text{---} \circ \quad (9)$$

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 generator for objects 1 and two generators for morphisms $\mu : 2 \rightarrow 1$ and $\eta : 0 \rightarrow 1$ subject to the three relations*

$$\begin{array}{lcl} \mu \circ (\mu \otimes \text{id}_1) & = & \mu \circ (\text{id}_1 \otimes \mu) \\ \mu \circ (\eta \otimes \text{id}_1) & = & \text{id}_1 = \mu \circ (\text{id}_1 \otimes \eta) \end{array} \quad (10)$$

The equations (10) correspond precisely to the equations for a monoid object (6). 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.

Remark 3. The presentations given here are not necessarily minimal. For example, in the theory of commutative monoids one equation for units of monoids (5) is derivable from the equation (8), one of the equations (7) and one of the equations for units of monoids (5):

A minimal presentation of this equational theory with three generators and seven equations is given in [Mas97]. However, not all the equational theories introduced in this paper have a known presentation which is proved to be minimal.

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

$$\begin{array}{lcl} \mu : B \otimes B \rightarrow B & \eta : I \rightarrow B & \\ \delta : B \rightarrow B \otimes B & \varepsilon : B \rightarrow I & \text{and } \gamma : B \otimes B \rightarrow B \otimes B \end{array}$$

such that $\gamma : B \otimes B \rightarrow B \otimes B$ 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 (3), μ and η as in (5), and δ and ε as in (9). Those two structures

comonoids which are dual of (6) (7) (8), and the four compatibility relations for bialgebras (11).

We also write \mathfrak{R} for the equational theory of qualitative bicommutative bialgebras which is defined as \mathfrak{B} , with the relation (12) added.

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

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

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

$$\begin{array}{c} R \\ \curvearrowright \\ L \end{array} \quad \text{and} \quad \begin{array}{c} L \\ \curvearrowleft \\ R \end{array}$$

making the diagrams

$$\begin{array}{ccc} & L \otimes R \otimes L & \\ L \otimes \eta \nearrow & & \searrow \varepsilon \otimes L \\ L & \xrightarrow{L} & L \end{array} \quad \text{and} \quad \begin{array}{ccc} & R \otimes L \otimes R & \\ \eta \otimes R \nearrow & & \searrow R \otimes \varepsilon \\ R & \xrightarrow{R} & R \end{array}$$

commute. Graphically,

$$\begin{array}{c} L \\ \curvearrowright \\ L \end{array} = L \text{ --- } L \quad \text{and} \quad \begin{array}{c} R \\ \curvearrowleft \\ R \end{array} = R \text{ --- } R$$

We write \mathfrak{D} for the equational theory associated to dual objects.

Remark 5. If \mathcal{C} is a category, two dual objects in the monoidal category $\text{End}(\mathcal{C})$ of endofunctors of \mathcal{C} , with tensor product given on objects by composition of functors, are adjoint endofunctors of \mathcal{C} . The theory of adjoint functors in a 2-category is described precisely in [SS86], the definition of \mathfrak{D} is a specialization of this construction to the case where there is only one 0-cell.

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 [HP00] and is proved in three different ways in [Laf95], [Pir02] and [Lac04]. 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.

The simplicial category. The simplicial category Δ is the monoidal theory whose morphisms $f : m \rightarrow n$ are the monotone functions from m to n . It has been known for a long time that this category is closely related to the notion of monoid, see [Mac71] or [Laf03] for example. This result can be formulated as follows:

Property 6. *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 $R : A \times B \rightarrow \mathbb{N}$. 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

$$\begin{array}{ccc} & R & \\ s \swarrow & & \searrow t \\ A & & B \end{array}$$

in the category **FinSet** of finite sets – for the latest case, the multiset representation can be recovered from the span by

$$R(a, b) = |\{ e \in R \mid s(e) = a \text{ and } t(e) = b \}|$$

for every element $(a, b) \in A \times B$. If $R_1 : A \rightarrow B$ and $R_2 : B \rightarrow C$ are two multirelations, their composition is defined by

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

This corresponds to the usual composition of matrices if we see R_1 and R_2 as matrices over \mathbb{N} , and as the span obtained by computing the pullback

$$\begin{array}{ccccc} & & R_2 \circ R_1 & & \\ & \swarrow & & \searrow & \\ & R_1 & & R_2 & \\ s_1 \swarrow & & t_1 & & \searrow s_2 \\ A & & B & & C \end{array}$$

if we see R_1 and R_2 as spans in **Set**. The cardinal $|R|$ of a multirelation $R : A \rightarrow B$ is the sum

$$|R| = \sum_{(a,b) \in A \times B} R(a, b)$$

of its coefficients. We write **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 1 can be equipped with the obvious structure of bicommutative bialgebra

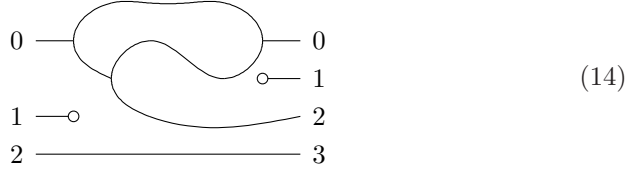
$$(1, R^\mu, R^\eta, R^\delta, R^\epsilon) \tag{13}$$

In this structure, $R^\mu : 2 \rightarrow 1$ is the multirelation defined by $R^\mu(i, 0) = 1$ for $i = 0$ or $i = 1$, $R^\delta : 1 \rightarrow 2$ is the multirelation dual to R^μ , and $R^\eta : 0 \rightarrow 1$ and $R^\varepsilon : 1 \rightarrow 0$ are uniquely defined by the fact that the object 0 is both initial and terminal in \mathbf{MRel} . We now show that the category of multirelations is presented by the equational theory \mathfrak{B} of bicommutative bialgebras. We write \mathcal{B} for the syntactic category of \mathfrak{B} (i.e. the monoidal category generated by the underlying signature of \mathfrak{B}), so that \mathcal{B}/\equiv is the monoidal category generated by \mathfrak{B} , where \equiv is the congruence generated by the relations of \mathfrak{B} . The bicommutative bialgebra structure (13) induces an “interpretation functor” $I : \mathcal{B} \rightarrow \mathbf{MRel}$ such that $I(1) = 1$, $I(\mu) = R^\mu$, $I(\eta) = R^\eta$, $I(\delta) = R^\delta$ and $I(\varepsilon) = R^\varepsilon$. Since, the morphisms (13) satisfy the equations of bicommutative bialgebra, the interpretations of two morphisms of \mathcal{B} related by \equiv will be equal. The interpretation functor thus extends to a functor $I/\equiv : \mathcal{B}/\equiv \rightarrow \mathbf{MRel}$.

Example 7. Consider the morphism

$$((\mu \otimes \eta \otimes 1) \circ (1 \otimes \delta) \circ (\delta \otimes \varepsilon)) \otimes 1 \quad : \quad 3 \rightarrow 4$$

of \mathcal{B} whose graphical representation is



Its interpretation is the multirelation

$$((R^\mu \otimes R^\eta \otimes 1) \circ (1 \otimes R^\delta) \circ (R^\delta \otimes R^\varepsilon)) \otimes 1 \quad (15)$$

This multirelation is a function $3 \times 4 \rightarrow \mathbb{N}$ (where 3 and 4 are respectively the sets $\{0, 1, 2\}$ and $\{0, 1, 2, 3\}$) and can thus be represented as the following \mathbb{N} -valued matrix of size 3×4 :

$$\begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

This matrix is computed by evaluating the formula (15) but has in fact a very natural interpretation if we consider the string diagrammatic representation (14) of the morphism: an entry (i, j) of the matrix is precisely the number of different paths in wires linking the object i on the input to the object j on the output (for example, from 0 there are two paths to 0 and one to 2, thus the first line of the matrix).

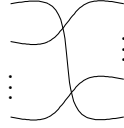
For every morphism $\phi : m+1 \rightarrow n$ in \mathcal{B} , where $m > 0$, we define a morphism written $S^{m \rightarrow n} \phi : m+1 \rightarrow n$ by

$$S^{m \rightarrow n} \phi = \phi \circ (\gamma \otimes \text{id}_{m-1}) \quad (16)$$

Graphically,

$$S^{m \rightarrow n} \phi = \text{[Diagram: A vertical rectangle labeled } \phi \text{ with } m \text{ horizontal lines on the left and } n \text{ on the right. The top two lines cross each other. Vertical ellipses are on both sides.]}$$

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 id_1 , or as the length of the stairs ϕ' plus one if it is of the form $S\phi'$. The stairs of length $n + 1$ is written $\gamma_n : n \rightarrow n$.

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

$$H^{m \rightarrow n} \phi' = \text{[Diagram: A vertical rectangle labeled } \phi' \text{ with } m \text{ lines on the left and } n \text{ on the right. A small circle is on the top line on the left. Vertical ellipses are on both sides.]} \quad \text{or} \quad E^{m \rightarrow n} \phi' = \text{[Diagram: A vertical rectangle labeled } \phi' \text{ with } m \text{ lines on the left and } n \text{ on the right. A small circle is on the top line on the right. Vertical ellipses are on both sides.]}$$

or

$$W_i^{m \rightarrow n} \phi' = \text{[Diagram: A vertical rectangle labeled } \phi' \text{ with } m \text{ lines on the left and } n \text{ on the right. A loop connects the top line on the left to the top line on the right. Vertical ellipses are on both sides.]}$$

where $\phi : m \rightarrow n$ is a precanonical form. In this case, we write respectively ϕ as $Z : 0 \rightarrow 0$ (the identity morphism id_0), as $H^{m \rightarrow n} \phi' : m \rightarrow n + 1$, as $E^{m \rightarrow n} \phi' : m + 1 \rightarrow n$ or as $W_i^{m \rightarrow n} \phi' : m \rightarrow n$ (where i is the length of the stairs in the morphism). Algebraically,

$$Z = \text{id}_0 \quad E^{m \rightarrow n} \phi' = \varepsilon \otimes \phi' \quad H^{m \rightarrow n} \phi' = \eta \otimes \phi'$$

and

$$W_i^{m \rightarrow n} \phi' = (i \otimes \mu \otimes (n-1-i)) \circ (\gamma_i \otimes (n-i)) \circ (1 \otimes \phi') \circ (\delta \otimes (m-1))$$

Precanonical forms ϕ are thus the well formed morphisms (where compositions respect types) generated by the following grammar:

$$\phi ::= Z \mid H^{m \rightarrow n} \phi \mid E^{m \rightarrow n} \phi \mid W_i^{m \rightarrow n} \phi \quad (17)$$

In order to simplify the notation, we will remove the superscripts in the following and simply write $W_i \phi$ instead of $W_i^{m \rightarrow n} \phi$.

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

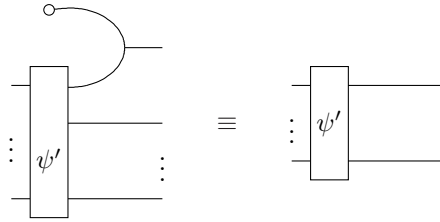
Lemma 8. *Every morphism $\phi : m \rightarrow n$ of \mathcal{B} is equivalent (wrt the relation \equiv) to a precanonical form.*

Proof. By induction on the size $|\phi|$ of ϕ .

- If $|\phi| = 0$ then $m = n$ and $\phi = \text{id}_n$. If $n = 0$ then $\phi = Z$. Otherwise, we have $\phi = \text{id}_{n+1} = 1 \otimes \text{id}_n = W_0 E H \text{id}_n$ and id_n is equivalent to a canonical form by induction on n .
- Otherwise, the morphism ϕ is of the form $\phi = \xi \circ \psi$ with $|\xi| = 1$ and $|\xi| + |\psi| = |\phi|$. By induction hypothesis, the morphism ψ is equivalent to a canonical form. Moreover, the morphism ξ is of the form $m_1 \otimes \pi \otimes m_2$ where π is either $\mu, \eta, \delta, \varepsilon$ or γ . We show the result by distinguishing these five cases for π and for each case by distinguishing whether the precanonical form of ψ is of the form $Z, H\psi', E\psi'$ or $W_i\psi'$.

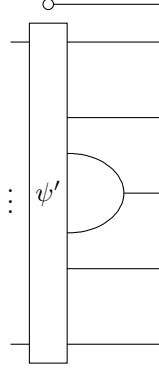
1. Suppose that $\pi = \mu$.

- (a) If $\psi = H\psi'$ then we distinguish two cases.
 - If $m_1 = 0$ then we have the equivalence



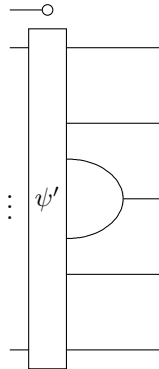
where ψ' is equivalent to a precanonical form by induction hypothesis.

– Otherwise, the morphism ϕ can be represented by



and is of the form $H(((m_1 - 1) \otimes \mu \otimes m_2) \circ \psi')$, where the morphism $((m_1 - 1) \otimes \mu \otimes m_2) \circ \psi'$ is equivalent to a pre-canonical form by induction hypothesis.

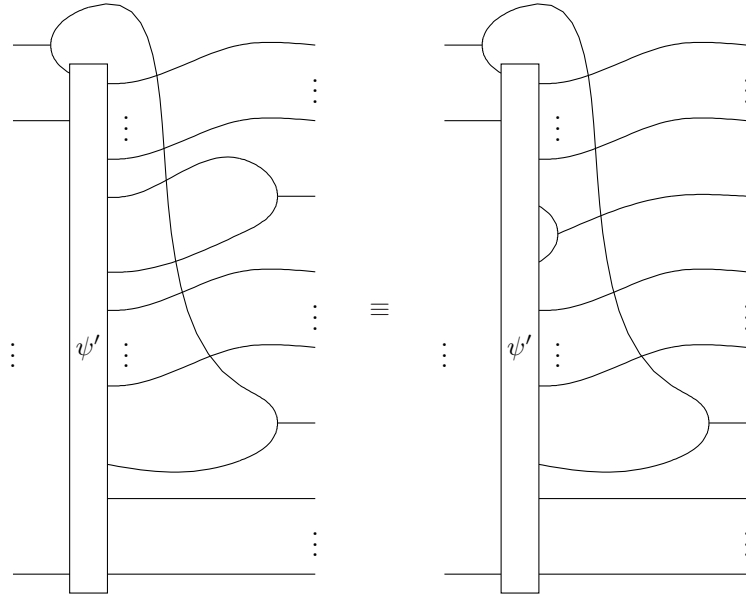
(b) If $\psi = E\psi'$ then the morphism ϕ can be represented by



and is of the form $E(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a pre-canonical form by induction hypothesis.

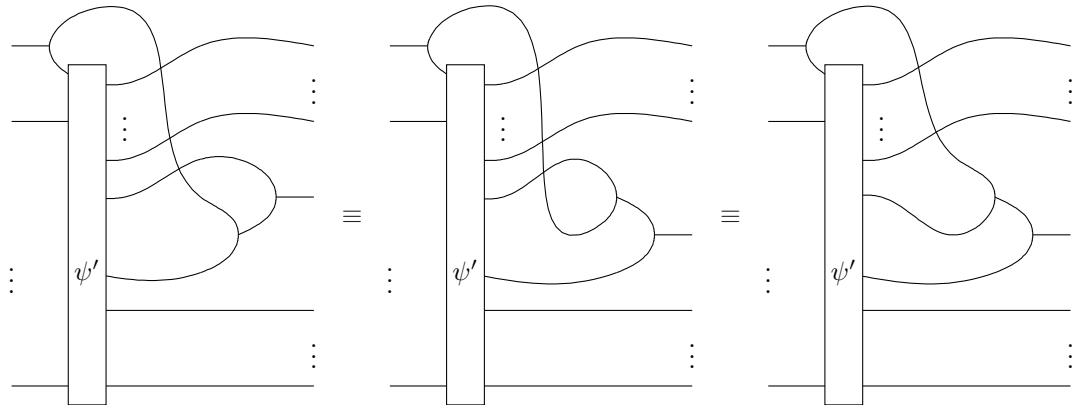
(c) If $\psi = W'_i \psi'$ then we distinguish four cases

– If $m_1 < i - 1$ then we have the equivalence



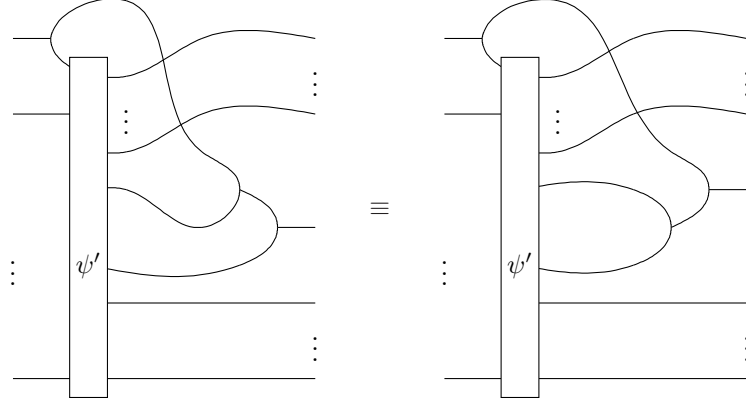
and ϕ is of the form $W_{i-1}((m_1 - 1 \otimes \mu \otimes m_2)) \circ \psi'$ where the morphism $((m_1 - 1 \otimes \mu \otimes m_2)) \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.

– If $m_1 = i - 1$ then we have the equivalences



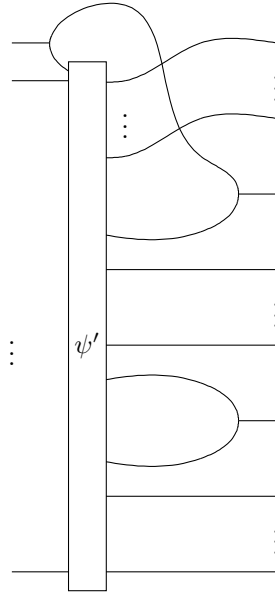
and we actually are in the case which is handled just below.

– If $m_1 = i$ then we have the equivalence



and ϕ is of the form $W_i(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.

– If $m_1 > i$ then ϕ can be represented by



and is of the form $W_i(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.

2. Suppose that $\pi = \eta$.

(a) If $\psi = Z$ then $\phi = HZ$ which is a precanonical form.

(b) If $\psi = H\psi'$ then we distinguish two cases.

– If $m_1 = 0$ then $\phi = HH\psi'$ which is a precanonical form.

– Otherwise, $\phi = H((m_1 - 1) \otimes \eta \otimes m_2) \circ \psi'$ where $(m_1 - 1) \otimes \eta \otimes m_2$ is equivalent to a precanonical form by induction hypothesis.

- (c) If $\psi = E\psi'$ then $\phi = E(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - (d) If $\psi = W_i\psi'$ then we distinguish two cases.
 - If $m_1 \leq i$ then $\phi \equiv W_{i+1}(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - Otherwise, $\phi = W_i(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
3. Suppose that $\pi = \delta$.
- (a) If $\psi = H\psi'$ then we distinguish two cases.
 - If $m_1 = 0$ then $\phi \equiv HH\psi'$ where ψ' is a precanonical form.
 - Otherwise, $\phi \equiv H((m_1 - 1) \otimes \delta \otimes m_2) \circ \psi'$ where $((m_1 - 1) \otimes \delta \otimes m_2) \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - (b) If $\psi = E\psi'$ then $\phi = E(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - (c) If $\psi = W_i\psi'$ then we distinguish three cases.
 - If $m_1 < i$ then $\phi \equiv W_{i+1}(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - If $m_1 = i$ then $\phi \equiv W_i W_{i+1}(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - Otherwise, $\phi = W_i(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
4. Suppose that $\pi = \varepsilon$.
- (a) If $\psi = H\psi'$ then we distinguish two cases.
 - If $m_1 = 0$ then $\phi \equiv \psi'$ where the morphism ψ' is a precanonical form.
 - Otherwise, $\psi = H((m_1 - 1) \otimes \varepsilon \otimes m_2) \circ \psi'$ where $((m_1 - 1) \otimes \varepsilon \otimes m_2) \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - (b) If $\psi = E\psi'$ then $\phi = E(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - (c) If $\psi = W_i\psi'$ then we distinguish three cases.
 - If $m_1 < i$ then $\phi \equiv W_{i-1}(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - If $m_1 = i$ then $\phi \equiv E(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - Otherwise, $\phi = W_i(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
5. Suppose that $\pi = \gamma$.
- (a) If $\psi = H\psi'$ then we distinguish two cases.
 - If $m_1 = 0$ then $\phi \equiv ((1 \otimes \eta \otimes m_2) \circ \psi')$ where the morphism $(1 \otimes \eta \otimes m_2) \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - Otherwise, $\phi = H(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.

- (b) If $\psi = E\psi'$ then $\phi = E(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
- (c) If $\psi = W_i\psi'$ then we distinguish four cases.
 - If $m_1 < i - 1$ then $\phi \equiv W_i(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - If $m_1 = i - 1$ then $\phi \equiv W_{i-1}(((m_1 + 1) \otimes \gamma \otimes m_2) \circ \psi')$ where the morphism $((m_1 + 1) \otimes \gamma \otimes m_2) \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - If $m_1 = i$ then $\phi \equiv W_{i+1}(((m_1 + 1) \otimes \gamma \otimes m_2) \circ \psi')$ where the morphism $((m_1 + 1) \otimes \gamma \otimes m_2) \circ \psi'$ is equivalent to a precanonical form by induction hypothesis.
 - Otherwise, $\phi = W_i(\xi \circ \psi')$ where the morphism $\xi \circ \psi'$ is equivalent to a precanonical form by induction hypothesis. \square

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

$$\begin{aligned}
HW_i &\Longrightarrow W_{i+1}H \\
HE &\Longrightarrow EH \\
W_iW_j &\Longrightarrow W_jW_i \quad \text{when } i < j
\end{aligned} \tag{18}$$

when considered as words generated by the grammar (17). It is routine verifications to show that two precanonical forms ϕ and ψ such that ϕ rewrites to ψ are equivalent. This rewriting system thus provides us with a notion of canonical form for precanonical forms:

Lemma 9. *The rewriting system (18) is normalizing.*

Proof. We first show that the rewriting system is terminating by defining an interpretation of precanonical forms into $\mathbb{N} \times \mathbb{N}$, ordered lexicographically. This interpretation $\llbracket - \rrbracket$ is defined on generators by

$$\llbracket Z \rrbracket = (0, 0) \quad \llbracket H \rrbracket = (0, 0) \quad \llbracket E \rrbracket = (1, 0) \quad \llbracket W_i \rrbracket = (1, i)$$

and on composition and identities by

$$\llbracket G \circ F \rrbracket = (\llbracket G \rrbracket_1 + 2 \times \llbracket F \rrbracket_1, \llbracket G \rrbracket_2 + 2 \times \llbracket F \rrbracket_2) \quad \text{and} \quad \llbracket \text{id} \rrbracket = (0, 0)$$

where F and G are such that $\llbracket F \rrbracket = (\llbracket F \rrbracket_1, \llbracket F \rrbracket_2)$ and $\llbracket G \rrbracket = (\llbracket G \rrbracket_1, \llbracket G \rrbracket_2)$. It can be remarked that the rules are strictly decreasing wrt this interpretation:

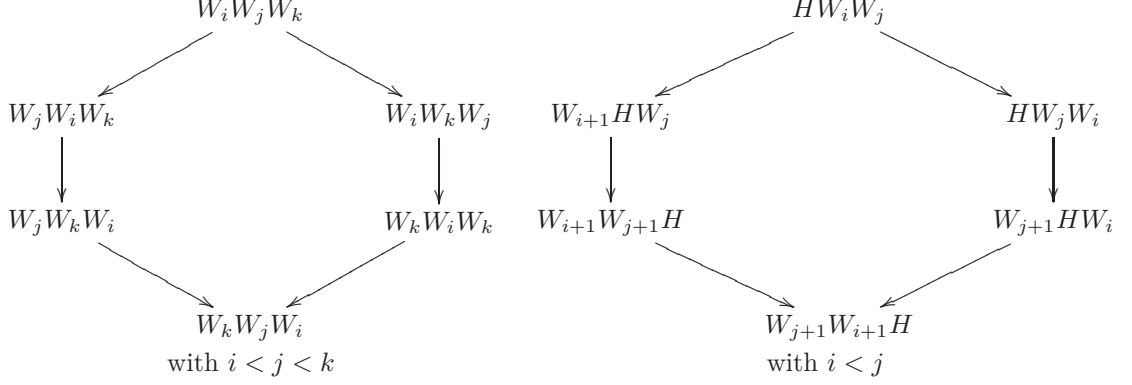
$$\llbracket HW_i \rrbracket = (2, 2i) > (1, i) = \llbracket W_iH \rrbracket \quad \llbracket HE \rrbracket = (2, 0) > (1, 0) = \llbracket EH \rrbracket$$

and

$$\llbracket W_iW_j \rrbracket = (3, i + 2j) > (3, j + 2i) = \llbracket W_jW_i \rrbracket$$

The rewriting system is therefore terminating. It moreover locally confluent,

since the two critical pairs are joinable:



The rewriting system being terminating, it is thus confluent. \square

Remark 10. Canonical forms are the precanonical forms of the form

$$W_{i_{k_n}^n} \cdots W_{i_1^n} E \cdots \cdots W_{i_{k_1}^1} \cdots W_{i_1^1} E H \cdots H Z \quad (19)$$

with $i_1^p \geq \dots \geq i_{k_p}^p$, for every p such that $1 \leq p \leq n$.

From Lemmas 8 and 9, we can finally deduce that every morphism of the category \mathcal{B} is equivalent to a unique canonical form.

Lemma 11. *The interpretation functor $I/\equiv : \mathcal{B}/\equiv \rightarrow \mathbf{MRel}$ is full.*

Proof. We show the result by showing that the functor $I : \mathcal{B} \rightarrow \mathbf{MRel}$ is full, i.e. that every multirelation $R : m \rightarrow n$ is the image of a precanonical form $\phi : m \rightarrow n$ in \mathcal{B} , by induction on m and on the cardinal $|R|$ of R .

1. If $m = 0$ then R is the interpretation of the precanonical form $H \dots H Z$, with n occurrences of H .
2. If $m > 0$ and for every $j < n$, $R(0, j) = 0$ then R is of the form $R = R^\varepsilon \otimes R'$, where $R' : m - 1 \rightarrow n$ is the multirelation such that $R'(i, j) = R(i + 1, j)$. By induction hypothesis, R' is the interpretation of a precanonical form ϕ' and R is therefore the interpretation of the precanonical form $E\phi'$.
3. Otherwise, we necessarily have $n \neq 0$ and there exists an index k' such that $R(0, k') \neq 0$. We write k for the greatest such index. The multirelation R is of the form

$$R = (k \otimes R^\mu \otimes n - 1 - k) \circ (R^{\gamma^k} \otimes n - k) \circ (1 \otimes R') \circ (R^\delta \otimes m - 1)$$

Where $R' : m \rightarrow n$ is the multirelation defined by $R'(0, k) = R(0, k) - 1$ and $R'(i, j) = R(i, j)$ for every $(i, j) \neq (0, k)$. The multirelation R' is thus of cardinal $|R'| = |R| - 1$ and is the interpretation of a precanonical form $\phi' : m \rightarrow n$ by induction hypothesis. Finally, R is the interpretation of the precanonical form $W_k \phi'$. \square

The proof of the previous lemma provides us with an algorithm which, given a multirelation R , builds a precanonical form ϕ whose interpretation is R . The execution of this algorithm consists in enumerating the coefficients of the multirelation column after column. We suppose given a multirelation $R : m \rightarrow n$. In pseudo-code, the algorithm can be written as follows:

```

for  $i = 0$  to  $m - 1$  do
  for  $j = n - 1$  downto  $0$  do
    for  $k = 0$  to  $R(i, j)$  do
      print " $W_j$ "
    done
  print " $H$ "
done
done
for  $j = 0$  to  $n - 1$  do
  print " $E$ "
done
print " $Z$ "

```

The word printed by the algorithm will be a precanonical form whose interpretation is R .

Knowing the general form (19) of canonical forms, it is easy to show that the precanonical form produced by the algorithm are actually canonical forms. Conversely, every canonical form (19) can be read as an “enumeration” of the coefficients of a multirelation in a way similar the previous algorithm. This shows that, in fact, multirelations $R : m \rightarrow n$ are in bijection with the canonical forms $\phi : m \rightarrow n$. A morphism of \mathcal{B} being equivalent to an unique canonical form, we finally deduce that

Theorem 12. *The categories \mathcal{B}/\equiv and \mathbf{MRel} are isomorphic, i.e. the category \mathbf{MRel} of natural numbers and multirelations is presented by the 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 $R_1, R_2 : m \rightarrow n$ are equivalent when they have the same null coefficients. We can therefore easily adapt the previous presentation to show that

Theorem 13. *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

$$W_i W_i \Longrightarrow W_i \tag{20}$$

to the rewriting system (18), which remains normalizing.

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, \dots with given arities,
- a set of function symbols f, g, \dots with given arities,
- and a set of first-order variables x, y, \dots

Terms t and *formulas* A are respectively generated by the following grammars:

$$\begin{aligned} t & ::= x \mid f(t, \dots, t) \\ A & ::= P(t, \dots, t) \mid \forall x.A \mid \exists x.A \end{aligned}$$

(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 (so that the obtained logic has the cut-elimination property). The logic associated to these formulas has the following inference rules:

$$\begin{array}{c} \frac{A[t/x] \vdash B}{\forall x.A \vdash B} (\forall\text{-L}) \qquad \frac{A \vdash B}{A \vdash \forall x.B} (\forall\text{-R}) \\ \text{(with } x \text{ not free in } A) \\ \\ \frac{A \vdash B}{\exists x.A \vdash B} (\exists\text{-L}) \qquad \frac{A \vdash B[t/x]}{A \vdash \exists x.B} (\exists\text{-R}) \\ \text{(with } x \text{ not free in } B) \\ \\ \frac{(P, Q) \in Ax}{P \vdash Q} (\text{Ax}) \qquad \frac{A \vdash B \quad B \vdash C}{A \vdash C} (\text{Cut}) \end{array}$$

Games and strategies. Games are defined as follows.

Definition 14. A game $A = (M_A, \lambda_A, \leq_A)$ consists of a set M_A whose elements are called moves, a function λ_A from M_A to $\{-1, +1\}$ which to every move m associates its polarity, and a partial order \leq_A on moves, called causality or justification, which should be well-founded, i.e. such that every move $m \in M_A$ defines a finite downward closed set

$$m \downarrow = \{ n \in M_A \mid n \leq_A m \}$$

A move m is said to be a Proponent move when $\lambda_A(m) = +1$ and an Opponent move otherwise.

The size $|A|$ of a game A is the cardinal of its set of moves M_A .

Remark 15. More generally, games should be defined as event structures [Win87] in order to be able to model additive connectives. We don't detail this here since we only consider formulas without connectives.

If A and B are two games, their tensor product $A \otimes B$ is defined by disjoint union on moves, polarities and causality:

$$M_{A \otimes B} = M_A \uplus M_B, \quad \lambda_{A \otimes B} = \lambda_A + \lambda_B \quad \text{and} \quad \leq_{A \otimes B} = \leq_A \cup \leq_B$$

The opposite game A^* of the game A is obtained from A by inverting polarities of moves:

$$A^* = (M_A, -\lambda_A, \leq_A).$$

Finally, 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 16. A strategy σ on a game A is a partial order \leq_σ on the moves of A which satisfies the two following properties:

1. polarity: for every pair of moves $m, n \in M_A$,

$$m <_\sigma n \quad \text{implies} \quad \lambda_A(m) = -1 \quad \text{and} \quad \lambda_A(n) = +1$$

2. acyclicity: the partial order \leq_σ 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_σ .

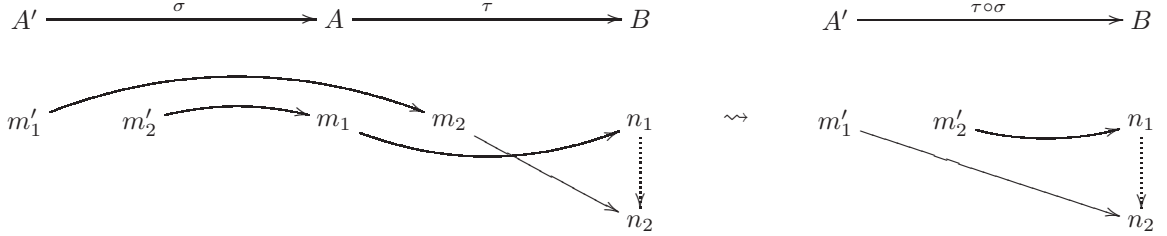
A category of games. At this point it would be very tempting to build a category whose

- objects are games,
- morphisms $\sigma : A \rightarrow B$ are strategies on the game $A \multimap B$.

The identity strategy $\text{id}_A : A' \rightarrow A$ (the apostrophe sign is only used here to identify unambiguously the two copies of A) would be the strategy such that for every move m in A and m' in A' , which are instances of a same move m , we have $m' \leq_{\text{id}_A} m$ whenever $\lambda_A(m) = +1$ and $m \leq_{\text{id}_A} m'$ whenever $\lambda_A(m) = -1$ (it can easily be checked that this definition satisfies the axioms for strategies). Now consider two strategies $\sigma : A \rightarrow B$ and $\tau : B \rightarrow C$. The partial order \leq_σ on the set $M_A \uplus M_B$ is relation on $M_A \uplus M_B$, i.e. a subset of $(M_A \uplus M_B)^2$, and similarly for τ . The partial order $\leq_{\tau \circ \sigma}$ corresponding to composite $\tau \circ \sigma : A \rightarrow C$ of the two strategies σ and τ would be defined as the transitive closure of the relation $\leq_\sigma \cup \leq_\tau$ on $M_A \uplus M_B \uplus M_C$ restricted to the set $M_A \uplus M_C$. It is easily checked that identities act as neutral elements for composition. Similar ideas for composing strategies were in particular developed in the appendix of [HS02].

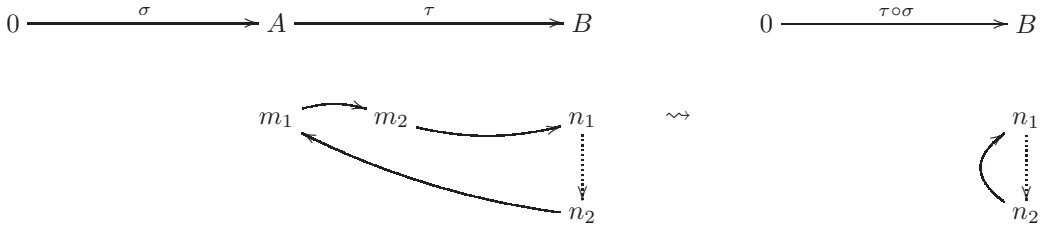
For example, consider the game A with two Proponent moves m_1 and m_2 and the empty causality relation, the game B with two Proponent moves n_1 and n_2 and the causality relation $n_1 \leq_B n_2$, the strategy $\sigma : A' \rightarrow A$ such that $m'_1 \leq_\sigma m_2$ and $m'_2 \leq_\sigma m_1$ and the strategy $\tau : A \rightarrow B$ such that $m_1 \leq_\tau n_1$

and $m_2 \leq_\tau n_2$. Their composite is the strategy $\tau \circ \sigma : A' \rightarrow B$ such that $m'_2 \leq_{\tau \circ \sigma} n_1$ and $m'_1 \leq_{\tau \circ \sigma} n_2$. This can be viewed graphically as follows:



In the diagram above the dotted arrows represent the causal dependencies in the games and solid arrows the dependencies in the strategies.

However, the composite of two strategies is not necessarily a strategy! For example consider the game A defined as before excepted that m_1 is now an Opponent move, the game B defined as before excepted that n_2 is now an Opponent move, the strategy $\sigma : 0 \rightarrow A$ (where 0 denotes the empty game) such that $m_1 \leq_\sigma m_2$ and the strategy $\tau : A \rightarrow B$ such that $n_2 \leq_\tau m_1$ and $m_2 \leq_\tau n_1$. Their “composite” is *not* a strategy because it does not satisfy the acyclicity property:



This is a typical example of the fact that compositionality of strategies in game semantics is often a subtle property that should be checked very carefully.

Remark 17. A more conceptual explanation of this compositionality problem can be given as follows. If we write P for the game with only one Proponent move, the game A should correspond, in a model of linear logic to either the tensor or the par of P and P^* . However, we have not included in our strategies conditions which are necessary to distinguish between the interpretation of tensor and par. This explains why we are not able to recover the compositionality of the acyclicity property, which is deeply linked with the correctness criterion of linear logic. We leave a precise investigation of this for future works, in which we plan to extend our model to first-order linear logic.

Fortunately, if we restrict the previous attempt of construction of a category, by only allowing *finite filiform games* as objects, then we actually construct a category (i.e. the composite of two morphisms is a morphism) that we write **Games**. Moreover, we show that the connective-free fragment of first-order propositional logic can be interpreted in this category and that the conditions imposed on strategies characterize exactly the strategies interpreting proofs (Theorem 26).

We could give a direct proof of the fact that **Games** is actually a category. However, a direct proof of the fact that the composite of two acyclic strategies is

acyclic is combinatorial, lengthy and requires global reasoning about strategies. This proof would show, by *reductio ad absurdum*, that if the composite of two strategies contains a cycle (together with the causality of the game) then one of the strategies already contains a cycle. So, it would moreover not be very satisfactory in the sense that it would not be constructive. Instead of proceeding in this way, we define the category **Games** in an abstract fashion, construct a presentation of this category, and conclude *a posteriori* that in fact its only morphisms are strategies, which implies in particular (Theorem 25) that strategies do actually compose!

We first define a weaker notion of strategy

Definition 18. *A cyclic strategy σ on a game A is a relation on the moves of A , i.e. a subset of $M_A \times M_A$, such that*

1. *the relation σ is reflexive and transitive,*
2. *polarity: for every pair of moves $m, n \in M_A$,*

$$m \sigma n \quad \text{and} \quad m \neq n \quad \text{implies} \quad \lambda_A(m) = -1 \quad \text{and} \quad \lambda_A(n) = +1$$

In particular, every strategy is a cyclic strategy. From this definition it is very easy to build a category **CGames** whose

- objects are games,
- morphisms $\sigma : A \rightarrow B$ are strategies on the game $A \multimap B$,
- identities and composition are defined as above.

Since the definition of cyclic strategy is much weaker than the notion of strategy, it is routine to check that the category is well-defined. We now define the category **Games** as the category generated in **CGames** by finite filiform games and strategies, i.e. the smallest category whose

- objects are finite filiform games,
- for every objects A and B , and every strategy $\sigma : A \multimap B$ in the sense of Definition 16, we have that σ is a morphism in $\text{Hom}(A, B)$,
- for every objects A, B and C , if σ is a morphism in $\text{Hom}(A, B)$ and τ is a morphism in $\text{Hom}(B, C)$ then their composite $\tau \circ \sigma$ (in the category **CGames**) is a morphism in $\text{Hom}(A, C)$.

As mentioned above, we will show in Theorem 25 that the only morphisms of this category are actually strategies.

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

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

This operation is extended as a bifunctor on strategies as follows. If $\sigma : A \rightarrow B$ and $\tau : C \rightarrow D$ are two strategies, the strategy $\sigma \otimes \tau : A \otimes C \rightarrow B \otimes D$ is defined

as the relation $\leq_{\sigma \otimes \tau} = \leq_{\sigma} \uplus \leq_{\tau}$. This bifunctor induces a monoidal structure $(\mathbf{Games}, \otimes, I)$ on the category \mathbf{Games} , where I denotes the empty game.

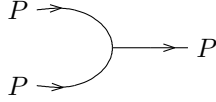
We write O for a game with only one Opponent move and P for a game with only one Proponent move. It can be easily remarked that finite filiform games A are generated by the following grammar

$$A ::= I \mid O \otimes A \mid P \otimes A$$

A game $X_1 \otimes \cdots \otimes X_n \otimes I$ where the X_i are either O or P is represented graphically as

$$\begin{array}{c} X_1 \\ \vdots \\ X_n \end{array}$$

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



is the strategy on the game $(O \otimes O) \otimes P$ 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 $\varepsilon^P : P \rightarrow I$, drawn as

$$P \longrightarrow \circ$$

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.

A game semantics. A formula A is interpreted as a filiform game $\llbracket A \rrbracket$ by

$$\llbracket P \rrbracket = I \quad \llbracket \forall x.A \rrbracket = O \otimes \llbracket A \rrbracket \quad \llbracket \exists x.A \rrbracket = P \otimes \llbracket A \rrbracket$$

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

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

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

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

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

respectively drawn as

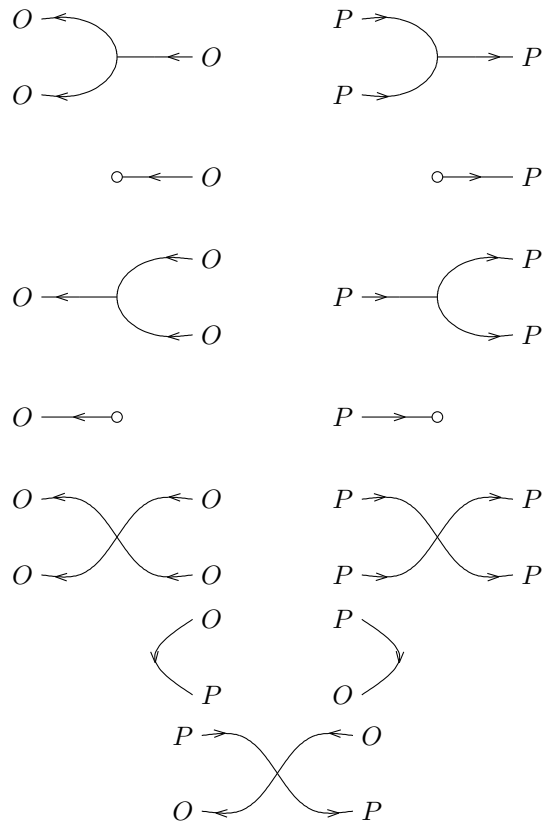


Figure 1: Generators of the strategies.

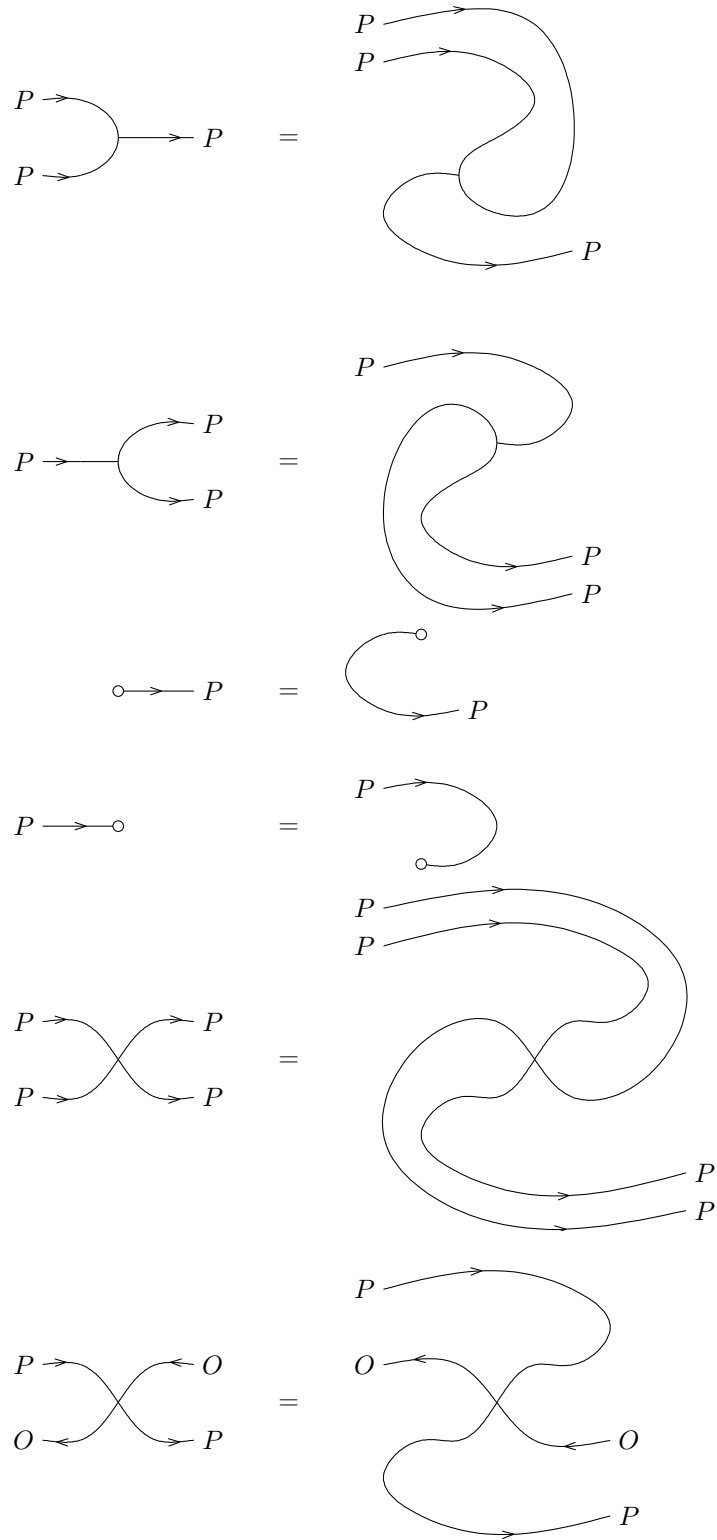


Figure 2: Proponent is left dual to Opponent.

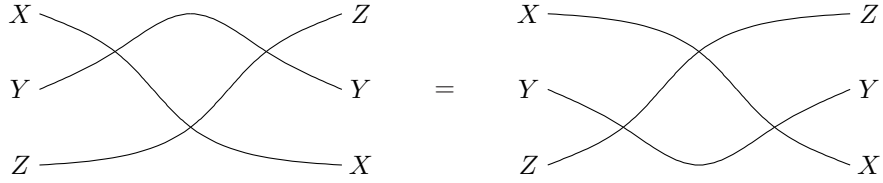
and

$$\frac{\frac{\frac{}{\top \vdash y = y}(\text{Ax})}{\top \vdash \exists z. y = z}(\exists\text{-R})}{\top \vdash \forall y. \exists z. y = z}(\forall\text{-R}) \quad \frac{\frac{\frac{\frac{}{0 = z \vdash z = 0}(\text{Ax})}{0 = z \vdash \exists x. x = 0}(\exists\text{-R})}{\exists z. 0 = z \vdash \exists x. x = 0}(\exists\text{-L})}{\forall y. \exists z. y = z \vdash \exists x. x = 0}(\exists\text{-L})}{\top \vdash \exists x. x = 0}(\text{Cut})$$

and the second proof reduces to the first one by cut-elimination.

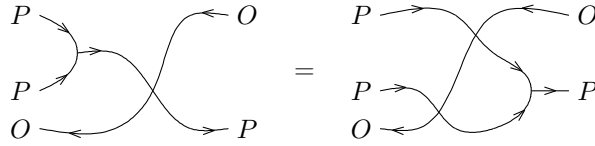
Lemma 22. *With the notations of 20, we have:*

- $(P, \mu^P, \eta^P, \delta^P, \varepsilon^P, \gamma^P)$ is a qualitative bicommutative bialgebra,
- the Yang-Baxter equalities

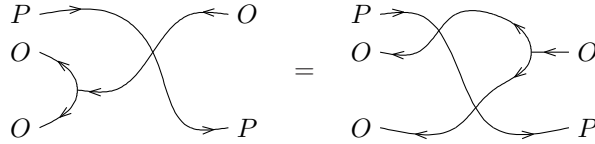


hold whenever (X, Y, Z) is either (O, O, O) , (P, O, O) , (P, P, O) or (P, P, P) ,

- the equalities

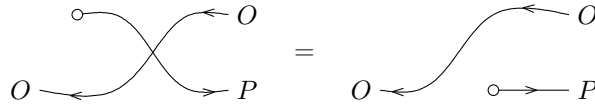


and

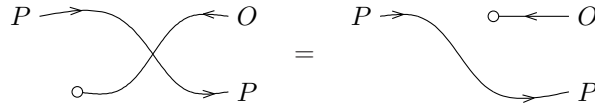


hold (and dually for comultiplications),

- the equalities

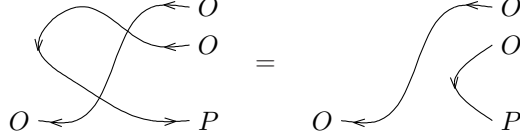


and

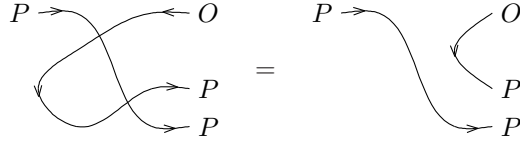


hold (and dually for counits),

– the equalities



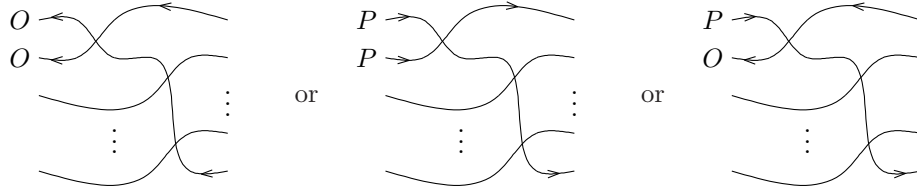
and



hold (and dually for the counit of duality).

We can now proceed as in Section 3 to show that the theory \mathfrak{G} introduced in Definition 20 presents the category **Games**. First, in the category **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 (16): a *stair* is either id_O or id_P or



The notion of *precanonical form* ϕ is now defined inductively as shown in Figure 3, 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

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

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 (18) into a rewriting system for

ϕ is either empty or

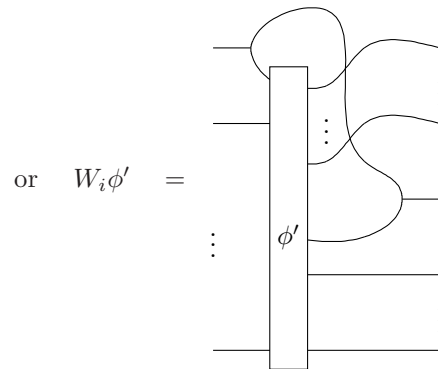
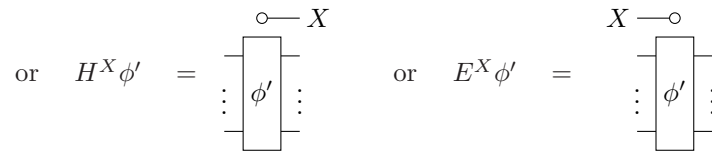
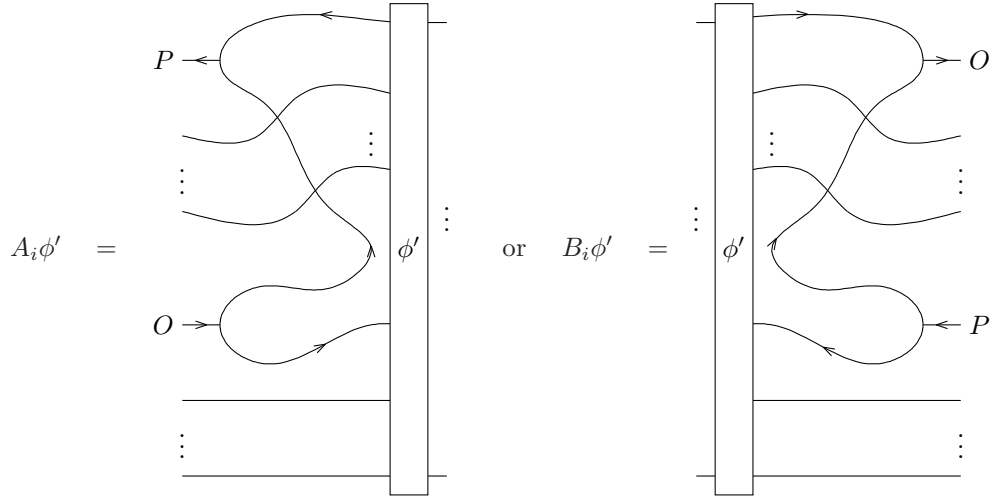


Figure 3: Precanonical forms for strategies.

precanonical forms, by adding the rules

$$\begin{array}{llll}
H^X W_i & \Longrightarrow & W_{i+1} H^X & \\
H^X E^Y & \Longrightarrow & E^Y H^X & \\
W_i W_j & \Longrightarrow & W_j W_i & \text{when } i < j \\
W_i W_i & \Longrightarrow & W_i & \\
H^X A_i & \Longrightarrow & A_i H^X & \\
A_i W_j & \Longrightarrow & W_j A_i & \\
A_i A_j & \Longrightarrow & A_j A_i & \text{when } i < j \\
A_i A_i & \Longrightarrow & A_i & \\
E^X B_i & \Longrightarrow & E^X & \\
B_i W_j & \Longrightarrow & W_j B_i & \\
B_i B_j & \Longrightarrow & B_j B_i & \text{when } i < j \\
B_i B_i & \Longrightarrow & B_i & \\
B_i A_j & \Longrightarrow & A_j B_i &
\end{array}$$

to the rewriting system containing the rules (18) and (20). It is simple to extend the proof of Lemma 9 in order to show that this rewriting system is normalizing. The general form for canonical forms is

$$\begin{aligned}
W_{i_{k_n}^n} \cdots W_{i_1^n} A_{j_{i_n}^n} \cdots A_{j_1^n} E \cdots W_{i_{k_1}^1} \cdots W_{i_1^1} A_{j_{l_1}^1} \cdots A_{j_1^1} E \\
\cdots B_{h_{m_p}^p} \cdots B_{h_1^p} H \cdots B_{h_{m_1}^1} \cdots B_{h_1^1} H Z
\end{aligned} \quad (23)$$

with

- $i_{k_p}^p > \dots > i_1^p$ for every integer r such that $1 \leq r \leq k_n$,
- $j_{i_p}^p > \dots > j_1^p$ for every integer r such that $1 \leq r \leq l_n$,
- $h_{i_p}^p > \dots > h_1^p$ for every integer r such that $1 \leq r \leq m_n$.

Lemma 23. *Every strategy $\sigma : A \rightarrow B$ is the interpretation of an unique canonical form.*

Proof. We show that every strategy $\sigma : A \rightarrow B$ is the interpretation of a precanonical form $\phi : A \rightarrow B$ by induction on the triple $(|A|, |\sigma|, |B|)$, ordered lexicographically.

1. If $A = B = I$ then σ is the interpretation of the precanonical form Z .
2. If $A = I$ and $B = X \otimes B'$, where X is either P or O then we distinguish two cases.
 - If no move depends on X in the strategy, this strategy is the image of a precanonical form $H_X \phi'$, where ϕ' is a precanonical form, obtained by induction hypothesis whose interpretation is the strategy $\sigma' : I \rightarrow B'$ obtained by restricting σ to the codomain B (the size of σ' is $|\sigma'| = |\sigma|$).
 - Otherwise, we write i for the index in B of the move of minimal index which depends on X in the strategy. The strategy is the image of a precanonical form $B_i \phi'$, where ϕ' is precanonical form, obtained by induction hypothesis, whose interpretation is the strategy $\sigma' : I \rightarrow B$ obtained from σ by removing the dependency of the i -th move of B on the first move of B (its size is such that $|\sigma'| < |\sigma|$).

3. If $A = X \otimes A'$, where X is either P or O , then we distinguish three cases.
- If no move depends on X in the strategy, this strategy is the image of a precanonical form $E^X \phi'$, where ϕ' is a precanonical form, obtained by induction hypothesis, whose interpretation is the strategy $\sigma' : A' \rightarrow B$ obtained by restricting σ to the domain A' .
 - If there exists a move of X which depends on X , we write i for the index in A of such a move of minimal index. The strategy is the interpretation of a precanonical form $A_i \phi'$, where ϕ' is a precanonical form, obtained by induction hypothesis, whose interpretation is the strategy $\sigma' : A \rightarrow B$ obtained from σ by removing the dependency of the i -th move of A on the first move of A (its size is such that $|\sigma'| < |\sigma|$).
 - Otherwise, there exists a move in B which depends on the move X . We write i of the index in B of such a move of minimal index. The strategy is the interpretation of a precanonical form $W_i \phi'$, where ϕ' is a precanonical form, obtained by induction hypothesis, whose interpretation is the strategy $\sigma' : A \rightarrow B$, obtained from σ by removing the dependency of the i -th move of B on the first move of A (its size is such that $|\sigma'| < |\sigma|$).

Knowing the general form (23) of canonical forms, it is easy to show that the precanonical forms thus constructed are actually canonical and that canonical forms $\phi : A \rightarrow B$ are in bijection with strategies $\sigma : A \rightarrow B$, as in the proof of Theorem 12. \square

We therefore deduce the main theorem of this article:

Theorem 24. *The monoidal category **Games** (with the \otimes tensor product) is presented by the equational theory \mathfrak{G} .*

As a direct consequence of this Theorem, we deduce the two following properties which show the technical benefits of our construction.

Theorem 25. *The composite of two strategies, in the sense of Definition 16, is itself a strategy (in particular, the acyclicity property is preserved by composition).*

Proof. Two strategies $\sigma : A \rightarrow B$ and $\tau : B \rightarrow C$ can be seen as morphisms $\tilde{\sigma}$ and $\tilde{\tau}$ the category \mathcal{G}/\equiv and the image of their composite is $\widetilde{\tau \circ \sigma} = \tilde{\tau} \circ \tilde{\sigma}$, which corresponds to the image of an unique acyclic strategy. \square

Theorem 26. *The strategies of **Games** are definable (when the set Ax of axioms is reasonably large enough): it is enough to check that generators are definable – for example, the first case of (21) shows that μ^P is definable.*

Proof. Suppose that there is a countable number of variable symbols. Suppose moreover that there exists a unary propositional symbol I , which enables us to see every term t as a proposition $I(t)$, which we will simply write t by abuse of notation. We also suppose that the set of propositions contains two nullary propositions \top and \perp and is closed under formal conjunctions and disjunctions: if we have that $P(x_1, \dots, x_n)$ and $Q(y_1, \dots, y_m)$ are propositions

then $P(x_1, \dots, x_n) \wedge Q(y_1, \dots, y_m)$ and $P(x_1, \dots, x_n) \vee Q(y_1, \dots, y_m)$ are also propositions. We then define a set Ax of axioms as the smallest set of pairs of propositions which is reflexive, transitive and such that:

- for every proposition P ,
 - $(P, \top) \in Ax$,
 - $(\perp, P) \in Ax$,
- for every propositions P, P_1 and P_2 ,
 - if $(P, P_1) \in Ax$ and $(P, P_2) \in Ax$ then $(P, P_1 \wedge P_2) \in Ax$,
 - if $(P, P_1) \in Ax$ or $(P, P_2) \in Ax$ then $(P, P_1 \vee P_2) \in Ax$,
 - if $(P_1, P) \in Ax$ or $(P_2, P) \in Ax$ then $(P_1 \wedge P_2, P) \in Ax$,
 - if $(P_1, P) \in Ax$ and $(P_2, P) \in Ax$ then $(P_1 \vee P_2, P) \in Ax$.

(for concision, we did not mention the arguments of propositions). By Theorem 24, every strategy can be expressed as a tensor and composite of the generating strategies pictured in Figure 1. It is therefore enough to show that those strategies are definable.

- the strategies μ^P and η^P are the respective interpretations of the proofs

$$\frac{\frac{\frac{}{x \wedge y \vdash x \wedge y}(\text{Ax})}{x \wedge y \vdash \exists z.z}(\exists\text{-R})}{\exists y.x \wedge y \vdash \exists z.z}(\exists\text{-L})}{\exists x.\exists y.x \wedge y \vdash \exists z.z}(\exists\text{-L}) \quad \text{and} \quad \frac{\frac{\frac{}{\top \vdash \top}(\text{Ax})}{\top \vdash \exists x.x}(\exists\text{-R})}{}{}$$

- the strategies δ^P and ε^P are the respective interpretations of the proofs

$$\frac{\frac{\frac{\frac{}{x \vdash x \wedge x}(\text{Ax})}{x \vdash \exists z.x \wedge z}(\exists\text{-R})}{x \vdash \exists y.\exists z.y \wedge z}(\exists\text{-R})}{\exists x.x \vdash \exists y.\exists z.y \wedge z}(\exists\text{-L}) \quad \text{and} \quad \frac{\frac{\frac{}{x \vdash \top}(\text{Ax})}{\exists x.x \vdash \top}(\exists\text{-L})}{}{}$$

- the strategies η^{OP} and ε^{OP} are the respective interpretations of the proofs

$$\frac{\frac{\frac{\frac{}{\top \vdash x \vee (x \vee \top)}(\text{Ax})}{\top \vdash \exists y.x \vee y}(\exists\text{-R})}{\top \vdash \forall x.\exists y.x \vee y}(\forall\text{-R}) \quad \text{and} \quad \frac{\frac{\frac{\frac{}{x \wedge (x \wedge \perp) \vdash \perp}(\text{Ax})}{\forall y.x \wedge y \vdash \perp}(\forall\text{-L})}{\exists x.\forall y.x \wedge y \vdash \perp}(\exists\text{-L})}{}{}$$

- the strategies γ^P and γ^{OP} are the respective interpretations of the proofs

$$\frac{\frac{\frac{\frac{\frac{}{x \wedge y \vdash x \wedge y}(\text{Ax})}{x \wedge y \vdash \exists t.t \wedge y}(\exists\text{-R})}{x \wedge y \vdash \exists z.\exists t.t \wedge z}(\exists\text{-L})}{\exists y.x \wedge y \vdash \exists z.\exists t.t \wedge z}(\exists\text{-L})}{\exists x.\exists y.x \wedge y \vdash \exists z.\exists t.t \wedge z}(\exists\text{-L}) \quad \text{and} \quad \frac{\frac{\frac{\frac{\frac{}{x \wedge z \vdash x \wedge z}(\text{Ax})}{x \wedge z \vdash \exists t.t \wedge z}(\exists\text{-R})}{\forall y.x \wedge y \vdash \exists t.t \wedge z}(\forall\text{-L})}{\exists x.\forall y.x \wedge y \vdash \exists t.t \wedge z}(\exists\text{-L})}{\exists x.\forall y.x \wedge y \vdash \forall z.\exists t.t \wedge z}(\forall\text{-R})}{}{}$$

– etc.

□

A given strategy is not necessarily the interpretation of a unique proof. In particular, as explained in the introduction, two proofs which only differ by the order of introduction of some successive connectives are identified in the semantics.

In the preceding proof, we could of course have taken the set of all pairs of propositions as set Ax of axioms. The set that we have used shows however that our definability result can be obtained with a reasonable set of axioms: it is in particular *coherent*, which means that there exists a sequent which cannot be proved (the sequent $\top \vdash \perp$ for example), which would not have been the case with the trivial set of axioms.

5 Conclusion

We have constructed a game semantics for first-order propositional logic and given a presentation of the category **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: games would be modeled as trees of connectives and strategies as “surface diagrams” between these trees. It would be particularly interesting to do this for the multiplicative fragment of linear logic (MLL) with first-order quantifiers since it would provide us with a local reformulation of the Danos-Regnier criterion for MLL extended with the MIX rule (this is hinted in Remark 17).

Some of the proofs (such as the proof of Lemma 8) are very repetitive, which we think is a good point: we believe that they could be mechanically checked or automated. It turns out that it is quite difficult to find a good representation of morphisms in monoidal categories, which is suitable for a computer to manipulate them without having to handle complex congruences such as the exchange law. We have proposed such a representation as well as an unification algorithm for monoidal rewriting systems [Mim10], but many properties and generalizations of these techniques remain to be investigated in order to have really useful tools. Formulated in categorical terms this amounts to generalize term rewriting techniques from Lawvere theories (which are categories with products, thus monoidal categories, thus 2-categories with one object) to the general setting of 2-categories. In particular, 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 [Laf03], for monoids and commutative monoids, etc., but for example finding a strongly normalizing rewriting system presenting the theory of bialgebras is a difficult problem [Mim08], not to

mention a strongly normalizing presentation of our category of games. Such a presentation would have a very high number of critical pairs which makes us see the development of automated tools to compute them a necessary preliminary step.

Finally, there is a striking analogy between the string diagrams we have used and wires in electronic circuits. This is actually one of the starting point of the current work of Ghica (as well as game semantics), who is currently elaborating a compiler from a high-level language into integrated circuits [Ghi07]. The categorical string-diagrammatic axioms reveal to be crucial in this setting in order to establish designing principles for the circuits. Following this point of view, we believe that a deep understanding of the algebraic structure of categories of semantics of programming languages will prove very useful in order to design and optimize circuits implementing programs in these languages.

Acknowledgments. I would like to thank Martin Hyland and Paul-André Mellies, as well as John Baez, Albert Burroni, Jonas Frey, Yves Guiraud, Yves Lafont, François Métayer and Luke Ong, for the lively discussion we had, during which I learned so much; I also thank the anonymous referee for valuable suggestions.

References

- [BL03] J. Baez and L. Langford. Higher-dimensional algebra IV: 2-tangles. *Advances in Mathematics*, 180(2):705–764, 2003.
- [Bur93] A. Burroni. Higher-dimensional word problems with applications to equational logic. *TCS*, 115(1):43–62, 1993.
- [Ghi07] D.R. Ghica. Geometry of synthesis: a structured approach to VLSI design. In *Proceedings of the 34th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, page 375. ACM, 2007.
- [HO00] M. Hyland and L. Ong. On Full Abstraction for PCF: I, II, III. *Information and Computation*, 163(2):285–408, 2000.
- [HP00] M. Hyland and J. Power. Symmetric Monoidal Sketches. In *Proceedings of PPDP'00*, pages 280–288, 2000.
- [HS97] J. Hintikka and G. Sandu. *Game-theoretical semantics*. 1997.
- [HS02] M. Hyland and A. Schalk. Games on Graphs and Sequentially Realizable Functionals. *Proceedings of the 17th IEEE Symposium on Logic in Computer Science*, pages 257–264, 2002.
- [JS91] A. Joyal and R. Street. The Geometry of Tensor Calculus, I. *Advances in Mathematics*, 88:55–113, 1991.
- [Lac04] S. Lack. Composing PROPs. *Theory and Applications of Categories*, 13(9):147–163, 2004.
- [Laf95] Y. Lafont. Equational Reasoning with 2-Dimensional Diagrams. *Term Rewriting*, pages 170–195, 1995.

- [Laf03] Y. Lafont. Towards an Algebraic Theory of Boolean Circuits. *J. Pure Appl. Algebra*, 184(2-3):257–310, 2003.
- [Law63] F. W. Lawvere. *Functorial Semantics of Algebraic Theories and Some Algebraic Problems in the context of Functorial Semantics of Algebraic Theories*. PhD thesis, 1963.
- [Mac65] S. MacLane. Categorical Algebra. *Bulletin of the American Mathematical Society*, 71:40–106, 1965.
- [Mac71] S. MacLane. *Categories for the Working Mathematician*. Graduate Texts in Mathematics. Springer Verlag, 1971.
- [Mas97] A. Massol. Minimality of the system of seven equations for the category of finite sets. *Theoretical Computer Science*, 176(1-2):347–353, 1997.
- [Mim08] S. Mimram. *Sémantique des jeux asynchrones et réécriture 2-dimensionnelle*. PhD thesis, 2008.
- [Mim10] S. Mimram. Computing critical pairs in 2-dimensional rewriting systems. In Christopher Lynch, editor, *Proceedings of the 21st International Conference on Rewriting Techniques and Applications*, volume 6 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 227–242, Dagstuhl, Germany, 2010. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- [MM07] 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.
- [Pir02] T. Pirashvili. On the PROP Corresponding to Bialgebras. *Cah. Top. Géom. Diff. Cat.*, 43(3):221–239, 2002.
- [SS86] S. Schanuel and R. Street. The Free Adjunction. *Cahiers de Topologie et Géométrie Différentielle Catégoriques*, 27(1):81–83, 1986.
- [Str76] R. Street. Limits indexed by category-valued 2-functors. *J. Pure Appl. Algebra*, 8(2):149–181, 1976.
- [Win87] G. Winskel. Event Structures. *Advances in Petri Nets*, 255:325–392, 1987.