A graph calculus for proving intuitionistic relation algebraic equations[*][†]

Renata de Freitas
Institute of Mathematics and Statistics,
UFF: Universidade Federal Fluminense,
Niterói, Brazil
freitas@vm.uff.br

Petrucio Viana
Institute of Mathematics and Statistics,
UFF: Universidade Federal Fluminense,
Niterói, Brazil
petrucio@cos.ufrj.br

We introduce a diagrammatic system in which diagrams based on graphs represent binary relations and reasoning on binary relations is performed by transformations on diagrams. We prove that if a diagram D_1 is transformed into a diagram D_2 using the rules of our system, under a set Γ of hypotheses, then "it is intuitionistically true that the relation defined by diagram D_1 is a subrelation of the one defined by diagram D_2, under the hypotheses in Γ". We present the system formally, prove its soundness, and left the question of its completeness for further investigation.

1 Introduction

Boolean reasoning, i.e. reasoning involving plain sets and the Boolean operations of union, intersection and complement, may be performed through the algebraic language of Boolean algebras [2]. Likewise, *relational reasoning*, i.e. reasoning involving relations, the Boolean operations, and the Peircean operations of composition, dual-composition and conversion, may be performed through the more elaborated algebraic language of De Morgan-Peirce-Schröder-Tarski relation algebras [15]. A main difference between these environments arises from the fact that, although there is a number of algorithms to decide validity or perform inferences in the calculus with sets [2], the analogous tasks for the relational language are highly undecidable [16]. Hence, the problem of *building mechanisms which may help in the design of relational algebraic proofs from scratch* arises.

The use of mechanized systems to help in the performance of relational inferences is not a new subject of research (cf. [14, 7]). Most of the proposed systems use equational logic [12], that is the high-school rule of replacing equals by equals, as the underlying logic, and thus do not correspond to the predominantly non-equational way relational reasoning in naturally performed [11]. Moreover, as can be seen by an examination of some papers where relation algebraic reasoning is developed and applied [4, 13], in practice relation algebraic inferences are performed in an environment consisting of a mixture of equational logic enriched with a sort of lattice theoretical inference engine, i.e. the passage from an object to a lesser or from an object to a bigger, at one side of an inclusion. Another drawback of these systems, in our view, is that most of them, with the exception of the systems outlined in [3, 6], make use of the linear format of discourse, in the form of equalities and inclusions between algebraic terms, to represent the information being processed.

The authors of this paper, together with some colleagues, have proposed a different mechanism based on diagrams to perform relational reasoning [8, 9, 10]. The environment in which we work can be summarized as follows.

[*]An abstract of this work was presented at the poster session of Diagrams 2012.
[†]Research partially sponsored by CNPq and FAPERJ.

Submitted to:
IMLA-Rio 2013

As stated earlier, most systems in the bibliography perform inferences with equalities and inclusions between relation algebraic terms. In our work, alternatively, we move to the lattice theoretical side and prefer to handle inclusions rather than equalities, but instead of relation algebraic terms, we use diagrams in the left and right hand sides of an inclusion. We have a set of rules to transform diagrams, in order to test whether an inclusion is a consequence of given a set of inclusions taken as hypotheses. Starting with the diagram in the left hand side of the target inclusion, by successive applications of our rules, mediated by the inclusions taken as hypotheses, either we end up with the diagram in the right hand side of the target inclusion, when the inclusion is a consequence of the hypotheses or, otherwise, build a possibly very large non constructive counter model (cf. [10] for details).

The main characteristic of the system presented in [10], besides its accordance with reasoning from hypotheses, is an explicit diagrammatic representation of complement. The diagrams representing binary relations may have occurrences of boxed subdiagrams to fit complement, and one of the main transformation rules allows one to change any given diagram into another one, by reproducing it in two parts, one having an occurrence of a subdiagram and the other having an occurrence of the same sub-diagram inside a box. This two part diagram represents two complementary alternatives: some relation or its complement holds between some pair of points in the domain. After the use of these diagrams and rules in some concrete situations, one can promptly inquire on the exact strength of the process outlined above. In particular, given the resemblance between this process and the axiom of the excluded middle of classical first-order logic, one may ask whether is it possible to modify our system in order to obtain a diagrammatic system which can cope with the intuitionistic inferences which can be performed in the relational algebraic language. This is the work we start here.

In Section 2, to motivate our work, we present a rough sketch of a problem faced by those who try to build relational equational proofs from scratch: that of finding and justifying the non trivial algebraic laws used in the proof. In Section 3, we summarize, by means of an example, our approach to solve instances of this challenging problem: the use of diagrams. In Section 4, we emphasize that one can distinguish intuitionistic from non intuitionistic diagrammatic proofs. Besides, we formalize the previous observation by making a slight change in the set of axioms and rules presented in [10], to produce intuitionistic diagrammatic proofs. In Section 5, we prove the main result of this paper which amounts to the soundness of our diagrammatic rules w.r.t intuitionistic inferences in the relational algebraic language.

2 Algebraic relational proofs

The *relation terms*, typically denoted by R, S, T, are generated by the following grammar:

$$R ::= r \mid \mathsf{U} \mid \mathsf{O} \mid \mathsf{I} \mid R^{\mathsf{C}} \mid R^{-1} \mid R \sqcap R \mid R \sqcup R \mid R \circ R,$$

where r belongs to a set of *relation variables*. A *relation inclusion*, respectively *relation equality*, is an expression of the form $R \sqsubseteq S$, respectively $R = S$.

Given a set u, considered as the *universe*, each relation variable is intended to denote a binary relation on u. Constants U, O and I denote the universal relation, the empty relation, and the identity relation, respectively. The relation operators $^{\mathsf{C}}$, $^{-1}$, $\sqcup$, $\sqcap$, and $\circ$ denote complementation, conversion, intersection, union and composition, respectively. So, given a set u, the relation terms denote those relations which can be defined from the relations denoted by the variables, by applying the relation operators recursively.

Concerning expressive power, the main application of the relation inclusions and equalities is the rewriting of statements involving binary relations, without making any reference to individuals. For example, if r is a binary relation symbol, to express that a relation denoted by r is functional, one may use the first-order sentence $\forall xyz(xry \land xrz \to y = z)$ or, equivalently, $\forall yz(\exists x(xry \land xrz) \to y = z)$. But this can also be expressed throughout a relation inclusion having no occurrences of individual variables. A binary relation r is *functional* iff it satisfy the inclusion $r^{-1} \circ r \sqsubseteq \mathsf{I}$.

Regarding deductive power, the main application of the relation inclusions and equalities is the proof of certain general facts involving binary relations, applying only equational reasoning or, in most cases, equational reasoning together with a sort of lattice theoretical inference engine. For example, using first-order logic one can easily prove that if two given relations are functional and have disjoint domains, then their union is also a functional relation. Thanks to the fact that $x \in \mathsf{dom} r$ iff $\exists y \in u(xry)$ iff $\forall z \in u(\exists y \in u(xry \land y\mathsf{U}z))$, one can reformulate the statement above in relation algebraic terms as follows.

Proposition 1 *If* $r^{-1} \circ r \sqsubseteq \mathsf{I}$, $s^{-1} \circ s \sqsubseteq \mathsf{I}$, *and* $(r \circ \mathsf{U}) \sqcap (s \circ \mathsf{U}) = \mathsf{O}$, *then* $(r \sqcup s)^{-1} \circ (r \sqcup s) \sqsubseteq \mathsf{I}$.

A first step to make a relation algebraic proof, in the lattice theoretical style that we are mentioning here, is to find out some algebraic laws which can be used in the development of the proof. In the case of Proposition 1, the use of some obvious laws such as $(r \sqcup s)^{-1} = r^{-1} \sqcup s^{-1}$ is easy to predict, while the correct way to choose and apply the more elaborated ones seems to be a matter of ingenuity allied to experience. As an example, a useful law for this case states that the following equivalences hold for any relations r, s, t:

$$r \circ s \sqsubseteq t \iff r^{-1} \circ t^{\mathsf{C}} \sqsubseteq s^{\mathsf{C}} \iff t^{\mathsf{C}} \circ s^{-1} \sqsubseteq r^{\mathsf{C}}. \tag{1}$$

From (1), the proof of Proposition 1 breaks down in three main steps. First, we prove $r^{-1} \circ s = \mathsf{O}$, from the hypothesis $(r \circ \mathsf{U}) \sqcap (s \circ \mathsf{U}) = \mathsf{O}$, as follows:

$$\begin{aligned} (r \circ \mathsf{U}) \sqcap (s \circ \mathsf{U}) = \mathsf{O} &\iff r \circ \mathsf{U} \sqsubseteq (s \circ \mathsf{U})^{\mathsf{C}} \\ &\iff r^{-1} \circ (s \circ \mathsf{U})^{\mathsf{C}\mathsf{C}} \sqsubseteq \mathsf{U}^{\mathsf{C}} \\ &\iff r^{-1} \circ (s \circ \mathsf{U}) \sqsubseteq \mathsf{O} \\ &\iff (r^{-1} \circ s) \circ \mathsf{U} = \mathsf{O} \\ &\iff r^{-1} \circ s = \mathsf{O}. \end{aligned}$$

Second, from this, we obtain $s^{-1} \circ r = \mathsf{O}$. Finally, we complete the proof:

$$\begin{aligned} (r \sqcup s)^{-1} \circ (r \sqcup s) &= (r^{-1} \sqcup s^{-1}) \circ (r \sqcup s) \\ &= (r^{-1} \circ r) \sqcup (r^{-1} \circ s) \sqcup (s^{-1} \circ r) \sqcup (s^{-1} \circ s) \\ &\sqsubseteq \mathsf{I} \sqcup \mathsf{O} \sqcup \mathsf{O} \sqcup \mathsf{I} \\ &= \mathsf{I}. \end{aligned}$$

Of course, the outlined proof can only be considered as *a proof* if all details left to the reader are filled and all general laws applied are either justified from a set of axioms or taken as axioms themselves. This is an easy task for certain laws and equivalences such as $r \circ (s \circ t) = (r \circ s) \circ t$ or $r \sqcap s = \mathsf{O} \iff r \sqsubseteq s^{\mathsf{C}}$, but someone may be uncomfortable with the use of (1) and may ask for a proper justification.

3 Diagrammatic relational proofs

We want to emphasize, by presenting the previous example, that the (far from being deterministic) main step in producing a relation algebraic proof of an inclusion or equality from a set of inclusions or equalities taken as hypotheses, consists in the choice of a nice set of relation algebraic laws to assist you in building the proof. The finding of these laws may be guided by experience, previous knowledge, luck,

Table 1: Informal explanation of some transformation rules.

Cv	Any sub-diagram D_1 of a diagram D can be replaced by another diagram D_2 that contains the information given by D_1, and possibly less information.
Hyp	Given a diagram D and an inclusion $R \sqsubseteq S$, any sub-diagram of D containing the information given by D_R can be replaced by another sub-diagram that contains the information given by D_S.
Hyp*	Any diagram D can be broken into another one, let us say $D_1 \vert D_2$, containing two alternatives: D_1 contains the information given by D in conjunction with a piece of information i, and D_2 contains the information given by D in conjunction with the information that is complementary to i.
Hyp$^{\emptyset}$	Any subdiagram containing contradictory information can be erased.

etc, but, whatever the medium used to find them, the laws used in the proof must ultimately be justified. The authors of this paper, together with some colleagues, have been trying a strategy based on diagrams. To exemplify our approach, let us explain how some sort of graphs can be used to produce a very convincing proof of Proposition 1, and even of the capital law (1).

The main idea of our approach in proving a relation inclusion $R \sqsubseteq S$ from a set of hypotheses is to associate diagrams D_R and D_S to the left and the right hand sides of the inclusion and, by the application of the hypotheses according certain rules, to transform diagram D_R into diagram D_S. In this case, certainly due to the conceptual proximity between *binary relations* and *graphs*, the diagrams that appear as the most appropriate to deal with are *sets of 2-pointed labeled directed graphs* [1, 5], which we simply call *diagrams*. Besides, a complete set of rules is given by considering the transformation rules in [10]. We describe the most important ones in very general terms in Table 1.

This set of rules plus other very intuitive ones used to iteratively transform relation terms in diagrams (cf. [10]), allow us to drawn Figure 1, containing a diagrammatic proof of Proposition 1. The proof consists of a sequence $(D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8)$ of eight diagrams. D_1 is an arc labeled with the term $(r \sqcup s)^{-1} \circ (r \sqcup s)$. This is just the diagram associated to the term, representing the left hand side of the inclusion we want to prove. D_2 is obtained from the D_1 by replacing the arc labeled with the term $(r \sqcup s)^{-1} \circ (r \sqcup s)$, having one main occurrence of composition, by two consecutive arcs, one labeled $(r \sqcup s)^{-1}$ and the other labeled $r \sqcup s$. D_3 is obtained from D_2 by replacing the arc labeled with the term $(r \sqcup s)^{-1}$, having one main occurrence of conversion, by one arc labeled $r \sqcup s$ which has the opposite direction to the arc it replaced. Now, the left arc in D_3, labeled $r \sqcup s$, represents two alternatives, one is r and the other is s. So, D_4 is obtained from D_3 by replacing it with a diagram consisting of two similar subdiagrams, one with the left arc labeled r, representing the first alternative, and the other with the left arc labeled s, representing the second alternative. In a entirely similar way, we obtain D_5 from D_4, by considering the alternatives given by the labels $r \sqcup s$ with occur in the right arc of both subdiagrams. Now, we have D_5, a diagram consisting of four alternatives, each one represented by a subdiagram. Observe that according to the hypothesis $r^{-1} \circ r \sqsubseteq \mathsf{I}$, the first alternative presented in D_5 is included in I. Then we have diagram D_6. Analogously, using the hypothesis $s^{-1} \circ s \sqsubseteq \mathsf{I}$, we obtain D_7. Moreover, according to the hyphotesis $(r \circ \mathsf{U}) \sqcap (s \circ \mathsf{U}) = \mathsf{O}$ the second and third alternatives in D_7 are inconsistent. So, they should be simply erased. Finally, we end up with D_8, consisting of an arc labeled I. That is the diagram

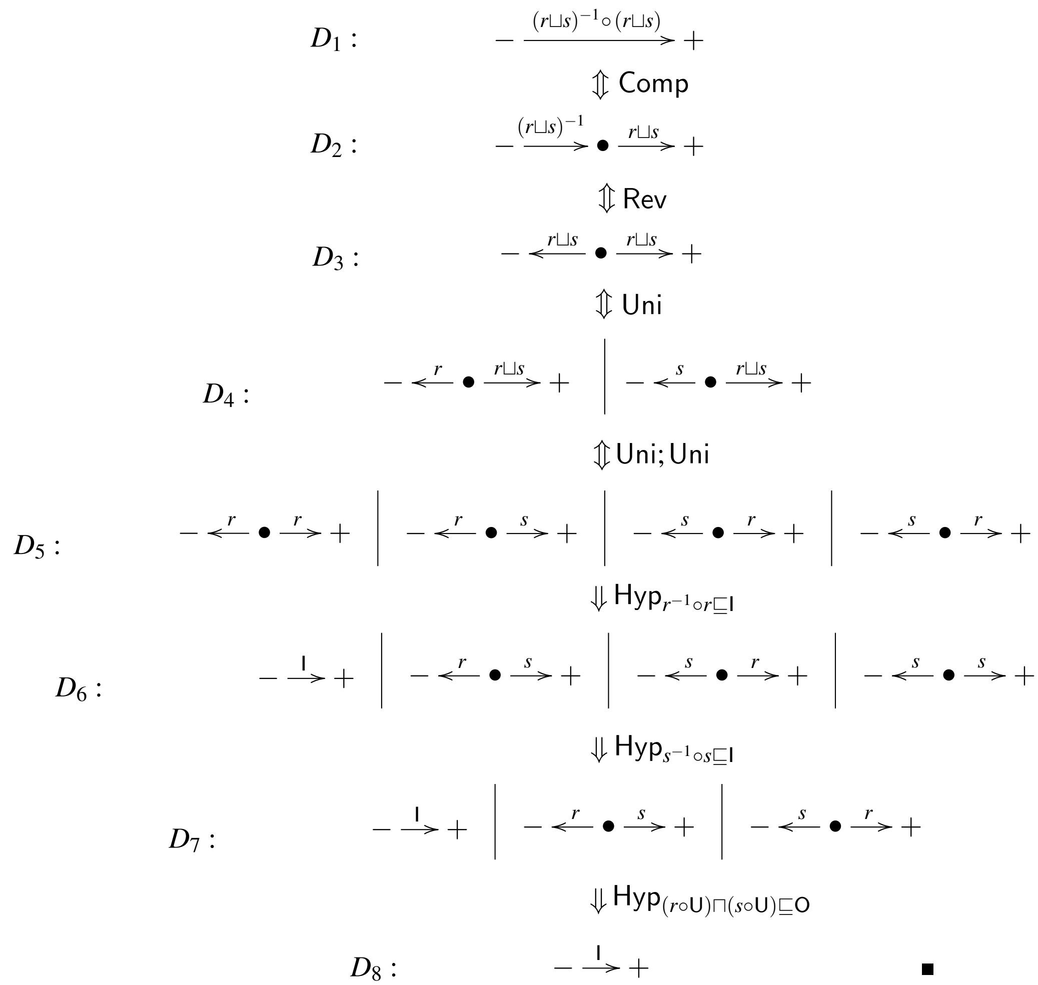

Figure 1: Diagrammatic proof of Proposition 1.

of the right hand side of the inclusion we want to prove.

Now, as we mentioned, the capital law used in the relation algebraic proof of Proposition 1, given above, was (1). Someone uncomfortable with it may wish to use our transformation rules to produce a convincing proof of it. We shall present, in Figure 3, a diagrammatic proof justifying the implication $r \circ s \sqsubseteq t \Longrightarrow r^{-1} \circ t^{\mathsf{C}} \sqsubseteq s^{\mathsf{C}}$. It consists of a sequence $(D_1, D_2, D_3, D_4, D_5, D_6, D_7, D_8)$ of eight diagrams. D_1 is the diagram representing the term $r^{-1} \circ t^{\mathsf{C}}$, i.e. D_1 represents the left-hand side of the inclusion we want to prove. D_2 is obtained from D_1 by replacing the main occurrence of composition by two consecutive arcs, labeled r^{-1} and t^{C}, respectively. D_3 is obtained from D_2 by replacing the arc r^{-1} by an arc labeled r in the opposite direction, and the arc t^{C}, labeled with a term having one main occurrence of complementation, by one arc labeled $\boxed{- \xrightarrow{t} +}$. We agree that a box around a diagram represent the negation of the information represented by that diagram. Now, D_4 is obtained from D_3 by replacing it by a diagram consisting of two subdiagrams representing two alternatives. We agree that, in general, a diagram represents alternatives a pair of points may satisfy in order to belong to the relation represented

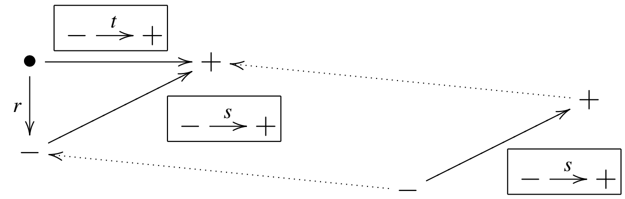

Figure 2: Mapping diagram representing s^{C} into D_6.

by the diagram. Also, as usual, any pair of points is related by a given relation or by its complement. Thus, by displaying two complementary alternatives to the same pair of nodes, diagram D_4 impose the same restrictions to any pair of nodes that is imposed by diagram D_3, i.e. both D_3 and D_4 represent the same relation. D_5 is obtained from D_4, according to the following idea that allow us to use the hypothesis $r \circ s \sqsubseteq t$ to transform diagram D_4. Since the left subdiagram of D_4 has a path from node $\bullet$ to node $+$ through node $-$ that represents the relation $r \circ s$ and since, by hypothesis, $r \circ s \sqsubseteq t$, we are allowed to transform D_4 by adding an arc labeled t from $\bullet$ to $+$. Now, observe that the left subdiagram of D_5 has two parallel arcs linking node $\bullet$ to $+$, one labeled t and the other labeled $\boxed{- \xrightarrow{t} +}$. We agree that parallel paths linking the same points mean that the points are simultaneously in the relations represented by each path. So, nodes $\bullet$ and $+$ are simultaneously in relations t and t^{C}, so that the left subdiagram of D_5 represents inconsistent information. Thus, we can erase it from D_5, obtaining D_6.

Now, note that inside D_6 we can locate a copy of the diagram representing s^{C}, as shown in Figure 2.

This means that D_7 imposes no more restrictions than D_6 in defining a relation and so, D_6 may be considered to represent a subrelation of D_7. Thus, we finally move from diagram D_7 to diagram D_8, that represents the right-hand side of the implication we want to prove.

We think that diagrammatic reasoning should talk by itself. So, we hope the explanations above are sufficient to give the reader a good idea of how our system works.

The attentive reader may have noticed the unexplained use we made of the symbol $*$ in the proof presented in Figure 3. There, this tag was introduced when we applied the rule that allows us to transform a diagram by breaking it in two parts, each one containing alternative complementary information. This passage occurred when we transformed diagram D_2 into diagram D_3. The tag was used to label the subdiagram which does not have the occurrence of the negated information, expressed in the form of a boxed diagram, and continued until the end of the proof, or, as in the case of this proof, until some derived information containing the tag was erased by the application of the appropriated rule. Hence, the diagrammatic proofs presented in Section 3 are of two kinds: those whose last diagram has occurrences of the tag $*$ and those whose last diagram does not have occurrences of $*$.

By experimenting with this idea, we observed that the proofs ending with diagrams without occurrences of the tag $*$ correspond to intuitionistic inferences and those ending in diagrams having occurrences of $*$ correspond to non intuitionistic ones. Hence, we decided to explore this characteristic of our calculus, adapting it to prove all the intuitionistic inferences expressible in its language. To this, we introduced the tag formally and we made all the necessary amendments to obtain an adequate intuitionistic diagrammatic system. In the next sections, we present these ideas formally and proof soundness of a calculus with graphs for the intuitionistic logic of binary relations.

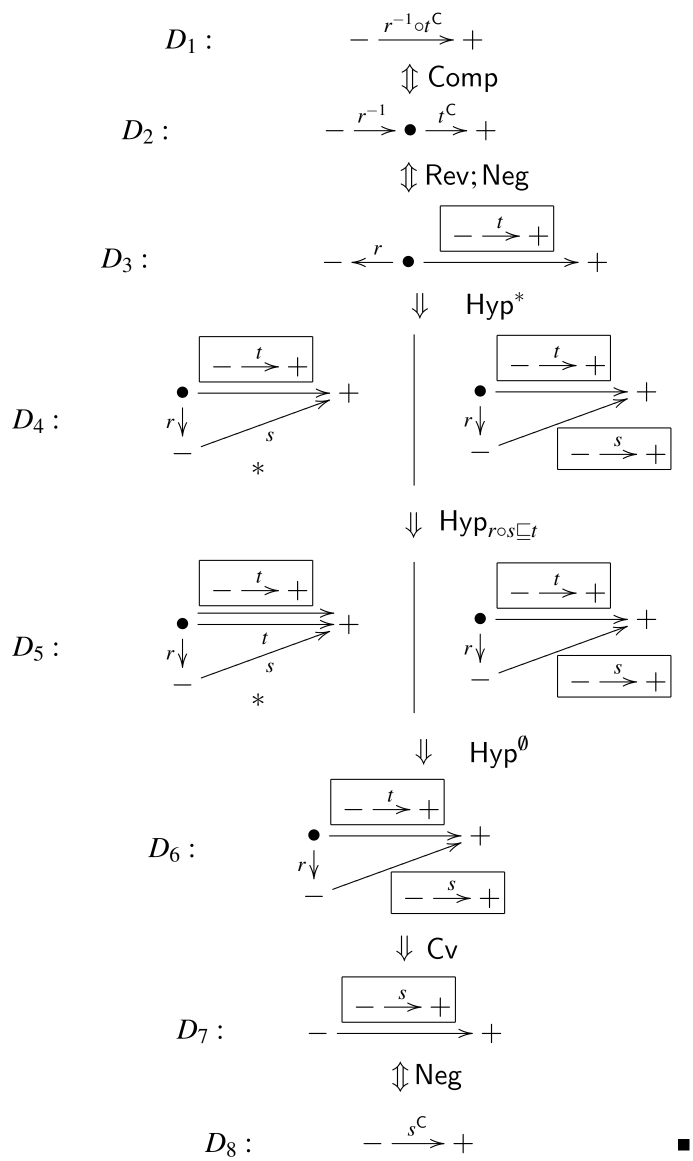

Figure 3: Diagrammatic proof of $r \circ s \sqsubseteq t \ \vdash_i \ r^{-1} \circ t^{\mathsf{C}} \sqsubseteq s^{\mathsf{C}}$.

4 Intuitionisitc graph calculus

Nodes and labeled arcs are the building blocks of graphs. Hence, we first consider the sets INOD of individual *nodes* and RVAR of *relation variables*, which we will keep fixed throughout.

A *graph*, typically denoted by G or H, is a structure (N,A,i,o,t), where N is a finite nonempty set of nodes, $A \subseteq N \times \mathfrak{L} \times N$ is a finite set of labeled *arcs* ($\mathfrak{L}$ is the set of all labels), i (*input*) and o (*output*) are, not necessarily distinct, distinguished nodes in N, and t is a finite sequence of natural numbers (*tag*). An *arc* of A is a triple, denoted by uLv, with $u,v \in N$ and L being a label. A *label* is a relational symbol or a *box* $\boxed{D}$, where D is a concrete diagram. A *concrete diagram* is a set of graphs.

Graphs $G_1 = (N_1,A_1,i_1,o_1,t_1)$ and $G_2 = (N_2,A_2,i_2,o_2,t_2)$ are *isomorphic* if there are bijections $f : N_1 \to N_2$ and $g : A_1 \to A_2$ such that (1) for all $urv \in A_1$, $g(urv) = furfv$; (2) for all $u\boxed{D}v \in A_1$, $g(u\boxed{D}v) = fu\boxed{D'}fv$ and D and D' are isomorphic; and (3) $fi_1 = i_2$ and $fo_1 = o_2$.

Concrete diagrams D and D' are *isomorphic* if there is a bijection $h : D \to D'$ such that $h(G)$ is isomorphic to G, for all $G \in D$. The usual identification of isomorphic concrete diagrams is reflected in our figures by the representation of every non-distinguished node by $\bullet$, of every input node by $-$, and of every output node by $+$. In figures, tag $\langle 1\rangle$ is represented by $*$. A *diagram* is an equivalence class of isomorphic concrete diagrams. In what follows, a diagram is identified with each of the concrete diagrams that represents the equivalence class. A *diagram inclusion* is an expression of the form $D \sqsubseteq D'$.

Now we present a set of axioms and a set of rules to transform a diagram into another. We first introduce two families of axioms of our graph calculus. Given a graph $G = (N_G,A_G,i_G,o_G,t_G)$, we define two diagrams as follows. The graph $O_G := \{(N_G,A_G \cup \{i_G \boxed{\{G\}}\, o_G\}, i_G, o_G, t_G)\}$ is obtained from G by adding to it a new arc from the input of G to the output of G labeled by $\boxed{\{G\}}$. The graph $E_G := \{(N_G,A_G,i_G,o_G,\langle 1\rangle),(\{i,o\},\{i\boxed{\{G\}}\,o\},i,o,\langle\,\rangle)\}$ is obtained from G by adjoining to G a new slice with two distinct nodes, input i and output o, and a single arc $i\boxed{\{G\}}\,o$. We shall take as schemes of axioms of the graph calculus the inclusions $O_G \sqsubseteq O$ and $E \sqsubseteq E_G$ for any graph G (Table 2).

The rules of our graph calculus are the Introduction/Elimination rules (one for each operator), Graph Cover rule, Hypotheses rule and Box rule. Introduction/Elimination rules covers the labels of the graphs. Graph Cover rule is used to compare diagrams with respect to inclusion, Hypotheses rule, to transform diagrams according to the set of inclusions taken as hypotheses, and Box rule, to simplify the inner structure of box labels.

Introduction/Elimination rules are presented in Table 2. Each one of these rules can be applied in both directions: downward and upward, allowing the *elimination* (downwards) and the *introduction* (upwards) of the operators. We will explain each two-way rule in the downward direction. Each one of these rules involves the application of the local transformation specified in the rule, leaving the rest of diagram untouched. Except for Imp, Introduction/Elimination rules are similar to those of the graph calculus presented in [8] and their presentation are taken from this paper. Rule Univ allows erasing an arc labeled by U from a graph. Rule Vd allows erasing a graph having an arc $u\mathsf{O}v$. Rule Iden allows erasing an arc $u\mathsf{I}v$ and a node u, renaming nodes and redirecting arcs accordingly. We use the *node substitution* notation $\frac{u}{v}$ for replacing u by v, which we extend naturally to sets as well as to tuples, e.g., for a set A of arcs, we put $A\frac{u}{v} = \{w\frac{u}{v}Lz\frac{u}{v} : wLz \in A\}$. Given a relation term R, the *diagram associated to R* is

$$D_R ::= \{(\{i,o\},\{iRo\},i,o,\langle\,\rangle)\}.$$

Rule Neg allows replacing an arc $uR^{\mathsf{C}}v$ by an arc $u\boxed{D_R}v$. Rule Rev allows replacing an arc $uR^{-1}v$ by vRu. Rule Int allows replacing an arc $uR \sqcap Sv$ by arcs uRv and uSv. Rule Uni allows replacing a graph

G having an arc $uR \sqcup Sv$ by two other graphs G_R and G_S, obtained from G by replacing the arc $uR \sqcup Sv$ by new arcs uRv and uSv, respectively. Rule Imp allows replacing a graph G having an arc $uR \sqsupset Sv$ by two other graphs G_R^* and G_S, obtained from G by replacing the arc $uR \sqsupset Sv$ by new arcs $u\boxed{D_R}v$ and uSv, respectively, and by adding the lower natural number not occurring in any tag in the graph proof to the tag of G_R^*. Rule Comp allows replacing an arc $uR \circ Sv$ by arcs uRw and wSv, with a new node w.

To define our next transformation rule, the concepts of homomorphism from a graph to another and that of a diagram covering another will be crucial. Given graphs $G = (N_G, A_G, i_G, o_G, t_G)$ and $H = (N_H, A_H, i_H, o_H, t_H)$, by a *graph homomorphism from H to G* we mean a function $\phi : N_H \to N_G$, denoted by $\phi : H \to G$, that preserves input, output, and arcs, i.e. $\phi i_H = i_G$, $\phi o_H = o_G$, and if $uLv \in A_H$ then $\phi uL\phi v \in A_G$. Given diagrams D_1 and D_2, we say that D_2 *covers* D_1 or D_1 *is covered by* D_2, denoted by $D_1 \leftarrow D_2$, when for each graph $G \in D_1$ there exist a graph $H \in D_2$ and a graph homomorphism $\phi : H \to G$. Rule Cv (Table 2) allows replacing a diagram by another one that covers it.

We now introduce the concepts of gluing graphs and draft homomorphism between graphs, which will be central in applying a diagram inclusion to transform a diagram into another. Intuitively, we glue graph H onto graph G by adding to G a copy of H and identifying designated nodes u, v of G to the input and output of H. More precisely, given graphs $G = (N_G, A_G, i_G, o_G, t_G)$ and $H = (N_H, A_H, i_H, o_H, t_H)$, as well as designated nodes $u, v \in N_G$, the result of *gluing H onto G via u, v* is the graph defined by $\mathsf{glue}_{(u,v)k}(H,G) := (N_G \uplus N_H, A_G \uplus A_H, i_G, o_G, t_G k t_H)\frac{i_H}{u}\frac{o_H}{v}$, where k is a given function associating tags to tags. We *glue* a diagram D onto a graph G, via nodes u, v of G, by gluing its graphs to G, i.e. $\mathsf{glue}_{(u,v)k}(D,G) := \{\mathsf{glue}_{(u,v)k}(H,G) : H \in D\}$. Given graphs $G = (N, A, i, o, t)$ and $G' = (N', A', i', o', t')$, by a *draft homomorphism from G' to G* we mean a function $\theta : N' \to N$, denoted by $\theta : G' \dashrightarrow G$, that preserves arcs. Now, given graphs G and G' as before, a draft homomorphism $\theta : G' \dashrightarrow G$, and diagram D, we set $\mathsf{glue}_{\theta k}(D,G) := \mathsf{glue}_{(\theta i', \theta o')k}(D,G)$. Rule Hyp_Γ (Table 2) allows gluing a diagram D onto a graph G of a diagram under a draft homomorphism $\theta : G' \dashrightarrow G$ when $D' \cup \{G'\} \sqsubseteq D$ is a hypothesis in Γ or is an axiom.

The Box rule (Table 2) is a two-way rule, i.e. it can be applied in the top-down and in the bottom-up directions. In the top-down direction, the Box rule allows replacing an arc labeled by a box $\boxed{D}$ having a diagram $D = \{G_j : j \in J\}$ inside of it, by a set of parallel arcs, each one labeled by a box $\boxed{\{G_j\}}$, and vice-versa, for the bottom-up direction. In the case $I = \emptyset$, the Box rule allows erasing (top-down) or to add (bottom-up) an arc labeled by a box with the empty diagram O inside of it.

The notion of derivation is standard. Given a set of diagram inclusions Γ, by a *derivation from* Γ, or simply a Γ*-derivation*, we mean a sequence $(D_0, \ldots, D_n)$ of diagrams such that each diagram D_k, for $k \in \{1, \ldots, n\}$, is obtained from diagram D_{k-1} by an application of one of the inference rules (Introduction/Elimination, Cv, Hyp_Γ, or Box). A diagram D' is *derivable from a diagram D using* Γ, or simply D' *is* Γ*-derivable from D*, denoted by $\Gamma \vdash D \sqsubseteq D'$, when there is a Γ-derivation $(D_0, \ldots, D_n)$ such that $D_0 = D$ and $D_n = D'$. An inclusion $D \sqsubseteq D'$ is a *theorem*, denoted by $\vdash D \sqsubseteq D'$, when D' is derivable from D using the empty set of hypotheses. A diagram D' is *intuitionistic derivable from a diagram D using* Γ, or simply D' *is* Γ*-i-derivable from D*, denoted by $\Gamma \vdash_i D \sqsubseteq D'$, when there is a Γ-derivation $(D_0, \ldots, D_n)$ such that $D_0 = D$, $D_n = D'$, and all natural numbers occurring in the tags of graphs of D' also occur in tags of graphs of D or of some diagram of the inclusions in Γ. An inclusion $D \sqsubseteq D'$ is an *intuitionistic theorem*, denoted by $\vdash_i D \sqsubseteq D'$, when D' is i-derivable from D using the empty set of hypotheses.

Table 2: Axioms and rules for transforming diagrams.

Axioms

$$O_G \sqsubseteq O \quad \text{and} \quad E \sqsubseteq E_G$$

Elimination/Introduction rules

$$\mathsf{Univ}\ \frac{(N,A\cup\{u\mathsf{U}v\},i,o,t)}{(N,A,i,o,t)} \qquad \mathsf{Vd}\ \frac{D\cup\{(N,A\cup\{u\mathsf{O}v\},i,o,t)\}}{D}$$

$$\mathsf{Iden}\ \frac{G\cup\{(N,A\cup\{u\mathsf{I}v\},i,o,t)\}}{G\cup\{(N,A,i,o,t)\frac{u}{v}\}} \qquad \mathsf{Neg}\ \frac{(N,A\cup\{uR^{\mathsf{C}}v\},i,o,t)}{(N,A\cup\{u\,\boxed{D_R}\,u\},i,o,t)}$$

$$\mathsf{Rev}\ \frac{(N,A\cup\{uR^{-1}v\},i,o,t)}{(N,A\cup\{vRu\},i,o,t)} \qquad \mathsf{Int}\ \frac{(N,A\cup\{uR\sqcap Sv\},i,o,t)}{(N,A\cup\{uRv,uSv\},i,o,t)}$$

$$\mathsf{Uni}\ \frac{D\cup\{(N,A\cup\{uR\sqcup Sv\},i,o,t)\})}{D\cup\{(N,A\cup\{uRv\},i,o,t),(N,A\cup\{uSv\},i,o,t)\}}$$

$$\mathsf{Imp}\ \frac{D\cup\{(N,A\cup\{uR\sqsupset Sv\},i,o,t)\}}{D\cup\{(N,A\cup\{u\,\boxed{D_R}\,v\},i,o,tn),(N,A\cup\{uSv\},i,o,t)\}}$$

if n is the lower natural number not occurring in any tag in the graph proof

$$\mathsf{Comp}\ \frac{(N,A\cup\{uR\circ Sv\},i,o,t)}{(N\cup\{w\},A\cup\{uRw,wSv\},i,o,t)} \quad \text{if } w\notin N$$

Graph Cover rule

$$\mathsf{Cv}\ \frac{D_1}{D_2} \quad \text{if } D_1 \leftarrow D_2$$

Hypotheses rule

$$\mathsf{Hyp}_\Gamma\ \frac{D_1\cup\{G\}}{D_1\cup \mathsf{glue}_{\theta k}(D_2,G)}$$

if $\theta : G' \dashrightarrow G$ and $D'\cup\{G'\}\sqsubseteq D_2$ is in Γ or is an axiom, and $kt = \begin{cases} tn \text{ if } t\neq\langle\,\rangle \\ t \text{ otherwise}\end{cases}$

where n is the lower natural number not occurring in any tag in the graph proof

Box rule

$$\mathsf{Box}\ \frac{D\cup\{(N,A\cup\{u\,\boxed{\{G_j : j\in J\}}\,v\},i,o,t)\}}{D\cup\{(N,A\cup\{u\,\boxed{\{G_j\}}\,v : j\in J\},i,o,t)\}}$$

5 Soundness of the calculus

Let R be a relational term and u,v be individual variables. The *uv-translation* of R into a first-order formula is defined recursively as follows: $\mathsf{ST}uv(r) = r(u,v)$, if r is a relational variable; $\mathsf{ST}uv(\mathsf{U}) = \top$; $\mathsf{ST}uv(\mathsf{O}) = \bot$; $\mathsf{ST}uv(R^{\mathsf{C}}) = \neg\mathsf{ST}uv(R)$; $\mathsf{ST}uv(R^{-1}) = \mathsf{ST}vu(R)$; $\mathsf{ST}uv(R \sqcap S) = \mathsf{ST}uv(R) \wedge \mathsf{ST}uv(S)$; $\mathsf{ST}uv(R \sqcup S) = \mathsf{ST}uv(R) \vee \mathsf{ST}uv(S)$; and $\mathsf{ST}uv(R \circ S) = \exists w(\mathsf{ST}uw(R) \wedge \mathsf{ST}wv(S))$, with w being a *new* variable. The *standard translation* of R is $\mathsf{ST}(R) = \mathsf{ST}xy(R)$.

Let us consider the set INOD of all nodes as a set of individual variables. Assume that $x,y \notin$ INOD. The *standard translation* of an arc a into a first-order formula is $\mathsf{ST}(a) = \mathsf{ST}uv(R)$, if $a = uRv$, and $\mathsf{ST}(a) = \neg\mathsf{ST}(D)\frac{u\ v}{x\ y}$, if $a = u\boxed{D}v$. The *standard translation* of a graph $G = (N,A,i,o,t)$ into a first-order formula is $\mathsf{ST}(G) = \exists N \setminus \{i,o\}\,(\bigwedge_{a\in A}\mathsf{ST}(a))\,\frac{x\ y}{i\ o}$. Remember that $x,y \notin N$, for every graph $G = (N,A,i,o,t)$. The *standard translation* of a diagram $D = \{G_1,\ldots,G_n\}$ into a first-order formula is $\mathsf{ST}(D) = \mathsf{ST}(G_1) \vee \cdots \vee \mathsf{ST}(G_n)$. It is immediate from these definitions that $\mathsf{ST}(D_R) = \mathsf{ST}(R)$.

Theorem 1 *Let $\Gamma \cup \{D \sqsubseteq D'\}$ be a finite set of diagram inclusions. If $\Gamma \vdash_i D \sqsubseteq D'$ and every natural number in the tag of every graph in D' also occurs in a tag of a graph in D or in Γ, then $\mathsf{ST}(D')$ is an intuitionistic consequence of $\mathsf{ST}(D)$ and $\mathsf{ST}(\Gamma)$.*

PROOF. Let $(D_0,\ldots,D_n)$ be a Γ-i-derivation of D' from D. We prove by induction on n that $\mathsf{ST}(D_n)$ is an intuitionistic consequence of $\mathsf{ST}(D)$ and $\mathsf{ST}(\Gamma)$. If D' is Γ-i-derivable from D by only one application of some rule, then this rule is neither $\mathsf{Hyp}_{E\sqsubseteq E_H}$ nor Imp, since both of them add a new natural number in a tag of a graph. Moreover, we have the following fact, that can be established by a tedious examination of cases.

FACT 1. If D_i derived from D_{i-1} by an application of any inference rule, except $\mathsf{Hyp}_{E\sqsubseteq E_H}$ and Imp, using Γ, then $\mathsf{ST}(D_i)$ is an intuitionistic consequence of $\mathsf{ST}(D_{i-1})$ and $\mathsf{ST}(\Gamma)$, where $\mathsf{ST}(\Gamma) = \{\mathsf{ST}(\gamma) : \gamma \in \Gamma\}$.

Hence, if $n = 1$, then $\mathsf{ST}(D')$ is an intuitionistic consequence of $\mathsf{ST}(D)$ and $\mathsf{ST}(\Gamma)$. Now, let $(D_0,\ldots,D_{k+1})$ be a Γ-i-derivation of D' from D. As $(D_1,\ldots,D_{k+1})$ is a Γ-i-derivation of D' from D_1 of length k, by the IH, $\mathsf{ST}(D_{k+1})$ is an intuitionistic consequence of $\mathsf{ST}(D_1)$ and $\mathsf{ST}(\Gamma)$. We consider two cases.

CASE 1. D_1 is derived from D_0 by an application of any inference rule, except $\mathsf{Hyp}_{E\sqsubseteq E_G}$ and Imp, using Γ. In this case, by Fact 1, $\mathsf{ST}(D_1)$ is an intuitionistic consequence of $\mathsf{ST}(D_0)$ and $\mathsf{ST}(\Gamma)$. Hence, $\mathsf{ST}(D_{k+1})$ is an intuitionistic consequence of $\mathsf{ST}(D_0)$ and $\mathsf{ST}(\Gamma)$, i.e., $\mathsf{ST}(D')$ is an intuitionistic consequence of $\mathsf{ST}(D)$ and $\mathsf{ST}(\Gamma)$.

CASE 2. D_1 is derived from D_0 by either an application of $\mathsf{Hyp}_{E\sqsubseteq E_H}$ or of Imp. In this case, $D_0 = D^{\langle\rangle} \cup \{G\}$ and $D_1 = D^{\langle\rangle} \cup \{G^{\langle\rangle}, G^m\}$, where $\{G^{\langle\rangle}, G^m\} = \mathsf{glue}_{\theta k}(E_H, G)$, G^m is a graph with a new natural number m in its tag and $G^{\langle\rangle}$ is a graph with the same tag as G, if the applied rule is $\mathsf{Hyp}_{E\sqsubseteq E_H}$; and $G = (N, A \cup \{uR \sqsupset Sv\}, i, o, t)$, $G^{\langle\rangle} = (N, A \cup \{uSv\}, i, o, t)$, $G^m = (N, A \cup \{u\boxed{D_R}v\}, i, o, tm)$, and m is a new natural number. If the applied rule is $\mathsf{Hyp}_{E\sqsubseteq E_H}$, or if it is Imp, we have the following results.

FACT 2. $\Gamma \vdash_i \{G^m\} \sqsubseteq \emptyset$. Since m does not occur in D' and the only way to delete a tag is to apply Vd.

Then, by the IH, $\mathsf{ST}(\emptyset) = \bot$ is an intuitionistic consequence of $\mathsf{ST}(G^m)$ and $\mathsf{ST}(\Gamma)$, since the Γ-i-derivation of $\emptyset$ from G^m is contained in $(D_1,\ldots,D_{k+1})$. We say that a Γ-derivation $(D_1,\ldots,D_n)$ is *contained* in a Γ-derivation δ if $D_1 \subseteq D'_1,\ldots,D_n \subseteq D'_n$ for some subsequence $(D'_1,\ldots,D'_n)$ of δ. Hence, since $\{G^{\langle\rangle}, G^m\} = \mathsf{glue}_{\theta}(E_H, G)$:

$$\mathsf{ST}(D^{\langle\rangle} \cup \{G^{\langle\rangle}\}) \text{ is an intuitionistic consequence of } \mathsf{ST}(D^{\langle\rangle} \cup \{G\}) \text{ and } \mathsf{ST}(\Gamma) \quad (2)$$

FACT 3. $\Gamma \vdash_i D^{\langle\rangle} \cup \{G^{\langle\rangle}\} \sqsubseteq D'$ — By the I.H., $\mathsf{ST}(D')$ is an intuitionistic consequence of $\mathsf{ST}(D_1)$

and $\mathsf{ST}(\Gamma)$. Recall that $D_1 = D^{\langle\rangle} \cup \{G^{\langle\rangle}, G^m\}$. Then, since m occurs in G^m but not in D', we have $\Gamma \vdash_i D^{\langle\rangle} \cup \{G^{\langle\rangle}, G^m\} \vdash_i D'$.

Hence, by the IH, since the Γ-i-derivation of D' from $D^{\langle\rangle} \cup \{G^{\langle\rangle}\}$ is contained in $(D_1, \dots, D_{k+1})$:

$$\mathsf{ST}(D') \text{ is an intuitionistic consequence of } \mathsf{ST}(D^{\langle\rangle} \cup \{G^{\langle\rangle}\}) \text{ and } \mathsf{ST}(\Gamma) \quad (3)$$

From (2) and (3), $\mathsf{ST}(D')$ is an intuitionistic consequence of $\mathsf{ST}(D_0)$ and $\mathsf{ST}(\Gamma)$, since $D_0 = D^{\langle\rangle} \cup \{G\}$. Hence, $\mathsf{ST}(D')$ is an intuitionistic consequence of $\mathsf{ST}(D)$ and $\mathsf{ST}(\Gamma)$. ■

Corollary 1 *Let $\Gamma = \{R_j \sqsubseteq S_j : j \in J\} \cup \{R \sqsubseteq S\}$ be a finite set of inclusions. If $\{D_{R_j} \sqsubseteq D_{S_j} : j \in J\} \vdash_i D_R \sqsubseteq D_S$, then $\forall xy(\mathsf{ST}(R) \rightarrow \mathsf{ST}(S))$ is an intuitionistic consequence of $\{\forall xy(\mathsf{ST}(R_j) \rightarrow \mathsf{ST}(S_j)) : j \in J\}$.*

PROOF. Immediate from Theorem 1, since for any relation term R, we have $\mathsf{ST}(D_R) = \mathsf{ST}(R)$. By the definition of D_R and the fact that, if $\mathsf{ST}(D')$ is an intuitionistic consequence of $\mathsf{ST}(D)$ and $\mathsf{ST}(\Gamma)$, then $\forall x \forall y(\mathsf{ST}(D) \rightarrow \mathsf{ST}(D'))$ is an intuitionistic consequence of $\mathsf{ST}(\Gamma)$, since the only free variables of $\mathsf{ST}(D)$ and $\mathsf{ST}(D')$ are x and y, and formulas in $\mathsf{ST}(\Gamma)$ have no free variables. ■

References

[1] H. Andréka & D.A. Bredikhin (1995): *The equational theory of union-free algebras of relations*. Algebra Universalis 33, pp. 516–532.

[2] F.M. Brown (2003): *Boolean Reasoning: The Logic of Boolean Equations*. Dover Books on Mathematics Series, Dover Publ.

[3] D. Cantone, A. Formisano, E.G. Omodeo & C.G. Zarba (2003): *Compiling dyadic specifications into map algebra*. Theoret. Comput. Sci. 293, pp. 447–475.

[4] L.H. Chin & A. Tarski (1951): *Distributive and Modular Laws in the Arithmetic of Relation Algebras*. University of California Publications in Mathematics, New series 1, Berkeley & Los Angeles.

[5] S. Curtis & G. Lowe (1996): *Proofs with graphs*. Sci. Comput. Programming 26, pp. 197–216.

[6] A. Formisano, E.G. Omodeo & M. Simeoni (2003): *A graphical approach to relational reasoning*. ENTCS 44, pp. 1–22.

[7] S. Foster, G. Struth & T. Weber (2011): *Automated engineering of relational and algebraic methods in Isabelle/HOL*. LNCS 6663.

[8] R. de Freitas, P.A.S. Veloso, S.R.M. Veloso & P. Viana (2008): *On a graph calculus for algebras of relations*. LNCS 5110, pp. 298–312.

[9] R. de Freitas, P.A.S. Veloso, S.R.M. Veloso & P. Viana (2009): *On graph reasoning*. Inform. and Comput. 207, pp. 1000–1014.

[10] R. de Freitas, P.A.S. Veloso, S.R.M. Veloso & P. Viana (2010): *A calculus for graphs with complement*. LNAI 6170, pp. 84–89.

[11] P. Höfner abd G. Struth (2008): *On automating the calculus of relations*. LNCS 5195, pp. 50–66.

[12] L. Henkin (1977): *The logic of equality*. Amer. Math. Monthly 84, pp. 597–612.

[13] Y. Kawahara (1988): *Applications of relational calculus to computer mathematics*. Bulletin of informatics and cybernetics 23, pp. 67–78.

[14] D. von Oheimb & T.F. Gritzner (1997): *RALL: Machine-supported proofs for relation algebra*. LNCS 1249, pp. 380–394.

[15] G. Schmidt & T. Ströhlein (1993): *Relation and Graphs: discrete mathematics for computer scientists*. Springer, Berlin.

[16] A. Tarski & S. Givant (1987): *A Formalization of Set Theory Without Variables*. American Mathematical Society.