



**HAL**  
open science

# Machine-Checked Categorical Diagrammatic Reasoning

Benoît Guillemet, Matthieu Piquerez, Assia Mahboubi

► **To cite this version:**

Benoît Guillemet, Matthieu Piquerez, Assia Mahboubi. Machine-Checked Categorical Diagrammatic Reasoning. 2024. hal-04471683v1

**HAL Id: hal-04471683**

**<https://inria.hal.science/hal-04471683v1>**

Preprint submitted on 22 Feb 2024 (v1), last revised 29 Feb 2024 (v5)

**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.



Distributed under a Creative Commons Attribution 4.0 International License

# 1 Machine-Checked Categorical Diagrammatic 2 Reasoning


3 Benoît Guillemet

4 École normale supérieure Paris-Saclay, France

5 Assia Mahboubi 

6 Nantes Université, École Centrale Nantes, CNRS, INRIA, LS2N, UMR 6004, France

7 Vrije Universiteit Amsterdam, the Netherlands

8 Matthieu Piquerez 

9 Nantes Université, École Centrale Nantes, CNRS, INRIA, LS2N, UMR 6004, France

---

## 10 Abstract

11 This paper describes a formal proof library, developed using the Coq proof assistant, designed  
12 to assist users in writing correct diagrammatic proofs, for 1-categories. This library proposes a  
13 deep-embedded, domain-specific formal language, which features dedicated proof commands to  
14 automate the synthesis, and the verification, of the technical parts often eluded in the literature.

15 **2012 ACM Subject Classification** Theory of computation → Logic and verification

16 **Keywords and phrases** Interactive theorem proving, Categories, Diagrams, Formal proof automation

17 **Digital Object Identifier** 10.4230/LIPIcs.CVIT.2016.23

## 18 1 Introduction

19 *Abstract nonsense*, a non derogatory expression attributed to Steenrod, usually refers to the  
20 incursion of categorical methods for a proof step deemed both technical and little informative,  
21 and therefore often succinctly described. *Diagrams* are typically drawn in this case, so as to  
22 guide the intuition of the audience, and help visualize the existence of certain morphisms or  
23 objects, identities between composition of morphisms, etc.

24 Formally, a categorical diagram is a functor  $F: J \rightarrow \mathcal{C}$ , with  $J$  a small category called the  
25 *shape* of the diagram [12]. Diagrams are depicted as directed multi-graphs, also called *quivers*,  
26 whose vertices are decorated with the objects of  $\mathcal{C}$  and whose arrows each represent a certain  
27 morphism, between the objects respectively decorating its source and its target. A directed  
28 path in the diagram is hence associated with a chain of composable arrows and a diagram  
29 *commutes* when all directed paths with same source and target lead to equal compositions.  
30 Equalities between compositions of morphisms thus correspond to the commutativity of  
31 certain sub-diagrams of a larger diagram. Chasing commutative sub-diagrams in a larger  
32 diagram provides an elegant alternative to equational reasoning, when the latter becomes  
33 overly technical. Diagrams actually play a central role in category theory, for they provide  
34 such an efficient way of delivering convincing enough proofs. Some classical textbooks  
35 introduce diagrams as early as in their introduction chapter [9], while others devote an entire  
36 section to diagrammatic categorical reasoning [15, Section 1.6] [6, Session 17]. The following  
37 diagrammatic proof of Lemma 1 provides a toy illustrative example of this technique.

38 ► **Lemma 1.** *Let  $\mathcal{C}$  be a category. For any morphism  $f$  and  $g$  such that  $g \circ f \in \text{Hom}(\mathcal{C})$ , if  
39  $g \circ f$  is a monomorphism, then so is  $f$ .*

40 **Proof.** Consider  $f: A \rightarrow B$ ,  $g: B \rightarrow C$  and  $g \circ f: A \rightarrow C$  morphisms in a category  $\mathcal{C}$ . Here  
41 is a very detailed diagrammatic proof, taking place in the diagram of Figure 1.

42 We need to prove that for any two other morphisms  $h, k: D \rightarrow A$  in  $\text{Hom}(\mathcal{C})$  such that  
43  $f \circ h = f \circ k$ , we have  $h = k$ , i.e., that the two-arrow diagram  $h, k$  commutes. By hypothesis



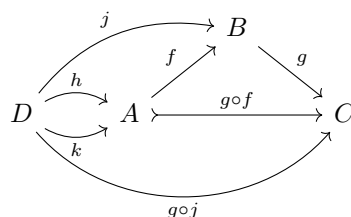
© Jane Open Access and Joan R. Public;  
licensed under Creative Commons License CC-BY 4.0  
42nd Conference on Very Important Topics (CVIT 2016).

Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:16



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



■ **Figure 1** Diagrammatic proof that if  $g \circ f$  is a monomorphism, then so is  $f$

44 on  $h$  and  $k$ , there is an arrow  $j$  such that the triangle diagrams respectively formed by arrows  
 45  $h, f, j$  and  $k, f, j$  both commute. By definition of composition, the triangle diagrams formed  
 46 by arrows  $f, g, g \circ f$  and  $j, g, g \circ j$  also commute. As a consequence, both triangle diagrams  
 47 formed by  $h, g \circ f, g \circ j$  and  $k, g \circ f, g \circ j$  commute. The conclusion follows because  $g \circ f$  is a  
 48 monomorphism. ◀

49 *Diagram chasing* actually refers to a central technique to homological algebra [8, 12],  
 50 operating on diagrams over abelian categories and used for proving the existence, injectivity,  
 51 surjectivity of certain morphisms, the exactness of some sequences, etc. The *five lemma* or  
 52 the *snake lemma* are typical examples of results proved by diagram chasing [8]. However,  
 53 complex diagram chases (see, e.g., [14, p.338]) only remain readable at the price of hiding  
 54 non-trivial technical arguments and are, in practice, challenging to rigorously verify by hand.  
 55 Typically, the reader of a diagrammatic proof is asked to solve instances of variable difficulty  
 56 of a decision problem hereafter referred to as the *commerge* problem: *Given a collection of*  
 57 *sub-diagrams of a larger diagram which commute, must the entire diagram commute?* In  
 58 addition, proofs may resort to non-trivial duality arguments, in which the reader has to  
 59 believe that a property about diagrams in any Abelian category remains true after reversing  
 60 all the involved arrows, although the replay of a given proof *mutatis mutandis* cannot be  
 61 fulfilled in general.

62 The long-term objective of the present work is thus to build a computer-aided instrument  
 63 for devising both fluent and reliable categorical diagrammatic reasoning, for 1-categories.  
 64 The present article describes the implementation of the core of such a tool, as a library for  
 65 the Coq proof assistant [16]. The design of this library follows two main design principles.  
 66 First, it aims at being independent from any specific library of formalized category theory  
 67 or abstract algebra, but rather usable as a helper for any existing one. Second, it should  
 68 feature enough automation tools for synthesizing the bureaucratic parts of proofs "by abstract  
 69 nonsense", and formal proofs thereof. The main contributions presented here are thus:

- 70 ■ a deep-embedded first-order language for category theory, geared towards diagrammatic  
 71 proofs, together with a generic formal definition of categorical diagrams, both based on a  
 72 previous work by two of the authors [10];
- 73 ■ automation support for proofs by duality in the corresponding reified proof system;
- 74 ■ automation support for the *commerge* problem.

75 The corresponding code is available at the following url [3]. The rest of the article is organized  
 76 as follows. Section 2 fixes some vocabulary and describes the corresponding formal definitions.  
 77 Section 3 describes the deep-embedded formalization of the first-order language, and of  
 78 the related reified proof system. Section 4 explains the algorithms involved in automating  
 79 commutativity proofs. We conclude in Section 5 by discussing related work and a few  
 80 perspectives.

## 2 Preliminaries

This section fixes some definitions and notations, and introduces their formalized counterpart when relevant. Some of them coincide with the preliminaries of our previous text [10], for the purpose of being self-contained. The description of their formalized counterpart is novel. We do not display implicit arguments in Coq terms. Throughout this article, we use the word *category* for 1-categories.

In all what follows,  $\mathbb{N} := \{0, 1, \dots\}$  refers to the set of non-negative integers, represented in Coq by the type `nat`, from its standard library. We also use the standard polymorphic type `list` for finite sequences, equipped with the library on sequences distributed by the Mathematical Components [11] library. Some names thus slightly differ from those present in the standard library. For instance, the size  $|l|$  of a finite sequence  $l$ , formalized as `l : list T`, is `size l`, instead of the standard `length l`. We document in comments the definitions we use from this library when their names are not self-explanatory. We recall that `b1 && b2` is the standard notation for the (boolean) conjunction of two boolean values `b1 b2 : bool`. If  $k \in \mathbb{N}$ , then  $[k]$  denotes the finite collection  $\{0, \dots, k - 1\}$ , which is implemented by the sequence `iota 0 n : list nat`.

► **Definition 2** (General quiver, dual). A general quiver  $\mathcal{Q}$  is a quadruple  $(V_{\mathcal{Q}}, A_{\mathcal{Q}}, s_{\mathcal{Q}} : A_{\mathcal{Q}} \rightarrow V_{\mathcal{Q}}, t_{\mathcal{Q}} : A_{\mathcal{Q}} \rightarrow V_{\mathcal{Q}})$  where  $V_{\mathcal{Q}}$  and  $A_{\mathcal{Q}}$  are two sets. The element of  $V_{\mathcal{Q}}$  are called the vertices of  $\mathcal{Q}$  and the element of  $A_{\mathcal{Q}}$  are called arrows. If  $a \in A_{\mathcal{Q}}$ ,  $s_{\mathcal{Q}}(a)$  is called the source of  $a$  and  $t_{\mathcal{Q}}(a)$  is called its target. The dual of a quiver  $\mathcal{Q}$  is the quiver  $\mathcal{Q}^{\dagger} := (V_{\mathcal{Q}}, A_{\mathcal{Q}}, t_{\mathcal{Q}}, s_{\mathcal{Q}})$ , which swaps the source and the target maps of  $\mathcal{Q}$ .

From now on, we casually call *quivers* the special case of quivers with  $V_{\mathcal{Q}}$  a finite subset of  $\mathbb{N}$ . The formal definition moreover assumes that vertices are labelled in order:

```
(* Data of a quiver *)
Record quiver : Type := quiver_Build {
  quiver_nb_vertex : nat; (* number of vertices *)
  quiver_arc : list (nat * nat); (* sequence of arrows *)
}.

(* Well-formedness condition for quivers :
   all arrows involved in A have a source and target in bound *)
Definition quiver_wf '(quiver_Build n A) : bool :=
  all (fun a => (a.1 < n) && (a.2 < n)) A.

(* The dual quiver of a quiver, with same vertices and reversed arrows *)
Definition quiver_dual '(quiver_Build n A) : quiver :=
  quiver_Build n (map (fun a => (a.2, a.1)) A).
```

An arrow of a formalized quiver `q : quiver` is thus given by an element in the sequence `quiver_arc q`, itself a pair of integers giving its source and target respectively. Note that the index in the sequence matters, as the sequence may have duplicate. A formalized quiver is well-formed when the sources and targets of its arrows are in bound.

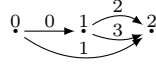
For the sake of readability, we use drawings to describe some quivers, as for instance:



For a quiver  $Q$  denoted by such a drawing, the convention is that  $V_Q = [\text{card}(V_Q)]$  and  $A_Q = [\text{card}(A_Q)]$ , where  $\text{card}(A)$  denotes the cardinal of a finite set  $A$ . From left to right, the

## 23:4 Machine-Checked Categorical Diagrammatic Reasoning

111 drawn vertices correspond to  $0, 1, \dots, \text{card}(V_Q) - 1$ . Arrows are then numbered by sorting  
 112 pairs  $(s_Q, t_Q)$  in increasing lexicographical order, as in:



112

113 ► **Definition 3** (Morphism, embedding, restriction). A morphism of quivers  $m: \mathcal{Q} \rightarrow \mathcal{Q}'$ , is  
 114 the data of two maps  $m_V: V_{\mathcal{Q}} \rightarrow V_{\mathcal{Q}'}$  and  $m_A: A_{\mathcal{Q}} \rightarrow A_{\mathcal{Q}'}$  such that  $m_V \circ s_{\mathcal{Q}} = s_{\mathcal{Q}'} \circ m_A$   
 115 and  $m_V \circ t_{\mathcal{Q}} = t_{\mathcal{Q}'} \circ m_A$ . Such a morphism is called an embedding of quivers if moreover  
 116 both  $m_V$  and  $m_A$  are injective. In this case we write  $m: \mathcal{Q} \hookrightarrow \mathcal{Q}'$ .

117 If  $A$  is a subset of  $A_{\mathcal{Q}}$ , the (spanning) restriction of  $\mathcal{Q}$  to  $A$  denoted by  $\mathcal{Q}|_A$  is the quiver  
 118  $(V_{\mathcal{Q}}, A, s_{\mathcal{Q}|_A}, t_{\mathcal{Q}|_A})$ . There is a canonical embedding  $\mathcal{Q}|_A \hookrightarrow \mathcal{Q}$ .

119 We also use drawings to denote embeddings. The black part represents the domain of the  
 120 morphism, the union of black and gray parts represents its codomain. Here is an example of  
 121 an embedding of the quiver  $\cdot \begin{array}{c} \curvearrowright \\ \curvearrowleft \end{array} \cdot$  into the quiver drawn above.



122

123 For the purpose of this work, we actually only need to define formally embedding  
 124 morphisms, called sub-quivers, which select the relevant vertices and arrows from a quiver:

```
Record subquiver := subquiver_Build {
  subquiver_vertex : list nat; (* labels of the selected vertices *)
  subquiver_arc : list nat; (* indices of the selected arrows *)
}.

(* Spanning morphism *)
Definition subquiver_spanning sA '(quiver_Build n A) :=
  subquiver_Build (iota 0 n) sA.

(* Performs the expected selection of vertices and arrows *)
Definition quiver_restr '(subquiver_Build sV sA) : quiver -> quiver := (...)
```

124

Here as well, restrictions of quiver only make sense under well-formedness conditions:

```
(* Indices of the arrows to be selected are in bound *)
Definition quiver_restr_A_wf sA '(quiver_Build n A) : bool :=
  all (gt n) sA.

Definition quiver_restr_V_wf sV '(quiver_Build n A) : bool :=
  uniq sV && (* sV is duplicate-free *)
  all (gt n) sV && (* all elements of sV are smaller than n *)
  all (fun a => (a.1 \in sV) && (a.2 \in sV)) A. (* any vertex involved in A is in sV *)

(* Well-formed condition on the restriction of a quiver *)
Definition quiver_restr_wf '(subquiver_Build sV sA) Q :=
  quiver_restr_A_wf sA Q && quiver_restr_V_wf sV (quiver_restr_A sA Q).
```

125

126 ► **Definition 4** (Path-quiver). The path-quiver of length  $k$ , denoted by  $PQ_k$ , is the quiver  
 127 with  $k + 1$  vertices and  $k$  arrows  $([k + 1], [k], \text{id}, (i \mapsto i + 1))$ .

128 A path-quiver can be drawn as:

129  $\bullet \longrightarrow \bullet \longrightarrow \bullet \cdots \bullet \longrightarrow \bullet$

130 with at least one vertex. Such a path-quiver is called *nontrivial* if it has at least two vertices.

131 If  $0 \leq k \leq l$  are two integers, we denote by  $\text{sp}_{k,l} : \text{PQ}_k \hookrightarrow \text{PQ}_l$  the leftmost embedding  
 132 of  $\text{PQ}_k$  into  $\text{PQ}_l$ , i.e., such that  $(\text{sp}_{k,l})_V(0) = 0$ . If  $k$  and  $l$  are clear from the context, we  
 133 draw  $\text{sp}_{k,l}$  as  $\sim$  if  $k \neq 0$  and as  $\curvearrowright$  if  $k = 0$ . Moreover, we denote by  $\text{tp}_{k,l} : \text{PQ}_k \hookrightarrow \text{PQ}_l$  the  
 134 rightmost embedding of  $\text{PQ}_k$  into  $\text{PQ}_l$ , i.e., such that  $(\text{tp}_{k,l})_V(k) = l$ . The corresponding  
 135 drawings are  $\curvearrowleft$  and  $\dashrightarrow$ . Moreover, if  $P$  is a nontrivial path-quiver, we define  $\text{st}_P : \bullet \hookrightarrow P$   
 136 to be the embedding mapping the first vertex on the leftmost vertex of  $P$  and the second  
 137 vertex on the rightmost vertex of  $P$ . We denote this embedding  $\curvearrowright$ .

138 If  $\mathcal{Q}$  is a general quiver, a morphism of the form  $p : \text{PQ}_k \rightarrow \mathcal{Q}$ , for some  $k$ , is called a *path*  
 139 of  $\mathcal{Q}$  from  $u$  to  $v$  of length  $k$ , where  $u := p(0)$  and  $v := p(k)$ . If moreover  $p_A$  is injective, it is  
 140 called a *trail* [18]. A trail  $p$  such that  $p_V(0) = p_V(k)$  is called a *cycle*. Two paths  $p_1 : P_1 \rightarrow \mathcal{Q}$ ,  
 141  $p_2 : P_2 \rightarrow \mathcal{Q}$  of  $\mathcal{Q}$  have the same extremities if  $p_1 \circ \text{st}_{P_1} = p_2 \circ \text{st}_{P_2}$ . We denote by  $\mathcal{BP}_{\mathcal{Q}}$ , resp.  
 142  $\mathcal{BT}_{\mathcal{Q}}$ , the set of pairs of paths, resp. of trails, of  $\mathcal{Q}$  having the same extremities. Such a pair  
 143 is called a *bipath*, resp. a *bitrail*. A general quiver is *acyclic* if any path of this quiver is an  
 144 embedding. For an acyclic quiver  $\mathcal{Q}$ ,  $\mathcal{BP}_{\mathcal{Q}}$  and  $\mathcal{BT}_{\mathcal{Q}}$  coincide.

145 Paths in a formal quivers are defined a ternary relation between two vertices and a  
 sequence of arrows:

```
(* Operations on lists:
- ( _ == _ ) is a generic boolean comparison test, in this case for lists of integers
- rcons l x is the list l followed by x
- unzip[1 | 2] l is the list of fst (resp snd) elements of the list of pairs l
- sub p A is the list of elements of A with index in p, in order *)
Definition path (A : seq (nat * nat)) (u : nat) (p : seq nat) (v : nat) : bool :=
(* all elements in p are in bound *)
all (gtn (size A)) p &&
(* p selects in A a list of adjacent arrows from u to v *)
(u :: unzip2 (sub p A) == rcons (unzip1 (sub p A)) v).
```

146 A path  $p$  from a vertex  $u$  to a vertex  $v$  can thus be concatenated to a path  $q$  from vertex  
 147  $v$  to a vertex  $w$ : when endpoints are obvious, we just write  $p \cdot q$  the resulting path from  $u$  to  
 148  $w$ . We sometimes abuse notations and write  $e \cdot p$  and  $p \cdot e$  when one of the paths contains a  
 149 single arrow  $e$ .  
 150

151 We now introduce a special case of relations on pairs of paths with same extremities  
 152 in a quiver, called *path relations*. A path relation is an equivalence relation induced from  
 153 a congruence on the corresponding free category to the quiver. Conversely, in a small  
 154 category, the composition axiom induces a path relation on the underlying quiver. The  
 155 formal definition of path relations is actually independent from that of quiver. A path  
 156 relation is just a family of equivalence relations on sequences of integers, indexed by pairs of  
 integers, that are compatible with the concatenation of paths:

```
Record path_relation := {
  pi_r :> forall u v : nat, relation (seq nat) ;
  pi_equiv : forall u v, equivalence _ (pi_r u v) ;
  pi_cat_stable : forall u v w p' q',
    pi_r u v p p' -> pi_r v w q q' -> pi_r u w (p ++ q) (p' ++ q')}.

```

157

158 Given a formal quiver and a path relation `r : path_relation`, `(pi_r r u v)` is expected  
 159 to be a relation on the paths from vertex `u` to vertex `v`. The full relation on sequences,  
 160 which relates any two sequences, can be used to complete a partial collection of relations,  
 161 e.g., the path relation induced by a certain category on its underlying quiver, avoiding this  
 162 way the need for otherwise cumbersome dependent types.

### 163 3 A two-level approach

#### 164 3.1 Formulas and diagrams

165 Paraphrasing Mc Lane [9], many properties of category theory can be "unified and simplified  
 166 by a presentation with diagrams of arrows". Categorical diagrammatic reasoning consists  
 167 in transforming a proof of category theory into a proof about some quivers, decorated with  
 168 the data of a certain category. Actually, once the appropriate quivers are drawn, the data  
 169 themselves can be forgotten, but for the induced path relation, which is the only relevant  
 170 information for a diagrammatic proof. In [10], we proposed a multi-sorted first-order language  
 171 for category theory, geared towards diagrammatic reasoning: following the structure of a  
 172 formula in this language constructs the quivers associated with the corresponding statement  
 173 of category theory, encoded in the sorts of the variables. We recall its definition:<sup>1</sup>

174 ► **Definition 5.** We define a many-sorted signature  $\Sigma$  with sorts the collection of finite  
 175 quivers. Signature  $\Sigma$  has one function symbol  $\text{restr}_m: Q' \hookrightarrow Q$ , of arity  $Q \rightarrow Q'$ , per each  
 176 injective quiver morphism  $m: Q' \hookrightarrow Q$  between two quivers  $Q$  and  $Q'$ , and one predicate  
 177 symbol  $\text{commute}_Q$ , on sort  $Q$ , for each finite acyclic quiver  $Q$ .

178 ► **Example 6.** Writing the sorts of quantified variables as a subscript of the quantifier, here  
 179 is for instance a predicate of arity  $\cdot \longrightarrow \cdot \times \cdot \longrightarrow \cdot \times \cdot \longrightarrow \cdot$  describing composite of arrows:

$$180 \quad \text{Comp}(x, y, z): \quad \exists \cdot \xrightarrow{\cdot} \cdot w, \quad \text{restr}_{\cdot \xrightarrow{\cdot} \cdot}(w) \approx x \wedge \text{restr}_{\cdot \xrightarrow{\cdot} \cdot}(w) \approx y \\ 181 \quad \wedge \text{restr}_{\cdot \xrightarrow{\cdot} \cdot}(w) \approx z \wedge \text{commute}(w)$$

182 ► **Example 7.** Here is a predicate of arity  $\cdot \xrightarrow{\cdot} \cdot$  describing monomorphisms:

$$183 \quad \text{Mono}(x): \quad \forall \cdot \xrightarrow{\cdot} \cdot w, \quad \text{restr}_{\cdot \xrightarrow{\cdot} \cdot}(w) \approx x \Rightarrow \text{commute}(\text{restr}_{\cdot \xrightarrow{\cdot} \cdot}(w)) \\ 184 \quad \Rightarrow \text{commute}(\text{restr}_{\cdot \xrightarrow{\cdot} \cdot}(w)) \Rightarrow \text{commute}(\text{restr}_{\cdot \xrightarrow{\cdot} \cdot}(x))$$

185 Listing 1 is the formalized counterpart of Definition 5. A term `t : term` is thus either a  
 186 variable `Var n`, named with a natural number `n`, or of the form `Restr m t` for `t` a term  
 187 and `m` a sub-quiver, seen as a morphism of quivers. Observe that the source quiver of this  
 188 morphism is left undefined – it only becomes explicit when the term is evaluated. The type  
 189 `formula` defines a first-order logic whose atoms stand for equality, commutativity or true.  
 190 Quantifiers bind de Bruijn indexes and are annotated with a quiver, the sort of the bound  
 191 variable. Computing the sort of a term thus requires first annotating each of its variables with  
 192 a sort. The sort of a term of the form `Restr m t` is then the quiver obtained by restricting  
 193 the sort of term `t` using `m`.

194 Given a list `l` of quivers, providing a sort to each of its variable, a term `t : term` is  
 195 well-formed in this context, written `term_wf l t`, if `l` is long enough and all the subterms

<sup>1</sup> For the sake of readability, we use here the name  $\Sigma$  for the signature called  $\mathring{\Sigma}$  in [10].

```

Inductive term :=
  | Var of nat (* variable, named with an integer *)
  | Restr of subquiver & term. (* the 'restr' symbol *)

Inductive formula :=
  | Forall of quiver & formula
  | Exists of quiver & formula
  | Imply of formula & formula
  | And of formula & formula
  | FTrue (* Top atom *)
  | Commute of term (* the 'com' symbol *)
  | EqD of term & term. (* the equality symbol*)

```

### ■ Listing 1 Terms and formulas

196 of `t` have a well-formed sort. In a closed formula, the sort of a variable is read on the  
 197 corresponding quantifier. More generally, a formula `f : formula` is well-formed in a context  
 198 `l`, written `wf_formula l f`, if `l` is long enough to provide a sort to each free variable in `f`  
 199 and if all the terms appearing in `f` have a well formed sort.

200 Here is the corresponding formal predicate to Example 7.

```

(* We use a notation for easing the definition of quivers
   without isolated vertices from their arcs*)
Definition monoQ : quiver := {Q [:: (0,1);(0,1);(0,2);(1,2)]}. (* This is  $\begin{array}{c} \bullet \\ \leftarrow \bullet \rightarrow \\ \bullet \end{array}$  *)
Definition mapQ : quiver := {Q [:: (0,1)]}. (* This is  $\bullet \rightarrow \bullet$  *)

(* Lambda_arc constructs a predicate from a sequence of quivers and a formula, the first
   is the arity, providing sorts for the free variables of the second, in order *)
Definition monoF : predicate :=
  Lambda_arc [:: mapQ] (* the one-element arity sequence *)
  (Forall monoQ (
    EqD (Restr {sA [:: 3]} $0) $1
    ==> Commute (Restr {sA [:: 0 ; 2 ; 3]} $0)
    ==> Commute (Restr {sA [:: 1 ; 2 ; 3]} $0)
    ==> Commute (Restr {sA [:: 0 ; 1]} $0))) .

```

201 The interpretation of a term `f : formula` as a Coq statement, in sort `Prop`, is relative to  
 202 a formal *diagram*, which is by definition an instance of the following structure `diagram_type` :

```

Record diagram_package (diagram : Type) := diagram_Pack {
  diagram_to_quiver : diagram -> quiver; (* underlying quiver of a diagram *)
  diagram_restr : subquiver -> diagram -> diagram; (* restriction *)
  eqD : equivalence diagram; (* setoid relation on type diagram *)
  eq_comp : diagram -> path_relation; (* path relation *)
}.

Structure diagram_type := diagram_type_Build {
  diagram_sort :> Type; (* diagram_type coerces to the carrier type *)
  diagram_to_package :> diagram_package diagram_sort;
}.

```

203  
 204 A diagram is thus a term in the carrier type of an instance of structure `diagram_type`,  
 205 which can be seen as a model. A diagram commutes when the associated path relation is  
 206 *full*, i.e., any two paths in the underlying quiver with same source and target are related:



## 23:8 Machine-Checked Categorical Diagrammatic Reasoning

```

Definition commute (d : diagram_type) (D : diagram) :=
  path_total (diagram_sort D) (eq_comp D).

```

207 Formal diagrams can be defined from categories, but not only. For instance, one can  
 208 define an instance of `diagram_type` with the following carrier type:

```

Record zmod_diagram : Type := ZModDiagram {
  zmob : nat -> zmodType;
  zmmmap : forall u v : nat, nat -> {additive zmob u -> zmob v};
  zmdiag_to_quiver : quiver}.

```

208 where `zmodType` is a structure for Abelian groups in the Mathematical Components library,  
 209 and `{additive A -> B}` is the type of morphisms between two Abelian groups `A` and `B`. We  
 210 can now explain how to turn a term `f : formula` into a Coq statement, given a sequence of  
 211 diagrams:

```

Fixpoint formula_eval (d : diagram_type) (stack : list d) (f : formula) : Prop :=
  match f with
  | Forall Q f => forallD D :: diagram_on Q, formula_eval d (D :: stack) f
  | Exists Q f => existsD D :: diagram_on Q, formula_eval d (D :: stack) f
  | Imply f1 f2 => formula_eval d stack f1 -> formula_eval d stack f2
  | And f1 f2 => formula_eval d stack f1 /\ formula_eval d stack f2
  | FTrue => True
  | Commute t => if term_oeval stack t is Some D then commute D else False
  | EqD t1 t2 =>
    match term_oeval stack t1, term_oeval stack t2 with
    | Some DG1, Some DG2 => eqD DG1 DG2
    | _, _ => False
    end
  end.

```

212 where notations `forallD D :: diagram_on Q, P` and `existsD D :: diagram_on Q, P` bind  
 213 variable `D` in `P`, so as to quantify `P` over diagrams `D : d` with underlying quiver  
 214 `diagram_to_quiver D` equal to `Q`. The evaluation `term_oeval stack t : option d` of a term  
 215 `t` in context `stack` defaults to `None` when the context `stack` is too small and otherwise  
 216 computes the possible restriction of the diagrams before the evaluation of the atom using the  
 217 relevant commutativity and equality predicates.

### 219 3.2 Structural duality

220 As briefly alluded to in the conclusion of our previous article [10], it is possible to prove  
 221 a duality theorem at the meta-level of the deep-embedded first-order language. For any  
 222 formula `f : formula`, we define its dual formula `formula_dual f` by dualizing all the quivers  
 223 involved in `f`.

224 Indeed, any type of diagrams `d : diagram_type` has a dual `model_dual d : diagram_type`,  
 225 obtained from `d` by keeping the same data, but dualizing its quiver. We can now prove the  
 226 following property of evaluation in the dual of a diagram:

227 Note that a coercion is hidden in the type of `ctx`, to the common carrier type of `M`  
 228 and `model_dual M`. As a corollary, if a formula is valid in any model, then so is its dual.  
 229 The variant `duality_theorem_with_theory` is equally direct but slightly more interesting, as

```
(* We assume a notion of diagram until the end of the section *)
Variable d : diagram_type.
Theorem formula_eval_duality (M : d) (ctx : seq M) (f : formula) :
  formula_eval (model_dual M) ctx (formula_dual f) <-> formula_eval M ctx f.
```

230 dependent type `P` shall be used to describe a specific class of models, e.g. models of a given theory, provided that their description is "auto-dual":

```
Corollary duality_theorem (ctx : seq d) (f : formula) :
  (forall M : d, formula_eval M ctx f) ->
  forall M : d, formula_eval M ctx (formula_dual f).

Corollary duality_theorem_with_theory (ctx : seq d) (f : formula) (P : d -> Prop) :
  (forall M : model d, P M -> P (model_dual M))
  -> (forall M : d, P M -> formula_eval M ctx f)
  -> forall M : d, P M -> formula_eval M ctx (formula_dual f).
```

231

### 232 3.3 Proofs

233 The deep-embedded level also features a data-structure `valid_proof` for (deep-embedded)  
 234 proofs of deep-embedded formulas, and implements a checker `check_proof` for these proofs. A  
 235 correctness theorem ensures that for any well-formed deep-embedded formula `f : formula`,  
 236 a positive answer of the proof checker entails the provability of the interpretation of `f` in  
 any model `d`:

```
Theorem check_proof_valid (d : diagram_type) (f : formula) (pf : valid_proof) :
  formula_wf [::] f -> check_proof f pf = true -> formula_eval d [::] f.
```

237

238 The deep-embedded level also features a data-structure `sequent`, used to reify a proof in  
 239 progress, and a type `tactic` for actions making progress in a proof:

```
Inductive sequent := sequent_Build {
  context : seq quiver;
  premises : seq formula;
  goal : formula;
}.

Definition tactic := sequent -> option sequent.
```

240 Note that there is only one goal attached to a sequent, as disjunction is not part of our formal  
 241 language. To a sequent with context `[Q_1, ..., Q_n]`, premises `[H_1, ..., H_m]` and goal  
 242 `G`, one can associate the following term in type `formula`:

```
Forall Q_1 ( ... ( Forall Q_n (
  Imply (And H_1 ( ... (And H_m Ftrue) ... )) G )) ... )
```

243 The sequent is well-formed if the corresponding formula is a well-formed formula. In the  
 244 other direction, to any `f : formula`, one can associate the sequent with goal `f` and with  
 245 empty context and no premise. A tactic  $\tau$  is *valid* when for any well-formed sequent  $s$ , if  $\tau s$   
 246 is some  $s'$ , then  $s'$  is also well-formed and the evaluation of  $s'$  implies the evaluation of  $s$ . In  
 247 this context, a *valid proof* is just a list of valid tactics.

## 23:10 Machine-Checked Categorical Diagrammatic Reasoning

248 To check that a valid proof effectively provides a proof of some given formula  $f$ , one can  
249 perform the following steps. First, compute the sequent associated to the formula. Then, for  
250 each tactic in the proof, apply the tactic. If at some point the tactic returns `None` the proof  
251 is not correct. Otherwise, check that the goal of the final sequent is `FTrue`. If this is the  
252 case, then the evaluation of  $f$  is true. In the implementation, the verification is performed  
253 by the function `check_proof`, and the conclusion is proven in Theorem `check_proof_valid`.

254 The next step is to implement a set of *useful* tactics, and to prove that they are valid.  
255 This has been done for basic tactics like introduction and elimination rules, or for more  
256 involved tactics like the `Rewrite` tactic, or the `Comauto` tactic, for automating the proof  
257 of commutative atoms. Starting from the rules of the proof system, more complex tactics  
258 combine existisng ones in a relevant way, so as to considerably reduce the size of the proofs.  
259 In order to be valid, some tactics may also require more assumptions from the model (the  
260 type of diagrams) used to evaluate the formulas.

261 Here is for instance the statement of the formula corresponding to Lemma 1, using an  
infix notation `-->` for the `ImPLY` constructor of type `formula` :

```
(*when the quiver of a formula have no isolated vertex, formula_fill_vertices  
allows for a shorter description of quivers, only by their arcs.*)  
Definition mono_monomPF : formula :=  
formula_fill_vertices [::] (  
  Forall compQ (  
    Commute $0 --> monoF App (Restr {sA [:: 1]} $0) --> monoF App (Restr {sA [:: 0]} $0))).
```

262 The reified proof of this statement is currently done by applying successively twelve  
263 tactics.<sup>2</sup>

264 In fact, duality arguments are implemented by instrumenting proofs so as to check that  
265 they are amenable to duality arguments, which is more convenient in practice than the  
266 structural argument described in Section 3.2. We thus identify tactics  $\tau$  that commutes with  
267 duality, i.e., such that for any sequent  $s$ , the dual of  $\tau s$  is equal to  $\tau$  applied to the dual of  
268  $s$ . Theorem `duality_theorem`, ensures that, indeed, if all tactics of a proof of some formula  
269 verifies this principle, then this will also be a proof of the dual formula.<sup>3</sup>

```
(* Biproofs are pairs of proofs of same size *)  
Structure biproof := biproof_Build {  
  biproof_primal : proof;  
  biproof_dual : proof;  
  biproof_eq_size : size biproof_primal == size biproof_dual;  
}.  
  
Theorem duality_theorem f (bpf : biproof) :  
(* assuming that the tactics in the pair of proofs bpf are pairwise dual *)  
biproofD bpf ->  
(* then the primal proof proves a formula iff the dual proof proves its dual *)  
check_proof (formula_dual f) (biproof_dual bpf) =  
check_proof f (biproof_primal bpf).
```

271 All the tactics currently implemented verify this principle (though for some of them, the  
272 proof has not yet been written). A duality argument can be used to prove the dual statement

<sup>2</sup> See `mono_monom_pf` in file `diagram_chasing/mono_monom.v`

<sup>3</sup> See file `diagram_chasing/FanL.v`

273 to Lemma 1, and we provide the corresponding deep-embedded formula.<sup>4</sup>

274 ► **Lemma 8.** *Let  $\mathcal{C}$  be a category. For any morphism  $f$  and  $g$  such that  $g \circ f \in \text{Hom}(\mathcal{C})$ , if*  
 275  *$g \circ f$  is an epimorphism, then so is  $g$ .*

276 **Proof.** From Lemma 1, by duality. ◀

```

Definition epiF :=
  Lambda_arc [:: mapQD]
  (Forall monoQD (
    EqD (Restr {sA [:: 3]} $0) $1
    ==> Commute (Restr {sA [:: 0 ; 2 ; 3]} $0)
    ==> Commute (Restr {sA [:: 1 ; 2 ; 3]} $0)
    ==> Commute (Restr {sA [:: 0 ; 1]} $0))).

Definition epi_mepiPF : formula :=
  formula_fill_vertices [::] (
    Forall compQD (
      Commute $0 ==> epiF App (Restr {sA [:: 1]} $0) ==> epiF App (Restr {sA [:: 0]} $0))).
  
```

277 which is similar to term `monoPF` and formula `mono_monomPF` except that quivers `monoQ`  
 278 and `compQ` have been dualized, respectively into `monoQ` and `compQ`. The reified proof takes  
 279 a single tactic, which dualizes the proof of the statement on monomorphisms.

## 280 4 Automating commutativity proofs

281 In order to apply most lemmas obtained by diagram chasing, one first has to prove that  
 282 a certain diagram is commutative. For instance, the so-called *five lemma*, which allows to  
 283 prove that some map is an isomorphism, requires to have a commutative diagram over the  
 284 quiver of Figure 2. Yet proving that such a diagram is commutative by checking one equality  
 285 per bipaths in this diagram would be excessively tedious. Commutativity of a larger diagram  
 286 is typically obtained from the commutativity of certain sub-diagrams, and the proof of this  
 287 implication is often little detailed, or not at all. For instance, in the case of Figure 2, it  
 288 actually suffices to check four equalities, one for each sub-square of the quiver. More precisely,  
 289 each pair of paths going from the top-left corner to the bottom-right corner must correspond  
 290 to equal morphisms. Once these four equalities has been proven, we infer that each square  
 commutes.<sup>5</sup>

$$\begin{array}{ccccccccc}
 A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E'
 \end{array}$$

■ **Figure 2** The five-lemma diagram.

291

292 In section 4.1, we describe an algorithm for deciding the commerge problem for diagrams  
 293 with acyclic underlying quivers, so as for instance to automate the proof that the diagram of  
 294 Figure 2 commutes as soon as the aforementioned four bipaths commute. In section 4.2, we

<sup>4</sup> See file `tests_and_examples/mono_monom.v`

<sup>5</sup> See file `diagram_chasing/Bipath.v` for a formalized proof.

295 describe a heuristic for discovering a collection of sub-diagrams whose commutativity entails  
 296 that of a larger one.

#### 297 4.1 Decision procedure for the commerge problem

298 In [10], we provided a pen-and-paper proof of the decidability of the commerge problem  
 299 for diagrams with acyclic underlying quiver, and the undecidability of its generalization to  
 300 possibly cyclic underlying quivers. In this section, we describe the more practical algorithm  
 301 implemented by the tactic `Comauto`. In particular, this implementation comes with a formal  
 302 proof of correctness, which is the main ingredient in the validity proof of the corresponding  
 303 tactic.

304 The algorithm operates on an acyclic quiver  $\mathcal{Q}$  and a collection  $l \in \mathcal{BP}_{\mathcal{Q}}$  of bipaths,  
 305 representing the commutativity assumptions. It checks whether  $cl_{\mathcal{Q}}(l)$ , the smallest path  
 306 relation induced by  $l$ , is full, that is  $cl_{\mathcal{Q}}(l) = \mathcal{BP}_{\mathcal{Q}}$ . Without loss of generality, we can assume  
 307 that the acyclic quiver  $\mathcal{Q}$  is topologically sorted in reverse order, that is, that any path in  $\mathcal{Q}$   
 308 follows a sequence of vertices with decreasing labels. The implementation actually performs  
 309 a topological sort of the quiver<sup>6</sup> and updates the representation of  $cl_{\mathcal{Q}}(l)$  accordingly.

310 For any given vertices  $u$  and  $v$  in  $V_{\mathcal{Q}}$ , we introduce  $\mathcal{A}_{u,v} \subset A_{\mathcal{Q}}$  the set of adjacent arrows  
 311 of  $u$  starting a path to  $v$  in  $\mathcal{Q}$  and  $\overline{\mathcal{A}}_{v,u} \subset A_{\mathcal{Q}}$  that of adjacent arrows of  $v$  ending a path  
 312 from  $u$  in  $\mathcal{Q}$ :

$$313 \quad \mathcal{A}_{u,v} \triangleq \{e \in A_{\mathcal{Q}} \mid \exists p, e \cdot p \text{ is a path from } u \text{ to } v\}$$

$$314 \quad \overline{\mathcal{A}}_{v,u} \triangleq \{e \in A_{\mathcal{Q}} \mid \exists p, p \cdot e \text{ is a path to } v \text{ from } u\}$$

315 We define  $\mathcal{G}_{u,v}$  the multigraph whose vertices are the elements of  $\mathcal{E}_{u,v} \triangleq \mathcal{A}_{u,v} \cup \overline{\mathcal{A}}_{v,u}$ . An arc  
 316 of  $\mathcal{G}_{u,v}$  relates vertices  $e_1, e_2 \in \mathcal{E}_{u,v}$  when:

- 317 ■ either there is a path from  $u$  to  $v$  containing both  $e_1$  and  $e_2$ ;
- 318 ■  $e_1$  appears in a path of a bipath in  $l$  from  $u$  to  $v$ , and so does and  $e_2$ .

319 We moreover introduce the binary relation  $R_{u,v}$ , on the elements of  $\mathcal{E}$ : for any  $e_1, e_2 \in \mathcal{E}$ ,  
 320  $R_{u,v}(e_1, e_2)$  holds if and only if any path  $p_1$  from  $u$  to  $v$  containing  $e_1$  is related by  $cl_{\mathcal{Q}}(l)$  to  
 321 any any path  $p_2$  from  $u$  to  $v$  containing  $e_2$ . If  $R_{u,v}$  is full, then  $cl_{\mathcal{Q}}(l)$  contains all the pairs  
 322 of paths from  $u$  to  $v$ .

323 ► **Lemma 9.** *For any vertices  $u, v \in V_{\mathcal{Q}}$ , if  $\mathcal{G}_{u,v}$  is connected, then  $R_{u,v}$  is full.*

324 The decision procedure constructs the multigraphs  $\mathcal{G}_{u,v}$  for any pair of vertices, and checks  
 325 that they are all connected. If so, then  $cl_{\mathcal{Q}}(l)$  contains  $\mathcal{BP}_{\mathcal{Q}}$ .

326 **Proof.** We prove Lemma 9 for vertices respectively labelled  $u+n$  and  $u$ , for a vertex  $u \in V_{\mathcal{Q}}$ ,  
 327 by induction on  $n$ . When  $n = 0$ , then the result holds because paths are empty.

328 We now assume that the result holds for any  $u$  and any  $k < n$ , and that  $\mathcal{G}_{u+n,u}$  is  
 329 connected. Observe first that as a consequence of the induction hypothesis, and because  
 330 the graph is topologically sorted in reverse order, any two paths from  $u+n$  to  $u$  sharing  
 331 their initial or their final arrow are in  $cl_{\mathcal{Q}}(l)$ . We now fix  $u \in V_{\mathcal{Q}}$  and  $e_1, e_2 \in \mathcal{E}_{u+n,u}$  and  
 332 we need to prove that  $R_{u+n,u}(e, e')$ . We proceed by induction on the length of a path in  
 333  $\mathcal{G}_{u+n,u}$  relating  $e_1$  and  $e_2$ . If this path is empty, then  $e_1 = e_2$  is either an element of  $\mathcal{A}_{u,v}$  or  
 334 of  $\overline{\mathcal{A}}_{v,u}$  and we can conclude using the initial observation. We now suppose that there is an

<sup>6</sup> See `diagram_chasing/TopologicalSort.v`

335 arc  $e \in \mathcal{E}_{u+n,u}$  and a path  $t$  in  $\mathcal{G}_{u+n,u}$  such that  $(e_1, e)$  is an arc of  $\mathcal{G}_{u+n,u}$  and  $t$  is a path  
 336 from  $e$  to  $e_2$  in  $\mathcal{G}_{u+k,u}$  for a  $k < n$  (the other cases are similar). Let  $p_1$  (resp.  $p_2$ ) be a path  
 337 in  $\mathcal{Q}$  containing  $e_1$  (resp.  $e_2$ ). If there is a path  $p$  in  $\mathcal{Q}$  from  $u$  to  $v$  containing both  $e$  and  $e_1$   
 338 then  $p$  is related to  $p_1$ , by the observation, as the two paths share either their initial or their  
 339 final arrow. But  $p$  is also related to  $p_2$  by the (second) induction hypothesis as  $p$  contains  $e$   
 340 and  $p_2$  contains  $e_2$ . The conclusion follows by transitivity of the path relation. Now suppose  
 341 that  $e$  and  $e_1$  respectively belong to  $q$  and  $q_1$ , paths in  $l$ . Paths  $q_1$  and  $q$  are related, by  
 342 definition of  $\text{cl}_{\mathcal{Q}}(l)$ . But  $q$  and  $p_2$  are also related by the (second) induction hypothesis, as  
 343 the respectively contain  $e$  and  $e_2$ . The conclusion follows by transitivity. ◀

## 344 4.2 Finding sufficient commutativity conditions

345 In fact, one can even use the computer to guess a sufficient list of equalities entailing that a  
 346 certain diagram commutes, instead of providing it explicitly by hand. In this section, we  
 347 explain how to do so in practice. The corresponding algorithm has been implemented under  
 348 the name *comcut*. Although not strictly needed for the purpose of a tactic, its correctness  
 349 has been proven formally.<sup>7</sup>

350 Let  $\mathcal{Q}$  be a quiver with vertices  $V = [n]$ , for some  $n \in \mathbb{N}$ , and arcs  $A_{\mathcal{Q}}$ . Moreover, we  
 351 assume that  $\mathcal{Q}$  is topologically sorted in a reversed order, i.e., if an arc goes from  $u$  to  $v$ ,  
 352 then  $u > v$ . From such an input, *comcut* returns a list of bipaths  $l \subseteq \mathcal{BP}_{\mathcal{Q}}$  such that  $\text{cl}_{\mathcal{Q}}(l)$ ,  
 353 the smallest path relation containing  $l$  is  $\mathcal{BP}_{\mathcal{Q}}$ .

354 The algorithm works by induction on the size of  $\mathcal{Q}$ . Let  $u_0 := n - 1$  be the top vertex. If  
 355 there is no arc whose source is  $u_0$ , then we just have to apply *comcut* to  $\mathcal{Q}$  deprived from the  
 356 vertex  $u_0$  (note that  $u_0$  cannot be a target). Otherwise, let  $a_0 \in A$  be an arc with source  $u_0$ .  
 357 Denote by  $v_0$  the target of  $a_0$ . Consider the quiver  $\mathcal{Q}'$  obtain from  $\mathcal{Q}$  by removing the arc  $a_0$ .  
 358 Applying the algorithm to  $\mathcal{Q}'$ , we get a list  $l' \subset \mathcal{BP}'_{\mathcal{Q}'}$  such that  $\text{cl}'_{\mathcal{Q}'}(l') = \mathcal{BP}'_{\mathcal{Q}'}$ . We complete  
 359 this list to a list  $l$  as follows. Let  $\widetilde{W} := \text{acc}(u_0) \cap \text{acc}(v_0)$  be the set of vertices accessible  
 360 both from  $u_0$  and from  $v_0$  in  $\mathcal{Q}'$ . Set

$$361 \quad W := \{w \in \widetilde{W} \mid \forall w' \in \widetilde{W} \setminus \{w\}, w \notin \text{acc}(w')\}.$$

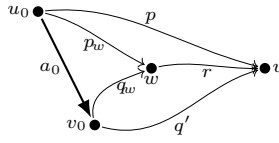
362 For each  $w \in W$ , select a path  $p_w$  from  $u_0$  to  $w$  in  $\mathcal{Q}'$  and a path  $q$  from  $v_0$  to  $w$  in  $\mathcal{Q}'$ . Set  
 363  $l := l' \cup \{(p_w, (a_0) \cdot q_w) \mid w \in W\}$ .

364 ▶ **Proposition 10.** *The list  $l$  constructed above verifies  $\text{cl}_{\mathcal{Q}}(l) = \mathcal{BP}_{\mathcal{Q}}$ .*

365 Before proving the proposition, let us quickly explain how to get an effective implementa-  
 366 tion from the above description. To be able to compute accessibility and to reconstruct the  
 367 different paths, one computes a square matrix indexed by vertices whose  $(u, v)$  entry is either  
 368 empty if there is no nontrivial path from  $u$  to  $v$ , or contains an arc  $a$  such that there is a  
 369 path from  $u$  to  $v$  which starts by  $a$ . To update such a matrix for the quiver  $\mathcal{Q}'$  into a matrix  
 370 corresponding to the quiver  $\mathcal{Q}$ , it suffices to set  $a_0$  to all the entries of the form  $(u_0, v)$  for  
 371  $v \in \text{acc}(v_0)$ . The rest of the algorithm is easy to write down.

372 **Proof.** Let  $p, q$  be paths from  $u$  to  $v$  in  $\mathcal{Q}$ . Note that the arc  $a$  can only appear as the first  
 373 element of  $p$  and  $q$ . If  $a$  does not appear in  $p$  nor in  $q$ , or if it appears in both, then  $(p, q)$   
 374 was already in  $\mathcal{BP}_{\mathcal{Q}}(l')$ . Hence, up to symmetry, it remains the case where  $u = u_0$ ,  $p$  belongs  
 375 to  $\mathcal{Q}'$  and  $q = (a_0) \cdot q'$  with  $q'$  a path of  $\mathcal{Q}'$ . By definition of  $\widetilde{W}$ ,  $v \in \widetilde{W}$ . Let  $w \in W$  such  
 376 that  $v$  is accessible from  $w$ . Let  $r$  be a path from  $v$  to  $w$  (cf. Figure 3). Then,  $(p, p_w \cdot r)$  and

<sup>7</sup> See the folder *comcut*



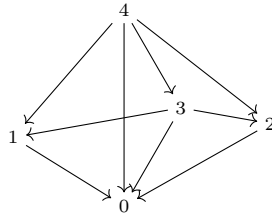
■ **Figure 3** Decomposition of the relation between two paths thanks to an element  $w \in W$ .

377  $(q_w \cdot r, q')$  both belong to  $\mathcal{BP}'_Q$ , and  $(p_w, (a_0) \cdot q_w)$  belongs to  $l$ . Hence we get the following  
 378 sequence of relations in  $\mathcal{cl}_Q(l')$ .

379 
$$p \sim p_w \cdot r \sim (a_0) \cdot q_w \cdot r \sim (a_0) \cdot q' = q,$$

380 which proves the proposition. ◀

381 ▶ **Remark 11.** Note that it may happen that  $l$  is not minimal, see Figure 4 for a counterexample.



■ **Figure 4** Counter example to the minimality of the comcut algorithm. Before adding the arc  $(4, 3)$ , we need four equalities to ensure the commutativity. Adding  $(4, 3)$  force to add two more relations, but one of the previous relations becomes useless.

382

383 **5 Conclusion**

384 We have described a first step towards the implementation of a generic library for writing  
 385 reliable categorical diagrammatic proofs, available online [3]. Such a library can serve two  
 386 purposes. The first one is to assist mathematician authors in writing reliable proofs, the other  
 387 is to provide the mandatory infrastructure for expanding the existing corpus of formalized  
 388 category theory, but also of formalized algebraic topology, and homological algebra. As  
 389 expressed by the MATHLIB community [7], the lack for such a tool is major showstopper for  
 390 the latter. However, the current state of the present library arguably only provides a low  
 391 level language for categorical statements and the next steps should enrich the collection of  
 392 formula combinators, e.g. for limits, pullbacks, etc. as well as the gallery of diagram models.

393 Independence from any library of category theory is achieved by hosting a dedicated proof  
 394 system inside that of a proof assistant, Coq in this case, following the classic formalization  
 395 technique of *deep-embedding* [2]. Dependent types allow to formalize a structural duality  
 396 property for this language. We are not aware of any comparable formal-proof-producing  
 397 automation tactics for proving the commutativity of diagrams, nor for performing duality  
 398 arguments. However, some existing libraries of formalized category theory, notably Mathlib,  
 399 for the Lean proof assistant, and Unimath, a Coq library for univalent mathematics, provide  
 400 some tools to ease proofs by diagram chasing, either with brute-force rewrite-based tactics, or

401 with a graphical editor for generating proof scripts [5]. Other existing libraries of formalized  
 402 category theory, including Jacobs and Timany’s [17], do not include any specific support  
 403 for diagrammatic proofs. We refer the interested reader to the later article for a survey of  
 404 existing libraries of formalized category theory, which remains quite relevant for the purpose  
 405 of this discussion, to the notable exception of the more recent **Mathlib** chapter on category  
 406 theory. The later serves as a basis for Himmel’s formalization of abelian categories in **Lean** [4],  
 407 including proofs of the five lemma and of the snake lemma, and proof (semi-)automation  
 408 tied to this specific formalization. Duality arguments are not addressed. Also in the **Mathlib**  
 409 ecosystem, Monbru [13] also discusses automation issues in diagram chases, and provides  
 410 heuristics for generating them automatically, albeit expressed in a pseudo-language.

411 Other computer-aided tools exist for diagrammatic categorical reasoning, with a specific  
 412 emphasis on the graphical interface. Notably, the accomplished **Globular** proof assistant [1]  
 413 stems from similar concerns about the reliability of diagrammatic reasoning, but for higher  
 414 category theory. It is geared towards visualization rather than formal verification and  
 415 implements various algorithms for constructing and comparing diagrams in higher categories.  
 416 Barras and Chabassier have designed a graphical interface for diagrammatic proofs which  
 417 also provides a graphical interface for generating **Coq** proof scripts of string diagrams, and  
 418 visualizing **Coq** goals as diagrams. But up to our knowledge, this tool does not include any  
 419 specific automation.

## 420 — References —

- 421 1 Krzysztof Bar, Aleks Kissinger, and Jamie Vicary. **Globular**: an online proof assistant for higher-  
 422 dimensional rewriting. *Log. Methods Comput. Sci.*, 14(1), 2018. doi:10.23638/LMCS-14(1:  
 423 8)2018.
- 424 2 Richard J. Boulton, Andrew D. Gordon, Michael J. C. Gordon, John Harrison, John Herbert,  
 425 and John Van Tassel. Experience with embedding hardware description languages in HOL. In  
 426 *TPCD*, volume A-10 of *IFIP Transactions*, pages 129–156. North-Holland, 1992.
- 427 3 Benoît Guillemet, Assia Mahboubi, and Matthieu Piquerez. **coq-diagram-chasing**. <https://gitlab.inria.fr/mpiquere/coq-diagram-chasing>, 2024.  
 428
- 429 4 Markus Himmel. Diagram chasing in interactive theorem proving. Bachelorarbeit. Karls-  
 430 ruher Institut für Technologie, 2020. [https://pp.ipd.kit.edu/uploads/publikationen/  
 431 himmel20bachelorarbeit.pdf](https://pp.ipd.kit.edu/uploads/publikationen/himmel20bachelorarbeit.pdf).
- 432 5 Ambroise Lafont. A categorical diagram editor to help formalising commutation proofs.  
 433 <https://amblafont.github.io/graph-editor/index.html>, 2024. Short paper presented in  
 434 the Journées Francophones des Langages Applicatifs.
- 435 6 F. William Lawvere and Stephen H. Schanuel. *Conceptual mathematics. A first introduction  
 436 to categories*. Cambridge: Cambridge University Press, 2nd ed. edition, 2009.
- 437 7 leanprover-community/mathlib. Condensed mathematics/snake lemma. [https://leanprover-community.github.io/archive/stream/267928-condensed-mathematics/  
 438 topic/snake.20lemma.html](https://leanprover-community.github.io/archive/stream/267928-condensed-mathematics/topic/snake.20lemma.html), 2021.
- 439
- 440 8 Saunders Mac Lane. *Homology*. Class. Math. Berlin: Springer-Verlag, reprint of the 3rd corr.  
 441 print. 1975 edition, 1995.
- 442 9 Saunders Mac Lane. *Categories for the working mathematician.*, volume 5 of *Grad. Texts  
 443 Math*. New York, NY: Springer, 2nd ed edition, 1998.
- 444 10 Assia Mahboubi and Matthieu Piquerez. A first order theory of diagram chasing. In *CSL*,  
 445 volume 288 of *LIPICs*, pages 38:1–38:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik,  
 446 2024.
- 447 11 Assia Mahboubi and Enrico Tassi. *Mathematical Components*. Zenodo, January 2021. doi:  
 448 10.5281/zenodo.4457887.



## 23:16 Machine-Checked Categorical Diagrammatic Reasoning

- 449 12 J. Peter May. *A concise course in algebraic topology*. Chicago, IL: University of Chicago Press,  
450 1999.
- 451 13 Yannis Monbru. Towards automatic diagram chasing. M1 report. École Normale Supérieure  
452 Paris-Saclay, 2022. [https://github.com/ymonbru/Diagram-chasing/blob/main/MONBRU\\_](https://github.com/ymonbru/Diagram-chasing/blob/main/MONBRU_Yannis_Rapport.pdf)  
453 [Yannis\\_Rapport.pdf](https://github.com/ymonbru/Diagram-chasing/blob/main/MONBRU_Yannis_Rapport.pdf).
- 454 14 Matthieu Piquerez. *Tropical Hodge theory and applications*. PhD thesis, Institut Polytechnique  
455 de Paris, November 2021. URL: <https://theses.hal.science/tel-03499730#>.
- 456 15 Emily Riehl. *Category Theory in Context*. Dover Publications, 2017. [https://math.jhu.edu/](https://math.jhu.edu/~eriehl/context.pdf)  
457 [~eriehl/context.pdf](https://math.jhu.edu/~eriehl/context.pdf).
- 458 16 The Coq Development Team. The coq proof assistant, June 2023. doi:10.5281/zenodo.  
459 8161141.
- 460 17 Amin Timany and Bart Jacobs. Category theory in coq 8.5. In *FSCD*, volume 52 of *LIPICs*,  
461 pages 30:1–30:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.
- 462 18 Douglas B. West. *Introduction to graph theory*. New Delhi: Prentice-Hall of India, 2nd ed.  
463 edition, 2005.