A formalization of diagrammatic proofs in abstract rewriting

Julien Narboux

A formalization of diagrammatic proofs in abstract rewriting

Julien Narboux

September 12, 2006

Abstract

Diagrams are commonly used in the rewriting community. In this paper, we present a formalization of this kind of diagrams. We give a formal definition of the diagrams which are used to state properties. We propose inference rules to formalize some diagrammatic proofs such as the proof of the Newman's lemma. We show that the system proposed is both correct and complete for a class of formulas called "coherent logic".

Contents

1 Introduction

Some diagrams can be seen as a high level description of a proof, in the sense that they convince the reader that some fact is true. This kind of diagrams appears in different domains of mathematics and computer science, such as euclidean geometry, number theory, real analysis, set theory, category theory, rewriting...
In [Jam01], Jamnik uses diagrams as a hint for an automated theorem prover in the field of number theory. In [BPB91], Dave Barker-Plummer and Sidney C. Bailin use also diagrams as a hint for an automated theorem prover in the field of abstract rewriting. In this paper, we want to give to the class of diagrams which are in used the abstract rewriting community the status of a *proof object* as we plan to use them as input language for the Coq proof assistant [Coq04, HKPM04]. This approach requires that we give a formal definition of the diagrams, its semantic and of the correctness of a proof diagram. Work has been done in this direction for some classes of diagrams: Miller has proposed a formal system for some diagrammatic proofs in euclidean geometry [Mil01] and Winterstein has given another system for diagrammatic proofs in the field of real analysis [Win04]. We focus on abstract rewriting because diagrams are commonly used in papers and books about this subject, for example in [BN98] diagrams appear throughout the book and are even given a precise meaning[1]. In this paper we will give a presentation of abstract rewriting similar to [BN98] except that our intent is not to consider diagrams as illustrations for proofs but as a proof objects in themselves.

First, we recall the definition of an abstract term rewriting system and give a formal definition of a rewriting diagram. Second, we define some properties diagrammatically and present a formal proof system using a simple proof as an example. Then, we introduce diagrammatic inference rules to formalize proofs by induction as well as well-founded induction and thereby we prove the Newman's lemma [New42]. Finally, we put forward the implemention of the inference rules within the Coq proof assistant.

[1] Note fully formal though, because sometimes variables are implicitly universally quantified and sometimes they are not.

2 Diagrammatic representation in abstract rewriting

In this section, we recall the definitions of an abstract term rewriting system and we propose a definition for the diagrams which are current in the literature.

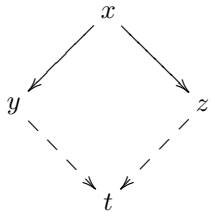
An *abstract reduction system* is a pair $(A, \rightarrow)$ where the *reduction* $\rightarrow$ is a binary relation on the set A, i.e. $\rightarrow \subseteq A \times A$.

Our aim in this paper is to formalize the kind of diagrams which are commonly used in the rewriting community. We do not try to invent a new kind of diagrams as in [BvOK98], our goal is to define a diagrammatic language which will be used later as an input language for the Coq proof assistant.

The fact that $(x, y) \in \rightarrow$ will be depicted by an arrow in infix position: $x \longrightarrow y$.

Informally, we use the usual convention according to which solid arrows stand for the hypotheses and dashed arrows stand for the conclusion. Vertices which are connected only to dashed arrows are supposed to be existentially quantified by default. Vertices which are connected to at least one solid arrow are always quantified universally.

Let's have a look at a first example before giving a formal definition. A well-known property of an abstract rewriting relation is the diamond property which is often used and is usually represented in the rewriting community by the following diagram :



The *meaning* of this diagram is the following :

$$\forall xyz,\ x \longrightarrow y \wedge x \longrightarrow z \Rightarrow \exists t,\ y \longrightarrow t \wedge z \longrightarrow t$$

Now as our goal is to treat diagrams as first class citizens, i.e. not as *notations* for some mathematical objects but as mathematical objects. To reach this goal, we need a formal definition of a diagram and its semantic.

We begin with the definition of a multi-graph since it is used in the definition of a diagram.

Definition 1 (directed multi-graph)**.** *A directed multi-graph is a 4-uple* (V, A, s, d) *where*

- V *is the set of vertices.*
- A *is the set of arrows.*
- $s : A \to V$ *is a function from arrows to vertices (the source of the arrow)*
- $d : A \to V$ *is a function from arrows to vertices (the destination of the arrow)*

Note that an arrow can have the same source and destination.

Definition 2 (Diagram)**.** *A rewriting diagram* D *is a finite directed multi-graph whose arrows are labeled by a relation and a status (either conclusion or hypothesis) and vertices are labeled by a name and a status (either universal, existential or free) verifying the following conditions :*

- *If a vertex is in contact with at least one hypothesis arrow then its status is not existential.*
- *There is at least one conclusion arrow.*
- *There is no vertex of degree zero.*

Formally, it is a 10-uple $(\Sigma_V, \Sigma_A, V, A, s, d, l_A, l_V, s_A, s_V)$ *where :*

- Σ_V *is the set of vertices symbols*
- Σ_A *is the set of relation symbols*
- V *is the set of vertices*
- A *is the set of arrows*
- $s : A \to V$ *is the source function*
- $d : A \to V$ *is the destination function*
- $l_A : A \to \Sigma_A$ *is a function from the set of arrows to the relation symbols*
- $l_V : V \to \Sigma_V$ *is an injective function from the set of vertices to the vertices symbols*
- $s_A : A \to \{\mathcal{H}, \mathcal{C}\}$ *is a function from the set of arrows to the arrows status*
- $s_V : V \to \{\forall, \exists, \mathcal{F}\}$ *is a function from the set of vertices to the vertices status*

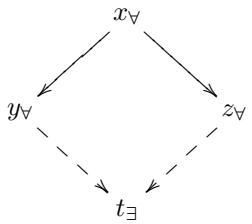
verifying that :

- $\forall v \in V, (\exists a \in A,\ (s(a) = v \vee d(a) = v) \wedge s_A(a) = \mathcal{H}) \Rightarrow s_V(v) \neq \exists$
- $\exists a \in A, s_A(a) = \mathcal{C}$
- $\forall v \in V, \exists a \in A, s(a) = v \vee d(a) = v$

2.0.1 First notations (N1):

When arrows are labeled by the same relation, the label of this relation is omitted.
Arrows which are marked as conclusion will be represented by a dashed arrow, and hypotheses by a solid arrow.
The universal vertices are labeled using the symbol $\forall$.
The existential vertices are labeled using the symbol $\exists$.
The free vertices are underlined.

Using these notations the diamond property is represented this way :



We say that a term $x \xrightarrow{R} y$ is represented by an arrow if the diagram contains an arrow labeled by R such that $s(f) = x$ and $d(f) = y$.

Now, we need to give a formal semantic to ours diagrams. Note that this definition is not necessary for the construction of a formal system to build proofs in abstract term rewriting. Indeed, we could consider that the semantic of diagrams is implicitly defined by the inference rules. We give here the semantic not only to clarify the presentation but also because it is necessary to state the correctness and completeness theorems with regard to the sequent calculus (see section 4).

Definition 3 (semantic)**.**
The semantic of an arrow $x \xrightarrow{R} y$ is $R(x, y)$.
Let $\overrightarrow{e}$ be the set of labels of existential vertices and $\overrightarrow{u}$ the set of labels of universal vertices.
Let C be the conjunction of the terms represented by a conclusion arrow.
Let H be the conjunction of the terms represented by an hypothesis arrow or true if the conjunction is empty.

By definition the semantic of the diagram D noted $[\![D]\!]$ is:

$$[\![D]\!] := \forall \overline{u}, H \Rightarrow \exists \overline{e}, C$$

Notice that in virtue of the first condition in the definition of a diagram, the conjunction C is not empty and in virtue of the second condition, H does not contain an occurrence of a variable which is in $\overline{e}$
Note also that we do not define the order of the variables in $\overline{e}$ and $\overline{u}$ and the order of the terms in C and H. This does not introduce fundamental ambiguities as the formulas obtained by permutation are equivalent.

It is clear from the definition of the semantic that not all first-order formulas can be represented by a diagram. We can describe only formulas of the form $\forall \overline{u} \bigwedge_i H_i \Rightarrow \exists \overline{e} \bigwedge_i C_i$ where the terms in H_i and C_i are predicates of arity two.

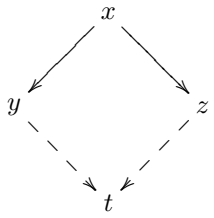
Remark 1. *If a diagram contains several connex components, its semantic is equivalent to the conjunction of the semantics of the different components.*

Proof: By injectivity of the function l_V. □

2.0.2 Second notations (N2):

As our goal is to give a definition of diagrams as close as possible to the comm on usage in the community, we introduce two other notations:

1. In the representation of a diagram if we omit the status of a vertex, it has the following implicit status :
   If the vertex is in contact with only conclusion arrows its status is existential, otherwise its status is universal.
   Now, we have the usual notation for the diamond property :



2. In the representation of a diagram, if we draw only solid arrows and we omit the status of the vertices, this is a notation to represent the same diagram consisting of only dashed arrows and free vertices.
   Example : $x \longrightarrow y$ is a notation for $\underline{x} - - \succ \underline{y}$

   Note that this notation is not ambiguous as every diagram has a least one conclusion arrow.
   Note also that if we swapped the role of the dashed and solid arrows in the definition of the semantic of a diagram we would not need this notation rule. We keep this definition to follow the common usage in the community.

Before going further, here are some small examples of diagrams and their semantic:

Formula	Diagram
$x \longrightarrow x$	$\underline{x}$ noted also[a] x
$\forall x,\ x \longrightarrow x$	$x_\forall$
$\exists x,\ x \longrightarrow x$	x
$\exists xy,\ x \longrightarrow y$	$x - - \succ y$
$\forall x \exists y,\ x \longrightarrow y$	$x_\forall - - \succ y$
$\forall xy,\ x \longrightarrow y$	$x_\forall - - \succ y_\forall$
$x \longrightarrow y$	$\underline{x} - - \succ \underline{y}$ noted also $x \longrightarrow y$

[a] in the absence of other arrows in the diagram

2.1 Extension to disjunctions.

Usually, in the literature about rewriting, disjunctions are not represented by diagrams. But, in order to define the transitive closure of a relation, we need to define diagrams representing disjunctions. Indeed we want to express the fact that[2] :

$$\forall xy, x \xrightarrow{+} y \Rightarrow (x \longrightarrow y \vee \exists y', x \longrightarrow y' \xrightarrow{+} y)$$

Definition 4 (disjunctive diagram)**.** *A disjunctive diagram is a finite set of diagrams (in the sens of the definition 2) whose sub-diagrams restrained to solid arrows and universal vertices are identical.*

Notation: We separate the sub-diagrams of the disjunction through the use of a vertical bar |.

The semantic is as follows:

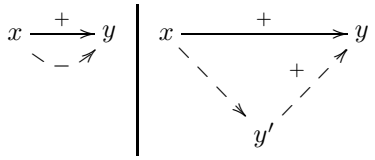
Definition 5 (disjunctive diagrams' semantic)**.**
Let $D = \{D_1 \dots D_n\}$ be a disjunctive diagram. As the diagrams D_i share the same solid arrows, we know that they have a semantic of the form:

$$\forall \overrightarrow{u}, H \Rightarrow \exists \overrightarrow{e_i}, C_i$$

The semantic of D is by definition:

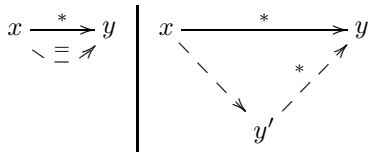
$$[\![D]\!] := \forall \overrightarrow{u}, H \Rightarrow \bigvee_{i \in 1 \dots n} \exists \overrightarrow{e_i}, C_i$$

For example, here are the diagrams which express the two possible cases of construction of the reductions $\xrightarrow{+}$ and $\xrightarrow{*}$:



[2] See section 2.4 for the definition of the relations $\xrightarrow{+}$ and $\xrightarrow{*}$.

$$\forall xy, x \xrightarrow{+} y \Rightarrow (x \longrightarrow y \vee \exists y', x \longrightarrow y' \xrightarrow{+} y)$$



$$\forall xy, x \xrightarrow{*} y \Rightarrow (x \xrightarrow{=} y \vee \exists y', x \longrightarrow y' \xrightarrow{*} y)$$

2.2 Language of the represented formulas

After the extension to disjunctive diagrams, the formulas which can be represented by a diagram are those of the form:

$$\forall \overline{u} \bigwedge_i H_i \Rightarrow \bigvee_i \exists \overline{e_i} \bigwedge_j C_{i_j}$$

where the H_i and C_{i_j} are predicates of arity two.

These formulas form a sub-language of the *coherent logic* of Marc Bezem and Thierry Coquand. For more information about this logic see [BC05, BC04].

Now, we will call $\mathcal{D}$ this class of formulas.

2.3 About the negation

The class $\mathcal{D}$ of formulas that we have defined does not contain negations. This is a limitation as we can not define for example the notion of normal form. But this property is important because the diagrams which we use consist in the representation of general fact by an example. It is difficult to denote diagrammatically, by an example, the fact that something does not hold. We have the same problem in geometry, impossible figures are hard to denote graphically.

In some domains, negations can be represented diagrammatically. For example, the fact that an element is not in a set can be represented through the use of an Euler diagram. But, in this context, negations do not have the same meaning as before since implicitly the logic is classical: if x is not in A then it is in its complementary $\neg A$.

2.4 Definitions and common properties

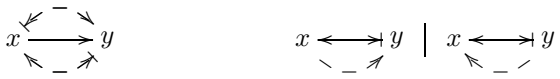
We give now some definitions using the diagrams we have defined. These definitions will be used in the main example of the next section.

We associate four relations to a given one:

- the reflexive closure ($\xrightarrow{=?}$),
- the transitive closure ($\xrightarrow{+}$),
- the reflexive and transitive closure ($\xrightarrow{*}$),
- the symmetric closure ($\leftrightarrow$).

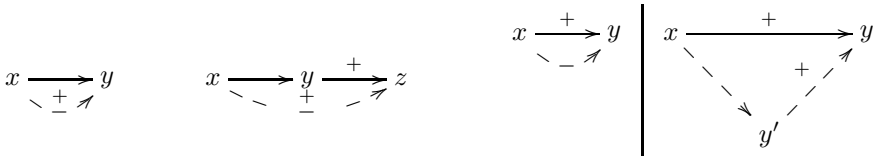
The first three definitions are the classical ones. For the definition of the symmetric closure we do not use the usual symbol ($\leftrightarrow$). Indeed, this symbol has the property it denotes: it is symmetric ! This is one of the reasons why this representation is really diagrammatic. We will see that in diagrammatic proofs, the symmetrical notation hide a reasoning step. We will explain how to deal with this kind of implicit reasoning steps in section 6.2.

Definition 6 (symmetric closure)**.** *The symmetric closure of a relation is defined by the two following diagrams:*

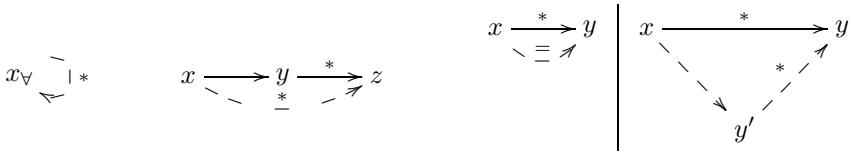


Definition 7 (reflexive closure)**.** *The reflexive closure of a relation is defined by the three following diagrams:*

Definition 8 (transitive closure)**.** *The transitive closure of a relation is defined*[3] *by the three following diagrams:*



Definition 9 (transitive and reflexive closure)**.** *The transitive and reflexive closure of a relation is defined by the three following diagrams:*



Definition 10 (Vocabulary)**.**

We say that x can be reduced if :

$$\underline{x} - - \succ y$$

We say that y is the direct successor of x if :

$$\underline{x} - - \succ \underline{y} \textit{ noted also } x \longrightarrow y$$

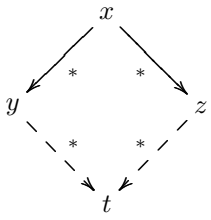
We say that y is a successor of x if :

$$\underline{x} \overset{+}{-} \succ \underline{y} \textit{ noted also } x \xrightarrow{+} y$$

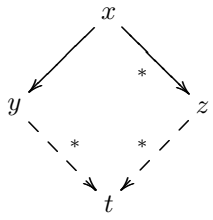
[3] As the transitive and reflexive-transitive closure are not first-order definable, this definition is not complete. It will be complete after the definition of the induction principle in section 5.

We say that x and y are joignable if :

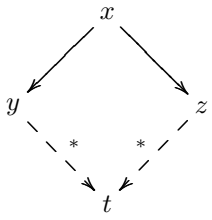
Definition 11 (Confluence properties)**.**



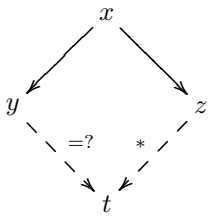
Confluence



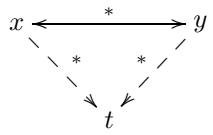
Semi-confluence



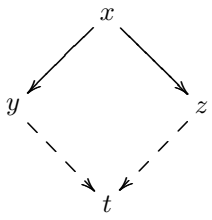
Local-confluence



Strong-confluence

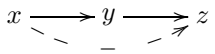


Church-Rosser



Diamond property

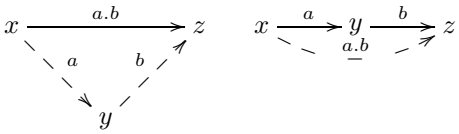
Definition 12 (Transitivity)**.**
A relation $\longrightarrow$ is transitive if the following diagram holds:



Definition 13 (Reflexivity)**.**
A relation $\longrightarrow$ is reflexive if the following diagram holds:

Definition 14 (Composition)**.**

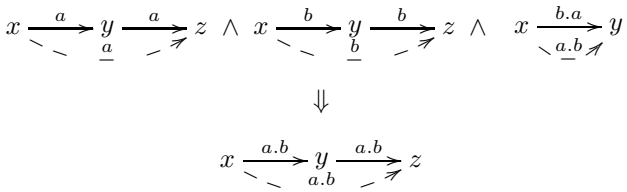
The composition of two relations $\xrightarrow{a}$ and $\xrightarrow{b}$ is defined by the following diagrams:



3 Diagrammatic proofs

In the previous sections we have formalized the diagrammatic notation which is commonly used in the rewriting community to define formulas involving relations. But these diagrams are also used to represent proofs. Before giving a formal definition, we will study one simple proof expressed by the mean of an informal diagram.

Example. *If* $\xrightarrow{a}$ *and* $\xrightarrow{b}$ *are two relations which are transitive and* $\xrightarrow{b.a} \subseteq \xrightarrow{a.b}$ *then* $\xrightarrow{a.b}$ *is transitive.*



Classic proof

Let x, y and z be such that $x \xrightarrow{a.b} y$ and $y \xrightarrow{a.b} z$.

We need to show that $x \xrightarrow{a.b} z$.

By the definition of $\xrightarrow{a.b}$ there exists u and v such that $x \xrightarrow{a} u \xrightarrow{b} y$ and $y \xrightarrow{a} v \xrightarrow{b} z$.

By the definition of $\xrightarrow{b.a}$, we have $u \xrightarrow{b.a} v$.

As $\xrightarrow{a.b} \subseteq \xrightarrow{b.a}$, we have $u \xrightarrow{a.b} v$.

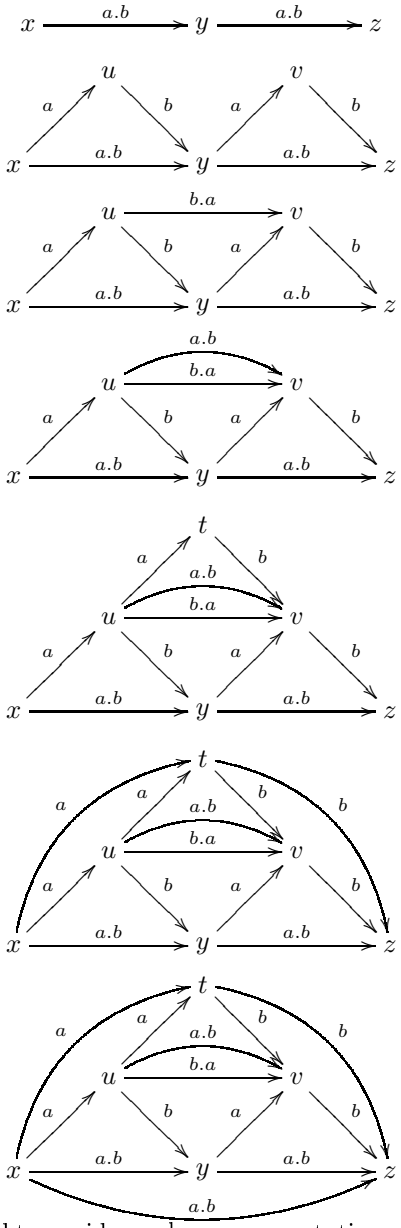
By the definition of $\xrightarrow{a.b}$, there exists t such that $u \xrightarrow{a} t$ and $t \xrightarrow{b} v$.

As $\xrightarrow{a}$ and $\xrightarrow{b}$ are transitive we know that $x \xrightarrow{a} t$ and $t \xrightarrow{b} z$.

We can conclude that :

$$x \xrightarrow{a.b} z$$

Diagrammatic proof



The diagram which is depicted on the right provides a clear representation of the proof. Note that it is necessary to give an "animation" of the way the diagram has been built, a proof consist in showing that a diagram can be constructed using some precise rules. The diagram represents what we know during the proof.

Our intent in this paper is to formalize this kind of diagrammatic proofs. We will define a few rules to allow us to have a small formal system to make proofs using the diagrams. Our aim here is to define the inference rules which

depict precisely the same reasoning step as those we perform while building the diagram. This is why the rules we define are not atomic from the logical point of view. Indeed, each of theses rules could be decomposed in "smaller" logical rules. We choose to define a formal system using the forward reasoning style, this means that the theorems will be proved step by step starting from the hypotheses.

The reasoning is formalized as usual. We assume that we have a set of hypotheses and a goal. The hypotheses and the goal are diagrams. Moreover we distinguish one hypothesis from the other ones, this hypothesis will be called *factual*, the other will be called *universal*. The factual hypothesis represents what we know during the proof, and the universal hypotheses are the tools to prove the theorem.

Definition 15 (factual hypothesis)**.** *We call* factual hypothesis*, a diagram which contains only free vertices and conclusion arrows.*

Remark 2. *Note that thanks to the notations we have defined, the factual diagrams can be represented with only solid arrows.*

Definition 16 (universal hypothesis)**.** *We call* universal hypothesis*, a diagram which is not factual.*

This means that we have pseudo-sequents of the following form:

$$U_1, U_2, \dots U_n, F \vdash D$$

where $U_1, \dots U_n$ are universal diagrams and F is a factual diagram.

To describe the rules of inference, we need first to define some transformation operations on diagrams.

Definition 17 (inversion)**.** *Let D be a diagram, the inversion of D is by definition D where each hypothesis arrow has been transformed into a conclusion arrow.*
Formally, if $D = (\Sigma_V, \Sigma_A, V, A, f, l_A, l_V, s_A, s_V)$ then

$$\mathcal{I}(D) = (\Sigma_V, \Sigma_A, V, A, f, l_A, l_V, s'_A, s_V)$$

where $s'(a) = \begin{cases} \mathcal{C} & \text{if } s_A(a) = \mathcal{H}, \\ s_A(a) & \text{otherwise} \end{cases}$

Definition 18 (union)**.** *We define the union of two factual diagrams.*
We say that D is the union of the factual diagrams D_1 and D_2, noted $D_1 \cup D_2$, iff the graph of D is the union of the graphs of D_1 and D_2 and all the vertices are free and all the arrows are conclusion.

Definition 19 (sub-diagram)**.**
We say that a diagram

$$D_1 = (\Sigma_{V_1}, \Sigma_{A_1}, V_1, A_1, s_1, d_1, l_{A_1}, l_{V_1}, s_{A_1}, s_{V_1})$$

is a sub-diagram of

$$D_2 = (\Sigma_{V_2}, \Sigma_{A_2}, V_2, A_2, s_2, d_2, l_{A_2}, l_{V_2}, s_{A_2}, s_{V_2})$$

noted $D_1 \subseteq D_2$ iff :

- $V_1 \subseteq V_2$
- $A_1 \subseteq A_2$
- *the functions* $s_1, d_1, l_{A_1}, l_{V_1}, s_{A_1}, s_{V_1}$ *and* $s_2, d_2, l_{A_2}, l_{V_2}, s_{A_2}, s_{V_2}$ *coincide (where they are both defined).*

Notations : We call D_H (resp. D_C) the sub-diagram of D which contains only hypothesis arrows (resp. conclusion).

3.1 Inference rules

Our system consist in six inference rules:

`intros` introduces hypotheses in the context,

`apply` uses the information contained in a universal diagram to enrich the factual diagram,

`conclusion` is an axiom rule, it allows to conclude a proof when the factual diagram contains enough information,

`substitute` and `reflexivity` are used for the equality,

`cut` allows to reuse previously proved lemmas.

Note that we choose to define equality as a primitive notion. We could have defined equality using diagrams. But this approach would have produced bigger proofs. We want to simplify the diagrams when two vertices are equal.

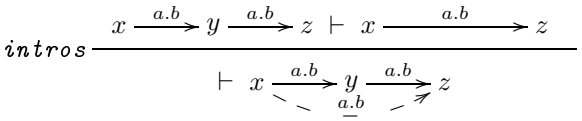
3.1.1 `intros`

The first rule is the `intros` rule, it was omitted in the informal example we have given.
Let $\overline{f}$ be the set of labels of the free vertices in $H_1, \ldots, H_n, G$.
Let $G_{hyp} = \sigma(\mathcal{I}(G_H))$ and $G_{concl} = \sigma(G_C)$, where σ is a substitution of a subset of the universal vertices of G into free vertices labeled by fresh variables.

$$\texttt{intros}\ \frac{H_1, \ldots, H_n, G_{hyp} \vdash G_{concl}}{H_1, \ldots, H_n \vdash G}$$

Note that using the second notation (N2), this means that graphically G_{hyp} is represented by the sub-diagram of G restrained to solid arrows.

Example.



3.1.2 `apply`

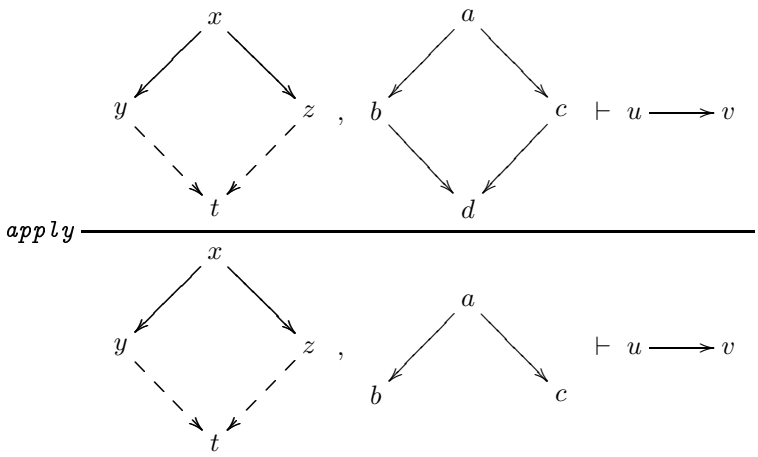
The second rule is the `apply` rule. This is the rule which is used at each step of the first example. It consists in applying a universal diagram D to a sub-diagram of the factual diagram F. If D is a disjunctive diagram this rule introduces a case distinction.

Let D be a universal diagram in the set of hypothesis and σ substitution which replaces universal vertices in such a way that the hypotheses of D is a sub-diagram of the factual diagram. For each diagram D_j in the disjunction, the `apply` rule demands to prove the goal with a factual diagram enriched by the conclusion D_i, existential vertices are instantiated by fresh variables.
Formally:

$$\texttt{apply}\ \frac{D_1,\ldots,D_n,F\cup\delta_1(F_1)\vdash G \qquad \ldots \qquad D_1,\ldots,D_n,F\cup\delta_m(F_m)\vdash G}{D_1,\ldots,D_n,F\vdash G}$$
$$\text{if } \exists i,\sigma,\mathcal{I}(\sigma(D_i)_H)\subseteq F$$
$$\text{and } (\sigma(D_i))_C=(F_1|\ldots|F_m)$$

and $\delta_1,\ldots,\delta_m$ associate fresh variables to the existential vertices of $F_1,\ldots,F_m$.

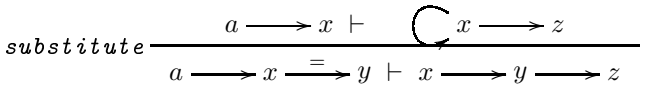
Example.



3.1.3 `substitute`

If the factual diagram contains a sub-diagram of the form $\underline{x} \xrightarrow{=} \underline{y}$ the `substitute` rule allows to replace some occurrences of $\underline{x}$ by $\underline{y}$ and/or to merge the vertices $\underline{x}$ and $\underline{y}$ in all the diagrams.

Example.



3.1.4 `reflexivity`

The reflexivity rule is the following:

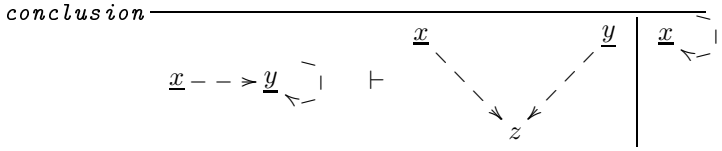
$$\texttt{reflexivity}\ \frac{}{\Gamma\vdash x=x}$$

3.1.5 `conclusion`

The conclusion rule is used to finish the proof. If the goal is a diagram $G = G_1|\dots|G_m$ without any hypothesis arrow nor universal vertex (where $m = 1$ if G is not disjunctive), the `conclusion` rule proves the theorem if there exists a diagram G_i and a substitution σ of the existential vertices of G_i such that $\sigma(G_i)$ is a sub-diagram of the factual hypothesis F.

$$\texttt{conclusion}\ \frac{}{D_1, \dots, D_n, F \vdash G_1|\dots|G_m}\ \text{if } \exists i \sigma, \sigma(G_i) \subseteq F$$

Example.



3.1.6 `cut`

The `cut` rule is the usual cut rule.

$$\texttt{cut}\ \frac{D_1, \dots, D_n, F \vdash G \qquad D_1, \dots, D_n, G, F \vdash J}{D_1, \dots, D_n, F \vdash J}$$

4 Correctness and completeness

In this section, we show the correctness and completeness of the formal system proposed with regard to a sequent calculus enriched with equality.

4.1 Intuitionist vs classical logic

Before proving the correctness and completeness of the system, we need to choose a logic. In particular, we need to choose between an intuitionist logic or classical logic system. In fact, for the class of formulas we consider, intuitionist and classical provability coincide. This result has been shown several times [BC04, Neg03], we show here that we can use a result proved by Gopalan Nadathur [Nad00] using Kleene permutation lemma [Kle52].

In this section, we note $\vdash_{LJ}$ intuitionist provability and $\vdash_{LK}$ classical provability[4]. As these two notions coincide for the class of formulas we consider, we will omit to distinguish them in the following sections.

Lemma 1 (Kleene)**.** *If $\Gamma \vdash_{LK} A, \Delta$ then it is possible to build proofs of the following sequents:*

- *if A is of the form $P \Rightarrow Q$ then $\Gamma, P \vdash_{LK} Q, \Delta$*
- *if A is of the form $\forall x\, P$ then $\Gamma \vdash_{LK} [c/x]P, \Delta$ with c a fresh variable.*

Proof: The proof of the lemma can be found in [Kle52] or in a more general form (generalized to deduction modulo) in [Her05]. □

Theorem 1 (Nadathur)**.**
Let's consider the following classes of H and G-formulas, assume that A is an atomic formula.

$$G ::= \top | \bot | A | G \wedge G | G \vee G | \exists x G$$

$$H ::= \top | \bot | A | G \Rightarrow H | H \wedge H | H \vee H | \exists x H | \forall x H$$

If Γ is a multi-set of H-formulas, and F is a G-formula then

$$\Gamma \vdash_{LK} F \iff \Gamma \vdash_{LJ} F$$

Proof: See [Nad00], Theorem 6. □

Theorem 2. *If $D_1, \ldots, D_n$ and G are in $\mathcal{D}$ then*

$$D_1, \ldots, D_n \vdash_{LK} G \iff D_1, \ldots, D_n \vdash_{LJ} G$$

Proof:
The implication from right to left is always true.
We need to show that $D_1, \ldots, D_n \vdash_{LK} G \Rightarrow D_1, \ldots, D_n \vdash_{LJ} G$.
Assume that $D_1, \ldots, D_n \vdash_{LK} G$.
As $G \in \mathcal{D}$, G is of the form:

$$\forall \overline{u} \bigwedge_i H_i \Rightarrow \bigvee_i \exists \overline{e_i} \bigwedge_j C_{i_j}$$

[4] Note that we adopt a presentation of the type G_3, we do not want to deal with the structural rules here.

where H_i and C_{i_j} are predicates of arity two.
Using Kleene lemma applied to $\forall$ and $\Rightarrow$, we can build a proof of:

$$D_1, \ldots, D_n, [\overline{c}/\overline{u}] \bigwedge_i H_i \vdash_{LK} [\overline{c}/\overline{u}] \bigvee_i \exists \overline{e_i} \bigwedge_j C_{i_j}$$

where $\overline{c}$ are fresh variables.
Using Nadathur's theorem, we have:

$$D_1, \ldots, D_n, [\overline{c}/\overline{u}] \bigwedge_i H_i \vdash_{LJ} [\overline{c}/\overline{u}] \bigvee_i \exists \overline{e_i} \bigwedge_j C_{i_j}$$

By application of the rules $\forall_{\mathcal{R}}$ and $\Rightarrow_{\mathcal{R}}$, we have $D_1, \ldots, D_n, \vdash_{LJ} G$. □

4.2 The system of reference

We define here the formal system we use as a reference for the correctness and completeness proofs. The class of formulas we consider, $\mathcal{D}$, does not contain the negation, we omit the associated rules. Moreover, as our system has built-in equality, we also add equality in the sequent calculus. The system we obtain is shown on table 1. We note $\vdash_=$ the provability in this system, $\vdash$ represents provability in the system with the rules E_1, E_2, $=_{\mathcal{R}}$. We note $\vdash_{\mathcal{D}}$ the provability in the diagrammatic system we have defined in section 3.1.

4.3 Correctness

In this section we prove the correctness of the system we propose. The correctness proof is straightforward since each of the diagrammatic inference rules corresponds to a set of inference rules of the sequent calculus. The only exception is the `substitute` rule. For this rule we need the following lemma:

Lemma 2. *The generalized substitution rules:*

$$GE_1 \frac{[s/x]\Gamma, s = t \vdash [s/x]\Delta}{[t/x]\Gamma, s = t \vdash [t/x]\Delta} \qquad GE_2 \frac{[t/x]\Gamma, s = t \vdash [t/x]\Delta}{[s/x]\Gamma, s = t \vdash [s/x]\Delta}$$

are admissible.

Proof: By induction on the structure of the derivation. □

Theorem 3 (Correctness)**.**
If $D_1, \ldots, D_n, F \vdash_{\mathcal{D}} G$ then $[\![D_1]\!], \ldots, [\![D_n]\!], [\![F]\!] \vdash_= G$.

Proof: By induction on the structure of the proof and by cases on the rule which is used:

`intros` *by application of the rules $\forall_{\mathcal{R}}$, $\Rightarrow_{\mathcal{R}}$, $\wedge_{\mathcal{L}}$.*

`apply` *by application of the rules $\forall_{\mathcal{L}}$, $\Rightarrow_{\mathcal{L}}$ then $\wedge_{\mathcal{R}}$,$\wedge_{\mathcal{L}}$, and axiom on one side, $\vee_{\mathcal{L}}$, $\exists_{\mathcal{L}}$, $\wedge_{\mathcal{L}}$, axiom on the other side.*

`conclusion` *by application of the rules $\vee_{\mathcal{R}}$, $\exists_{\mathcal{R}}$, $\wedge_{\mathcal{R}}$, $\wedge_{\mathcal{L}}$, axiom.*

`substitute` *by application of the rules GE_1 and GE_2.*

`reflexivity` *by application of the rule $=_{\mathcal{R}}$.*

`cut` *Since the cut rule of the sequent calculus is admissible we can use it here.*

□

Table 1: Classical sequent calculus without negation

$$\text{axiom}\ \frac{}{\Gamma, A \vdash \Delta, A}$$

$$\Rightarrow_{\mathcal{L}}\ \frac{\Gamma \vdash A, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta} \qquad \Rightarrow_{\mathcal{R}}\ \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}$$

$$\wedge_{\mathcal{L}}\ \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad \wedge_{\mathcal{R}}\ \frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}$$

$$\vee_{\mathcal{L}}\ \frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}$$

$$\vee_{\mathcal{R}}\ \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}$$

$$\forall_{\mathcal{L}}\ \frac{\Gamma, \forall x B, B[x \leftarrow t] \vdash \Delta}{\Gamma, \forall x B \vdash \Delta} \qquad \forall_{\mathcal{R}}\ \frac{\Gamma \vdash B[x \leftarrow c], \Delta}{\Gamma \vdash \forall x B, \Delta}$$

$$\exists_{\mathcal{L}}\ \frac{\Gamma, B[x \leftarrow c] \vdash \Delta}{\Gamma, \exists x B \vdash \Delta} \qquad \exists_{\mathcal{R}}\ \frac{\Gamma \vdash \exists x B, B[x \leftarrow t], \Delta}{\Gamma \vdash \exists x B, \Delta}$$

$$=_{\mathcal{R}}\ \frac{}{\Gamma \vdash s = s, \Delta}$$

$$E_1\ \frac{\Gamma, s = t \vdash [s/x]\Delta}{\Gamma, s = t \vdash [t/x]\Delta} \qquad E_2\ \frac{\Gamma, s = t \vdash [t/x]\Delta}{\Gamma, s = t \vdash [s/x]\Delta}$$

in $\exists_{\mathcal{L}}$, c does not appear free in $\exists x\, B, \Gamma, \Delta$
in $\forall_{\mathcal{R}}$, c does not appear free in $\forall x\, B, \Gamma, \Delta$

4.4 Completeness

It is possible to separate the reasoning about equality from the other part of the proof. In virtue of this, we can exploit some known results about the reasoning without equality. For the proof of completeness of the reasoning without equality, we use a result by Marc Bezem and Thierry Coquand. Although we developped our rules separately and with a different goal in mind[5], our inference rules corresponds precisely to those of the definition 6.1 of [BC04]. Note that the sequent calculus that we use, is not defined in the same way as in [BC04] (for instance our $\vee$ rule is multiplicative). As the two systems are equivalent we do not distinguish between them.

4.4.1 System without equality

Theorem 4 (Partial completeness)**.**
If $D_1, \ldots, D_n, F$ and G are in $\mathcal{D}$ and $D_1, \ldots, D_n, F \vdash G$ then there exists some diagrams D'_1,...,D'_n, F' and G' such that:

$$[\![D'_1]\!] = D_1, \ldots, [\![D'_n]\!] = D_n,\ [\![F']\!] = F \text{ and } [\![G']\!] = G \text{ and}$$

$$D'_1, \ldots, D'_n, F' \vdash_{\mathcal{D}} G'$$

Proof: As G is in $\mathcal{D}$, G is of the form $\forall \overline{u}, C \Rightarrow D$. By Kleene lemma, we can build a proof of

$$D_1, \ldots, D_n, F, [\overline{c}/\overline{u}]C \vdash D.$$

By theorem 6.2 in [BC04] with for all X, X' is any diagram such that $[\![X']\!] = X$, we have

$$D'_1, \ldots, D'_n, F', [\overline{c}/\overline{u}]C' \vdash_{\mathcal{D}} D'.$$

(the base case of definition 6.1 of [BC04] corresponds to the `conclusion` rule and the inductive case corresponds to the `apply` rule.)
Thanks to the `intros` rule we can conclude that:

$$D'_1, \ldots, D'_n, F' \vdash_{\mathcal{D}} G'$$

□

4.4.2 Dealing with equality

In this section, we show the completeness of the system with equality. In order to use the result about the system without equality we use the fact that the reasoning about equality can be pushed up to the leaves of the derivation tree. In other words, if $\Gamma \vdash_{=} \Delta$ then $\Gamma \vdash_{|=} \Delta$, the system $\vdash_{|=}$ is given on table 2. The system $\vdash_{|=}$ corresponds to $\vdash_{=}$ where the equality rules have been deleted and the axiom rule has been replaced by a small formal system about equality.

Lemma 3. $\Gamma \vdash_{=} \Delta \iff \Gamma \vdash_{|=} \Delta$

Proof: See [Pfe04]. □

Lemma 4. *If $\Gamma \vdash_{|=} \Delta$ then there exists Γ' a multi-set of formulas which belong to the coherent logic such that $\Gamma', \Gamma \vdash \Delta$ and forall X in Γ' there exists X' such that $[\![X']\!] = X$ and $\vdash_{\mathcal{D}} X'$.*

[5] Marc Bezem and Thierry Coquand are interrested in the automation of coherent logic.

$$axiom_{=}\ \frac{}{\Gamma, A \vdash_{Ax_{=}} A} \qquad =_{\mathcal{R}}\ \frac{}{\Gamma \vdash_{Ax_{=}} x = x}$$

$$E_1\ \frac{\Gamma, s = t \vdash_{Ax_{=}} [s/x]\Delta}{\Gamma, s = t \vdash_{Ax_{=}} [t/x]\Delta} \qquad E_2\ \frac{\Gamma, s = t \vdash_{Ax_{=}} [t/x]\Delta}{\Gamma, s = t \vdash_{Ax_{=}} [s/x]\Delta}$$

$$\text{eq-axiom}\ \frac{\Gamma \vdash_{Ax_{=}} \Delta}{\Gamma \vdash_{|=} \Delta}$$

$$\Rightarrow_{\mathcal{L}}\ \frac{\Gamma \vdash_{|=} A, \Delta \qquad \Gamma, B \vdash_{|=} \Delta}{\Gamma, A \Rightarrow B \vdash_{|=} \Delta} \qquad \Rightarrow_{\mathcal{R}}\ \frac{\Gamma, A \vdash_{|=} B, \Delta}{\Gamma \vdash_{|=} A \Rightarrow B, \Delta}$$

$$\wedge_{\mathcal{L}}\ \frac{\Gamma, A, B \vdash_{|=} \Delta}{\Gamma, A \wedge B \vdash_{|=} \Delta} \qquad \wedge_{\mathcal{R}}\ \frac{\Gamma \vdash_{|=} \Delta, A \qquad \Gamma \vdash_{|=} \Delta, B}{\Gamma \vdash_{|=} \Delta, A \wedge B}$$

$$\vee_{\mathcal{L}}\ \frac{\Gamma, A \vdash_{|=} \Delta \qquad \Gamma, B \vdash_{|=} \Delta}{\Gamma, A \vee B \vdash_{|=} \Delta}$$

$$\vee_{\mathcal{R}}\ \frac{\Gamma \vdash_{|=} A, B, \Delta}{\Gamma \vdash_{|=} A \vee B, \Delta}$$

$$\forall_{\mathcal{L}}\ \frac{\Gamma, \forall x B, B[x \leftarrow t] \vdash_{|=} \Delta}{\Gamma, \forall x B \vdash_{|=} \Delta} \qquad \forall_{\mathcal{R}}\ \frac{\Gamma \vdash_{|=} B[x \leftarrow c], \Delta}{\Gamma \vdash_{|=} \forall x B, \Delta}$$

$$\exists_{\mathcal{L}}\ \frac{\Gamma, B[x \leftarrow c] \vdash_{|=} \Delta}{\Gamma, \exists x B \vdash_{|=} \Delta} \qquad \exists_{\mathcal{R}}\ \frac{\Gamma \vdash_{|=} \exists x B, B[x \leftarrow t], \Delta}{\Gamma \vdash_{|=} \exists x B, \Delta}$$

in $\exists_{\mathcal{L}}$, c does not appear free in $\exists x\, B, \Gamma, \Delta$
in $\forall_{\mathcal{R}}$, c does not appear free in $\forall x\, B, \Gamma, \Delta$
in $axiom_{=}$, A is an atom

Table 2: The system $\vdash_{|=}$.

Proof: *Let Γ_i and Δ_i be respectively the hypotheses and conclusions of the premises of the rules eq-axiom.*
We define Γ' as the union of the :

$$\Gamma'_i \Rightarrow \Delta'_i$$

where Γ'_i is the conjunction of the atoms in Γ_i and Δ'_i the disjunction of the formulas in Δ_i. Note that as the rule $axiom_=$ is restrained to atoms, the elements of Δ_i are atoms. The elements of Γ' belongs to the set of formulas that can be represented by a diagram.
We obtain the result for the rule $axiom_=$ thanks to the rules `intros`, `apply` *and* `conclusion`. *For the other rules (E_1,E_2 and $=_{\mathcal{R}}$) we use* `substitute` *and* `reflexivity`. □

Theorem 5 (Completeness)**.**
If $D_1, \ldots, D_n, F \vdash_= G$ then there exists some diagrams D'_1,...,D'_n, F' and G' such that:

$$[\![D'_1]\!] = D_1, \ldots, [\![D'_n]\!] = D_n,\ [\![F']\!] = F \text{ and } [\![G']\!] = G \text{ and}$$

$$D'_1, \ldots, D'_n, F' \vdash_{\mathcal{D}} G'$$

Proof: *Suppose that $D_1, \ldots, D_n, F \vdash_= G$ then by lemma 3 we know that $D_1, \ldots, D_n, F \vdash_{|=} G$.*
By lemma 4 there exists Γ such that $\Gamma, D_1, \ldots, D_n, F \vdash G$ and forall X in Γ there exists a diagram X' such that $[\![X']\!] = X$ and $\vdash_{\mathcal{D}} X'$.
From the completeness of the system without equality, we can conclude that there exists Γ', D'_1, ..., D'_n and G' such that

$$\Gamma', D'_1, \ldots, D'_n, F' \vdash_{\mathcal{D}} G'$$

as the diagrams in Γ' can be derived in the empty context, using the `cut` *rule we have*

$$D'_1, \ldots, D'_n, F' \vdash_{\mathcal{D}} G'$$

□

5 Extension to proof by induction

In this section, we extend our system in order to deal with proofs by induction. We formalize proofs by induction on the length of a derivation as well as well-founded induction.

5.1 Classical induction

The principle of induction over the length of a derivation $\xrightarrow{*}$ is the following: In order to prove $\forall xy, P(x,y)$ with $x \xrightarrow{*} y$, it is sufficient to show $P(x,x)$ and $P(x,y)$ knowing that there exists some y' such that $x \longrightarrow y' \xrightarrow{*} y$ and $P(y',y)$ hold. Here is the traditional rule:

$$ind_* \frac{\forall xy\, x = y \Rightarrow P(x,y) \qquad \forall xy'y\, x \longrightarrow y' \xrightarrow{*} y \wedge P(y',y) \Rightarrow P(x,y)}{\forall xy\, x \xrightarrow{*} y \Rightarrow P(x,y)}$$

Diagrammatically, we use the following rule:
Let G be a diagram with two universal vertices x and y such that $x \xrightarrow{*} y$.
Let $G_=$ be the same diagram where first the vertices x and y have been replaced by free vertices labelled by fresh variables and second the arrow $x \xrightarrow{*} y$ has been replaced by $x = y$.
Let G_{ind} be the diagram G where first the vertex labelled by x is labelled by y' and second y' and y are free.
Let G_H, be the factual diagram $x \longrightarrow y' \xrightarrow{*} y$.
Let G_+, be the diagram G where x and y are free.
We have:

$$ind_* \frac{\Gamma \vdash G_= \qquad \Gamma, G_{ind}, G_H \vdash G_+}{\Gamma \vdash G}$$

Example. $\xrightarrow{*}$ *is transitive.*

Proof:

$$\vdash\ x \xrightarrow{*} y \xrightarrow{*} z$$

Case 1 :

$$\vdash\ \underline{x} \xrightarrow{=} \underline{y} \xrightarrow{*} z$$

by the rule `intros`

$$x \xrightarrow{=} y \xrightarrow{*} z\ \vdash\ x \xrightarrow{*} z$$

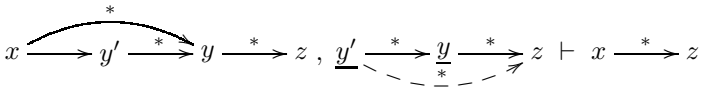
by the rule `substitute`

$$x \xrightarrow{*} z\ \vdash\ x \xrightarrow{*} z$$

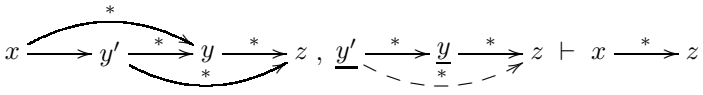
The `conclusion` *rule allows to conclude this case.*
Case 2 :

$$x \longrightarrow y' \xrightarrow{*} y\ ,\ \underline{y'} \xrightarrow{*} \underline{y} \xrightarrow{*} z\ \vdash\ \underline{x} \xrightarrow{*} \underline{y} \xrightarrow{*} z$$

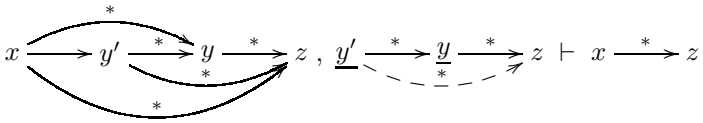
by the rule `intros`



by the rule `apply`



by the rule `apply` *applied to the definition of* $\overset{*}{\longrightarrow}$



The `conclusion` *rule allows to conclude this case.* □

5.2 Well-founded induction

In this section, we add the rule for well founded induction. The induction rule states that if a relation $\longrightarrow$ is terminating then to prove that $\forall x\, P(x)$ it is sufficient to show that $P(x)$ holds knowing that $P(y)$ holds for all y such that $x \overset{+}{\longrightarrow} y$.
Formally:

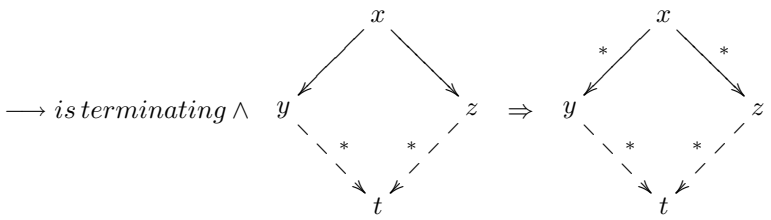
$$\frac{\forall x\, (\forall y\, x \overset{+}{\longrightarrow} y \Rightarrow P(y)) \Rightarrow P(x)}{\forall x\, P(x)} \text{ if } \longrightarrow \text{ is terminating}$$

We can formalize this inference rule diagrammatically:
Let G be a diagram. If G contains at least one universally quantified vertex and the relation $\longrightarrow$ is terminating then, we can use the rule for well-founded induction. The well-founded induction rule has two arguments: the first one is the terminating relation, the second one is the universally quantified vertex of the goal (let's call it x). The effect of the induction rule is to add a diagram corresponding to the induction hypothesis H_i in the hypotheses and to change the goal into a diagram G'. The induction hypothesis diagram H_i is composed by G where x has been renamed into a fresh variable y and enriched with a new arrow: $\underline{x} \overset{+}{\longrightarrow} y$.
The diagram G' is G excepted that the status of x is now $\mathcal{F}$.

$$\texttt{wf\_induction}\, \frac{D_1, \ldots, D_n, H_i \vdash G'}{D_1, \ldots, D_n, F \vdash G}$$

We extend our language by a new special hypothesis which states that a relation is terminating.

Example (Newman's lemma)**.**
A relation which is terminating is confluent if it is locally confluent.

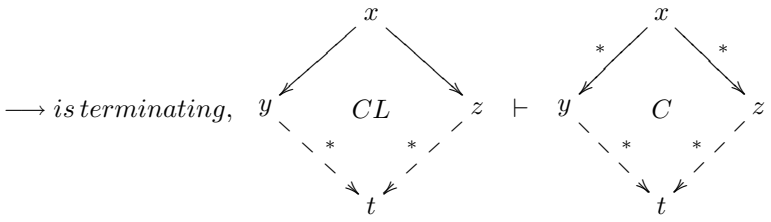


Traditional proof *(Gérard Huet [Hue80])*
We need to show that $\forall xyz, x \xrightarrow{*} y \wedge x \xrightarrow{*} z \Rightarrow \exists t, y \xrightarrow{*} t \wedge z \xrightarrow{*} t$.
Let's prove the theorem by well-founded induction using the fact that $\longrightarrow$ *is terminating and the predicate* $P(x) = \forall yz, x \xrightarrow{*} y \wedge x \xrightarrow{*} z \Rightarrow \exists t, y \xrightarrow{*} t \wedge z \xrightarrow{*} t$.
If $x = y$ *the theorem is verified because* $x \xrightarrow{*} z$ *and* $z \xrightarrow{*} z$.
If $x = z$ *the theorem is verified because* $x \xrightarrow{*} y$ *and* $y \xrightarrow{*} y$.
Otherwise $x \neq y$ *and* $x \neq z$ *then there exists* y' *and* z' *such that* $x \longrightarrow y' \xrightarrow{*} y$ *and* $x \longrightarrow z' \xrightarrow{*} z$.
By local confluence we know that there exists some t *such that* $y' \xrightarrow{*} t$ *and* $z' \xrightarrow{*} t$.
By induction hypothesis and the fact that $x \xrightarrow{+} y'$ *we know that there exists some* u *such that* $y \xrightarrow{*} u$ *and* $t \xrightarrow{*} u$.
By induction hypothesis and the fact that $x \xrightarrow{+} z'$ *we know that there exists some* v *such that* $u \xrightarrow{*} v$ *and* $z \xrightarrow{*} v$.
As $y \xrightarrow{*} u$ *and* $u \xrightarrow{*} v$ *we can deduce that* $y \xrightarrow{*} v$.

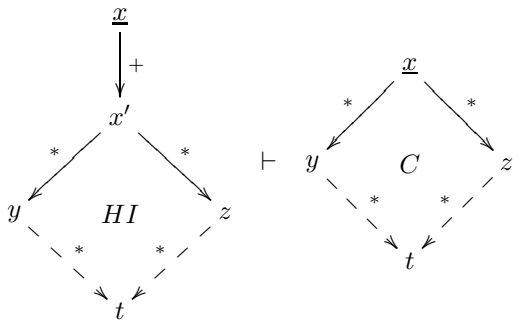
Diagrammatic proof

To shorten the presentation, we omit the diagrams concerning the definitions of $\xrightarrow{+}$ *and* $\xrightarrow{*}$*. We admit that the context contains the diagram about the transitivity of* $\xrightarrow{*}$.

The statement is the following:



by induction over $\longrightarrow$

$\longrightarrow is terminating, CL,$  $\vdash$

using the `intros` *rule:*

$$\longrightarrow is terminating, CL, HI,\ y \overset{*}{\longleftarrow} x \overset{*}{\longrightarrow} z \ \vdash\ \underline{y} - \overset{*}{-} \succ t \prec \overset{*}{-} - \underline{z}$$

by case distinction on $x \overset{*}{\longrightarrow} y$

Case 1

$$\longrightarrow is terminating, CL, HI,\ y \overset{=}{\longleftarrow} x \overset{*}{\longrightarrow} z \ \vdash\ \underline{y} - \overset{*}{-} \succ t \prec \overset{*}{-} - \underline{z}$$

by the `substitute` *rule*

$$\longrightarrow is terminating, CL, HI,\ x \overset{*}{\longrightarrow} z \ \vdash\ \underline{x} - \overset{*}{-} \succ t \prec \overset{*}{-} - \underline{z}$$

by `apply` *using the definition of* $\overset{*}{\longrightarrow}$

$$\longrightarrow is terminating, CL, HI,\ x \overset{*}{\longrightarrow} z\ ,\ z \overset{*}{\longrightarrow} z \ \vdash\ x \overset{*}{\longrightarrow} z \overset{*}{\longleftarrow} z$$

The `conclusion` *rule allows to conclude this case.*

Case 2

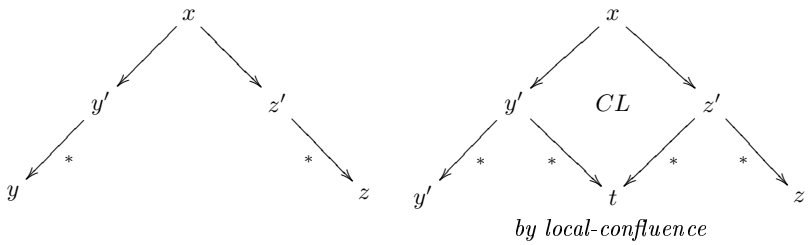
$$\longrightarrow is terminating, CL, HI,\ y \overset{*}{\longleftarrow} y' \longleftarrow x \longrightarrow z \ \vdash\ \underline{y} - \overset{*}{-} \succ t \prec \overset{*}{-} - \underline{z}$$

By case distinction on $x \overset{*}{\longrightarrow} z$

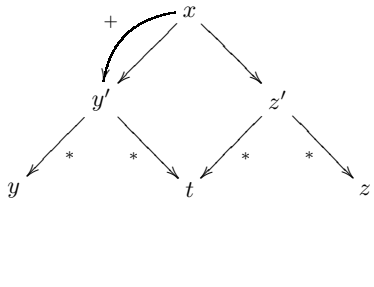
Case 2.1 *is similar to case 1*

Case 2.2

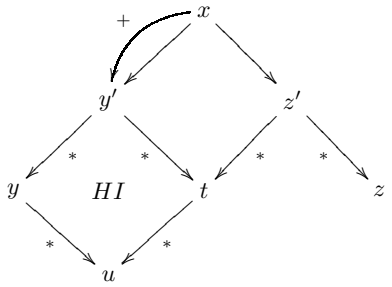
For the end of the proof we represent only the factual hypothesis:



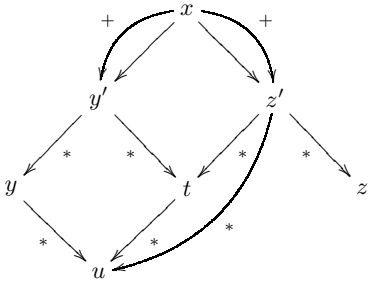
by local-confluence



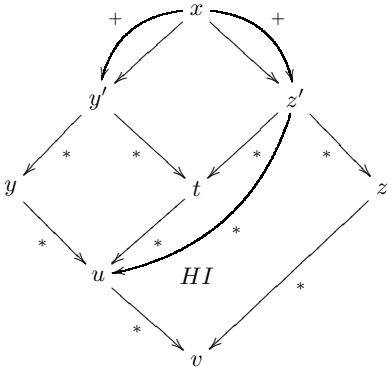
by the definition of $\xrightarrow{+}$



by induction hypothesis

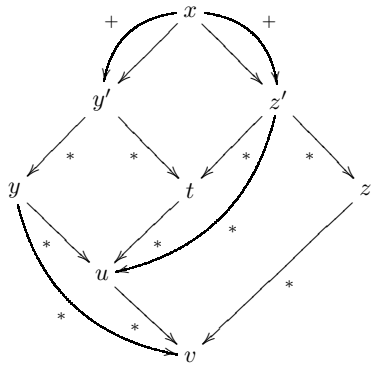


by the definition of $\xrightarrow{+}$ *and transitivity of* $\xrightarrow{*}$



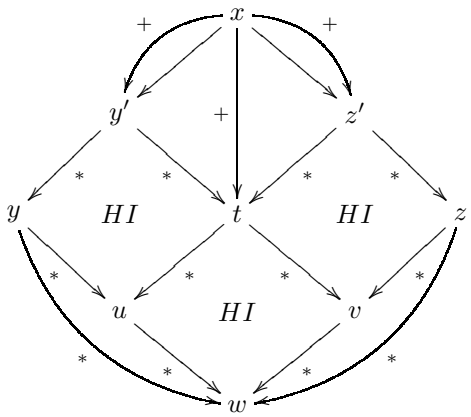
by induction hypothesis

by transitivity of $\xrightarrow{*}$



Note that there is a proof whose final diagram is symmetric. But this proof

uses the induction hypothesis (noted HI on the diagram) three times.



6 Implementation using Coq

The formal system that we have presented can be implemented and used to produce proofs within a proof assistant. We describe here the implementation we have realized using the tactic language of Coq ($\mathcal{L}_{tac}$) [Del01, Del00, Coq04]. We will see that the system we propose produces concise proofs reflecting precisely the diagrammatic proofs.

6.1 Inference rules

We detail here the implementation of the `apply` rule, the other rules can be translated directly using Coq[6].

To build a tactic corresponding to the `apply` rule, we first define a tactic which can find the conclusion of an hypothesis[7]:

```
Ltac conclusion_aux t :=
  match t with
    | ?P1 -> ?P2 => conclusion_aux P2
    | _ => t
end.
```

To implement `apply`, we first prove that the conclusion of the universal diagram is true using the tactics `auto` and `apply_decompose`. Then we decompose the new hypothesis thanks to the left rules for $\vee$,$\wedge$ and $\exists$ using the tactic `decompose`.

```
Ltac decompose_and_clear id :=
 progress (decompose [or and ex] id);clear id.

Ltac apply_decompose H :=
  let t := type of H in
  let conc := conclusion_aux t in
  let id:= fresh in
  (assert (id:conc);[auto|try decompose_and_clear id]).

Ltac apply_diagram H :=
  let id:=fresh in
  (assert (id:=H);apply_decompose id;clear id);
  unfold_all.
```

6.1.1 Example

We give here the proof of the Newman's lemma using Coq.

```
Theorem newman :
 local_confluence S R -> noetherian S R -> confluence S R.
Proof.
intros.
```

[6] Warning, the tactic implemented can prove more goals than the inference rules we have defined. We assume that the tactics are used in the same manner as the inference rules.

[7] We assume that hypothesis are curryfied

```
(* induction *)
assert (ind:=H0 (confluence_in S R));clear H0.
unfold confluence.
apply ind;clear ind.
unfold confluence_in.

start.
rename y into x.
rename y0 into y.

(* First degenerated case *)
apply_diagram (Rstar_cases x y).
substitute y.
apply_diagram (Rstar_cont_eq S R z).
conclusion.

(* Second degenerated case *)
apply_diagram (Rstar_cases x z).
substitute z.
apply_diagram (Rstar_cont_eq S R y).
conclusion.

(* General case *)
start.
apply_diagram (H x x0 x1).
apply_diagram (H0 x0);apply_diagram (H4 y x2).
apply_diagram (Rstar_transitivity x1 x2 x3).
apply_diagram (H0 x1);apply_diagram (H12 x3 z).
apply_diagram (Rstar_transitivity y x3 x4).
conclusion.
Qed.
```

6.2 Implicit rules

As the reader may have already noticed, the diagrammatic proofs using our formal system are very close to the informal proof but they still contain some reasoning steps which do not appear in the informal proof. In the informal proof, some properties are implicit, for example the fact that a relation is contained in its transitive closure.

Now, we explain how these reasoning steps can be made implicit in the Coq implementation.

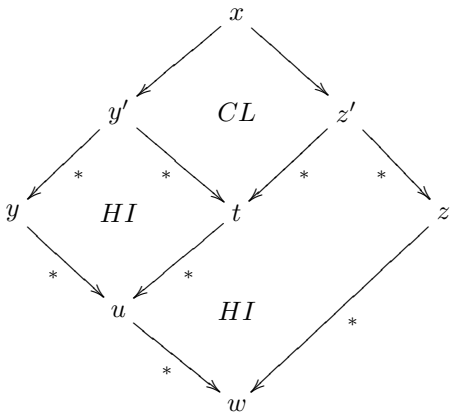
The properties that we choose to keep implicit are the following:

- $\xrightarrow{*}$ is transitive,
- $\xrightarrow{+}$ is transitive,
- $\xrightarrow{*}$ is reflexive,
- $\xrightarrow{*}$ contains $\longrightarrow$,
- $\xrightarrow{+}$ contains $\longrightarrow$.

First we add these properties to a base of «Hints» for Coq. Then we redefine the tactic we have described. These new tactics allows to produce proofs without giving the reasoning steps we have defined as implicit.

```
Ltac Rconclusion :=
   eauto with Rules.
Ltac Rapply_diagram H :=
   apply_diagram H;[idtac|eauto with Rules].
```

The use of these tactics allows to automatise three steps in the proof we have presented above. We obtain the proof corresponding to the usual diagram for the proof of the Newman's lemma:

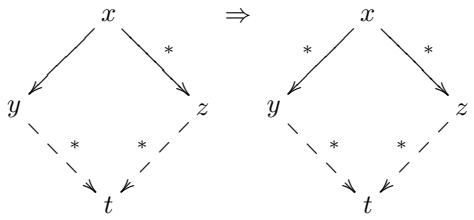


7 Some diagrammatic proofs.

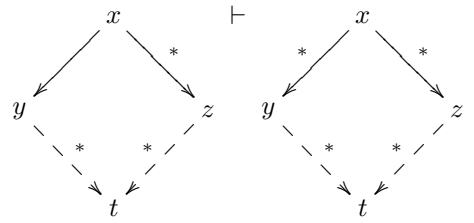
In this section we give some examples of diagrammatic proofs of some common properties.

7.1 Confluence properties

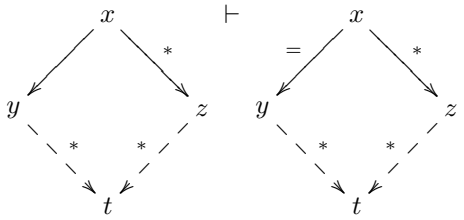
Lemma 5. *Semi-confluence implies confluence.*



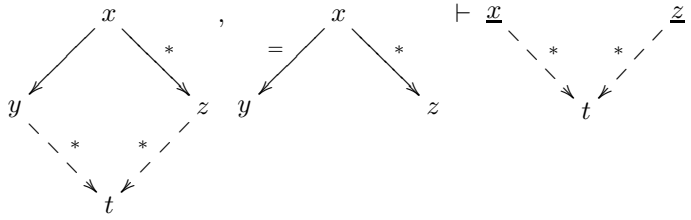
Proof:



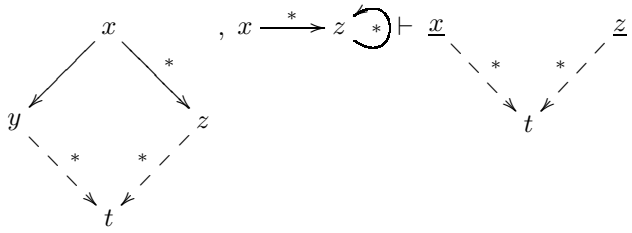
By the rule ind_*
Case 1:



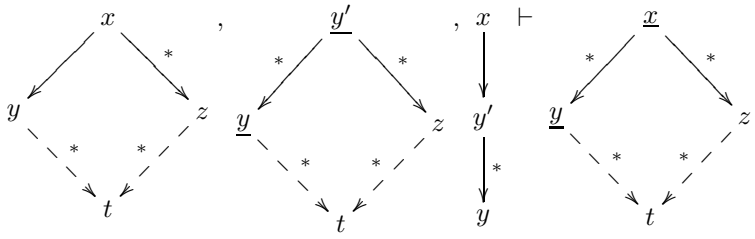
by the rule **intros**



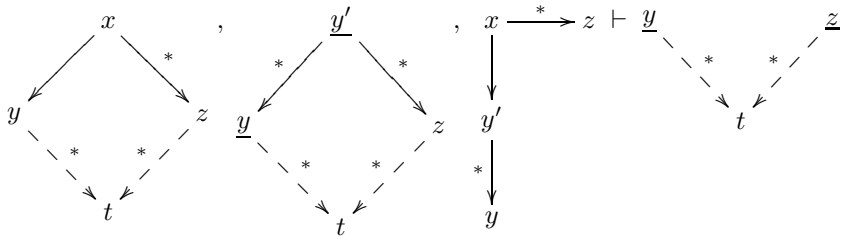
by the rule **apply** *applied to the definition of* $\xrightarrow{*}$



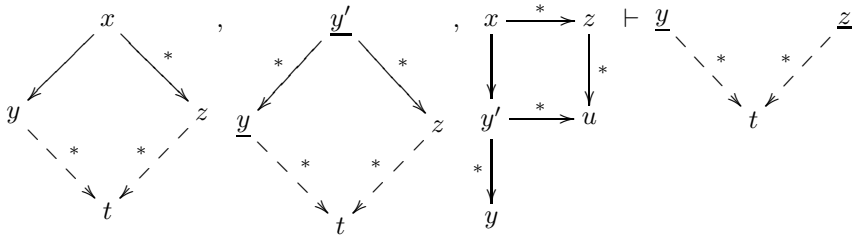
Case 2:



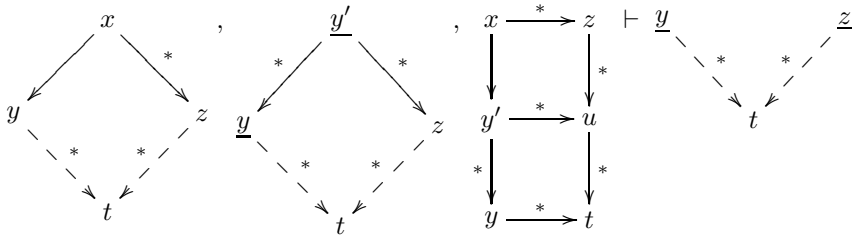
by the rule **intros**



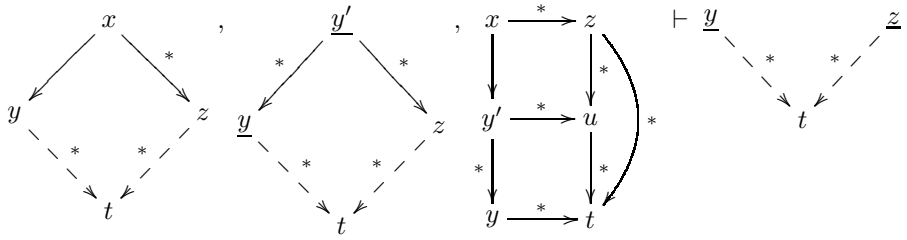
by the rule **apply**



by the rule **apply**

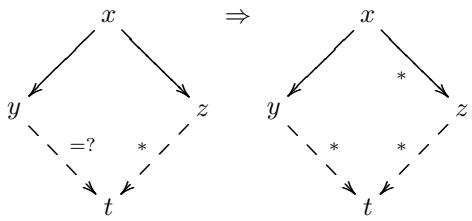


by the rule **apply** *applied to the transitivity of* $\xrightarrow{*}$

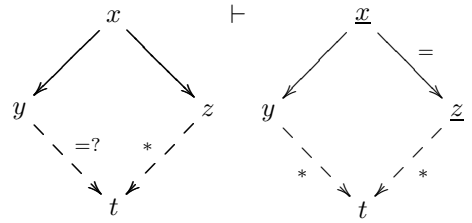


□

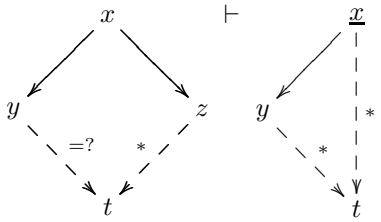
Lemma 6. *Strong-confluence implies semi-confluence.*



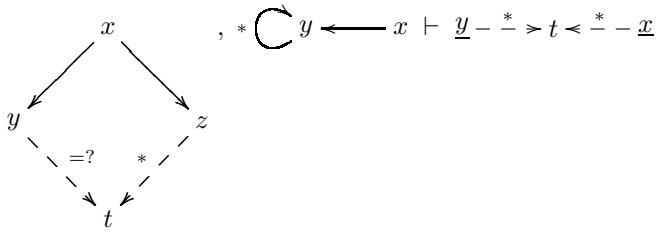
Proof:
by the rule ind_*
Case 1 :



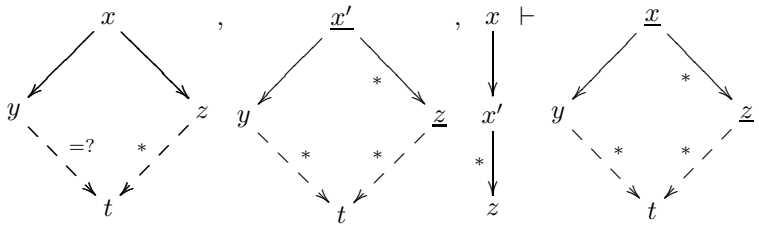
by the rule **substitute**



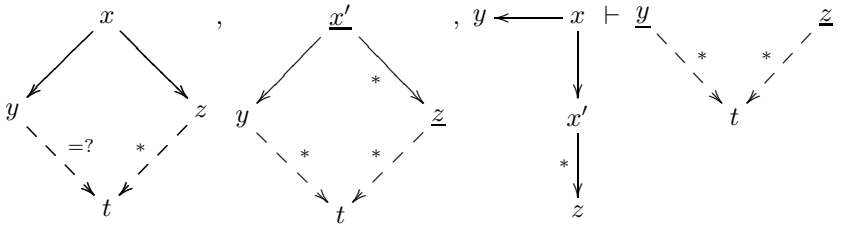
by the rules **intros** *and* **apply**



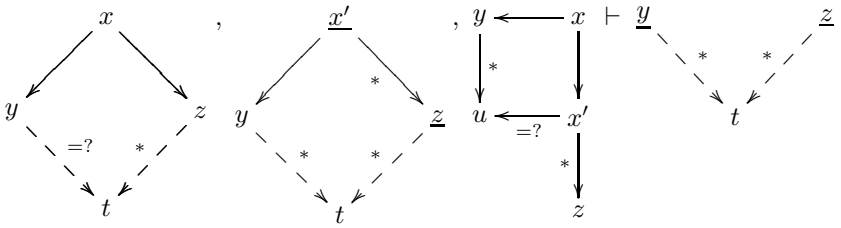
Case 2 :



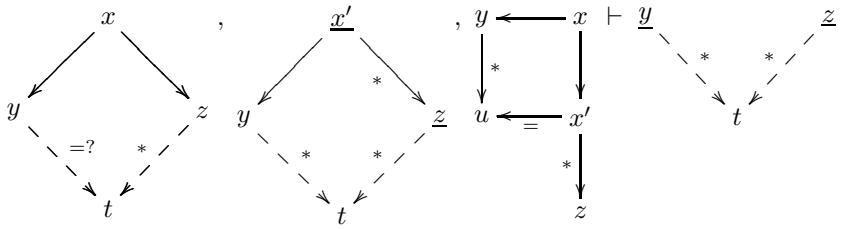
by the rule **intros**



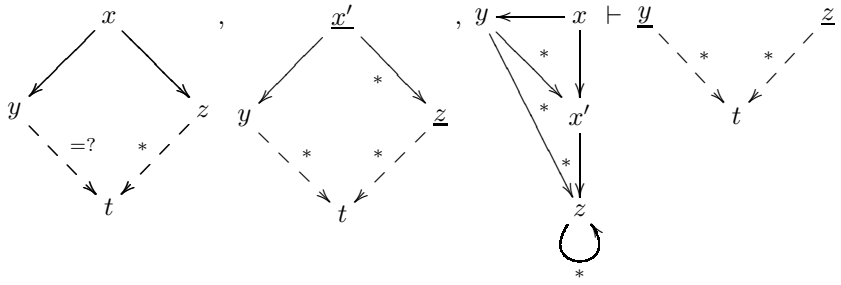
by the rule **apply**



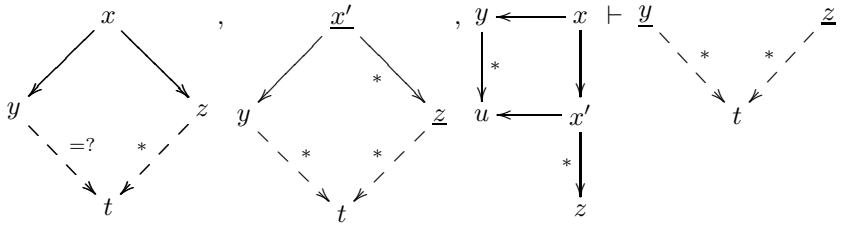
by the rule **apply** *applied to the definition of* $\stackrel{=?}{\longrightarrow}$
Case 2.1 :



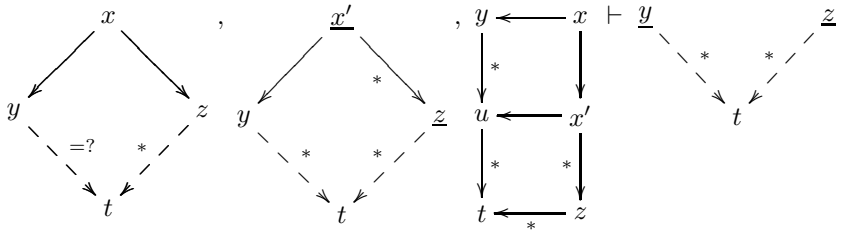
by the rule **substitute** *and the rule* **apply** *applied twice*



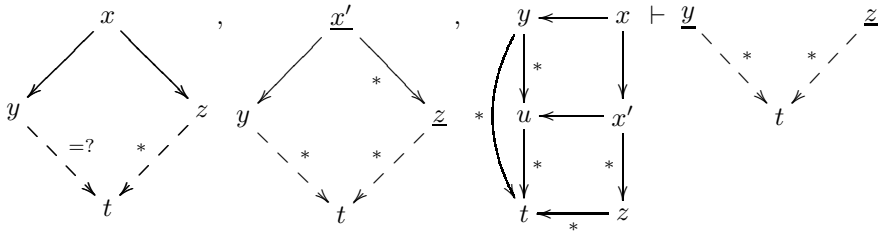
Case 2.2 :



by the rule **apply**

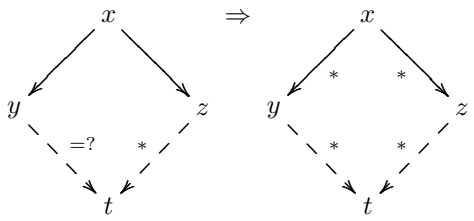


by the rule **apply** *applied to the transitivity of* $\stackrel{*}{\longrightarrow}$



□

Theorem 6. *Strong-confluence implies confluence.*



Proof: By the cut rule. □

8 Conclusion and future work

We have formalized the diagrams used in the literature about abstract rewriting systems. This includes an extension to deal with disjunctions. We have raised the diagrams from the status of a *proof illustration* or *proof hint* to that of a *proof object*. We have proposed a formal system which is both correct and complete for the formulas of the coherent logic restrained to predicates of arity two.

The work presented here should be considered as the foundations for a future implementation. Our aim is to use the formalization presented in this paper to implement a prototype to build diagrammatic proofs about abstract rewriting *interactively*. We have developed a dynamic geometry software called *GeoProof*. It allows the user to create complex geometric constructions step by step, using free objects and predefined atomic constructions depending on other objects. The free objects can be dragged using the mouse and the figure is updated in real time. It can communicate with the Coq proof assistant to state theorems graphically in the field of euclidean geometry.

Our plan is to extend GeoProof from the field of euclidean geometry to abstract rewriting theory. Indeed, the diagrammatic proofs displayed in this paper are very similar to the way a figure is built in a dynamic geometry software. The application of a diagram to some hypotheses for instance is very similar to the execution of a macro in a dynamic geometry environment.

We also plan several extensions of the theory. It would be interesting to explore the representation of the facts which belong to the geometric theories (such as projective geometry) which can be axiomatized using coherent logic. Our framework could also be extended to be able to deal with the numerous diagrammatic proofs of category theory. These multiple possible extensions suggest that coherent logic is well adapted to diagrammatic reasoning.
We think that the two essential components of a diagrammatic reasoning system are the following.
First, facts should be easily visualizable by a syntax which mimic the semantic (for instance the notation for the symmetric closure is symmetric).
Second, for the class of formulas that we manipulate, it must be possible to perform the proofs using this scheme: we start from the hypotheses and complete the diagram in order to obtain an instance of the goal.
Note that in this scheme, the goal does not change during the proof and thus it can therefore remain implicit in the graphical representation. We think that this scheme of reasoning is well adapted to diagrammatic reasoning, and that it would be interesting to find the largest class of formulas for which there exists a complete formal system conforming to this scheme.

Availability.

The Coq files corresponding to this paper are available at the following url:
`http://www.lix.polytechnique.fr/Labo/Julien.Narboux/Rewriting/rewriting.html`

Acknowledgements.

I am indebted to Hugo Herbelin for his help during the elaboration of this work.

References

[BC04] Marc Bezem and Thierry Coquand. Newman's lemma – a case study in proof automation and geometric logic. *Current trends in Theoretical Computer Science*, 2:267–282, 2004.

[BC05] Marc Bezem and Thierry Coquand. Automating coherent logic. In Geoff Sutcliffe and Andrei Voronkov, editors, *12th International Conference, LPAR 2005*, volume 3835 of *Lecture Notes in Computer Science*, pages 246–260. Springer-Verlag, 2005.

[BN98] Franz Baader and Tobias Nipkow. *Term rewriting and all that.* Cambridge University Press, New York, USA, 1998.

[BPB91] Dave Barker-Plummer and Sidney C. Bailin. Proofs and pictures, proving the diamond lemma with the GROVER theorem proving system. AAAI Symposium on Reasoning with Diagrammatic Representations, November 1991.

[BvOK98] Marc Bezem, Vincent van Oostrom, and Jan Willem Klop. Diagram techniques for confluence. *Information and Computation*, 141(2):172–204, March 1998.

[Coq04] Coq development team, The. *The Coq proof assistant reference manual, Version 8.0.* LogiCal Project, 2004.

[Del00] David Delahaye. A Tactic Language for the System Coq. In *Proceedings of Logic for Programming and Automated Reasoning (LPAR), Reunion Island (France)*, volume 1955 of *LNCS/LNAI*, pages 85–95. Springer-Verlag, November 2000.

[Del01] David Delahaye. *Conception de langages pour décrire les preuves et les automatisations dans les outils d'aide à la preuve: une étude dans le cadre du système* Coq. PhD thesis, Université Pierre et Marie Curie (Paris 6), décembre 2001.

[Her05] Olivier Hermant. *Méthodes Sémantiques en Déduction modulo.* PhD thesis, Université Paris 7, 2005.

[HKPM04] Gérard Huet, Gilles Kahn, and Christine Paulin-Mohring. *The* Coq *Proof Assistant - A tutorial - Version 8.0*, April 2004.

[Hue80] Gérard Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, 1980.

[Jam01] Mateja Jamnik. *Mathematical Reasoning with Diagrams: From Intuition to Automation.* CSLI Press, 2001.

[Kle52] Stephen Cole Kleene. Permutability of inferences in Gentzen's calculi LK and LJ. *Memoirs of the American Mathematical Society*, 10:1–26, 1952.

[Mil01] Nathaniel Miller. *A diagrammatic formal system for Euclidean geometry.* PhD thesis, Cornell University, May 2001.

[Nad00] Gopalan Nadathur. Correspondences between classical, intuitionistic and uniform provability. *Theoretical Computer Science*, 232:273–298, 2000.

[Neg03] Sara Negri. Contraction-free sequent calculi for geometric theories with an application to Barr's theorem. *Archives of Mathematic Logic*, 4(42):389–401, 2003.

[New42] Maxwell Herman Alexander Newman. On theories with a combinatorial definition of 'equivalence'. *Annals of Mathematics*, 43(2):223–243, 1942.

[Pfe04] Franck Pfenning. Automated theorem proving handouts, April 2004. draft.

[Win04] Daniel Winterstein. *Using Diagrammatic Reasoning for Theorem Proving in Continous Domain*. PhD thesis, The University of Edinburgh, 2004.