Reasoning About Cardinalities of Relations with Applications Supported by Proof Assistants

Insa Stucke(✉)

Institut für Informatik, Christian-Albrechts-Universität zu Kiel, Kiel, Germany
ist@informatik.uni-kiel.de

Abstract. In this paper we prove the correctness of a program for computing vertex colorings in undirected graphs. In particular, we focus on the approximation ratio which is proved by using a cardinality operation for heterogeneous relations based on Y. Kawaharas characterisation.

All proofs are mechanised by using the two proof assistants Coq and Isabelle/HOL. Our Coq formalisation builds on existing libraries providing tools for heterogeneous relation algebras and cardinalities. To formalise the proofs in Isabelle/HOL we have to change over to untyped relations. Thus, we present an axiomatisation of a cardinality operation to reason about cardinalities algebraically also in homogeneous relation algebras and implement this new theoretical framework in Isabelle/HOL. Furthermore, we study the advantages and disadvantages of both systems in our context.

1 Introduction

Relation algebra (as first introduced in [19] and further studied, e.g., in [10,16]) provides an elegant way to reason about many discrete structures. For instance, there is a direct relationship between relations and graphs via adjacency relations. Hence, computational problems on graphs can be expressed and solved by using the relation-algebraic method as shown in [16], for example. The relation-algebraic approach is known for many methodical advantages in contrast to the conventional set-theoretic one. For example, it allows consice problem specifications and hence very formal calculations. Due to this, relation-algebraic reasoning turned out to be well-suited for mechanisation.

Thus, in [2] the authors develop a relational program for computing vertex colorings in undirected (and loop-free) graphs. The correctness proof is given by combining the assertion-based verification method with relation-algebraic calculations. In this context the usability of an automated theorem prover and the proof assistants Coq and Isabelle/HOL is shown and compared. However, the approximation ratio of the underlying Greedy algorithm is not studied at all since there were no obvious tools to tackle proofs involving cardinalities.

In the last years there has been a lot of work concerning the cardinalities of relations, mostly based on a definition of a cardinality operation for heterogeneous relation algebras presented by Kawahara in [9]. For example, in [3] and

P. Höfner et al. (Eds.): RAMiCS 2017, LNCS 10226, pp. 290–306, 2017.
DOI: 10.1007/978-3-319-57418-9_18

[1], the authors present first results about the cardinalities of special relations as points and vectors building the basis for reasoning about approximation ratios algebraically. Furthermore, in [5], a library for Coq providing an implementation of this cardinality operation in heterogeneous relation algebras is developed.

In the present paper the mentioned results about cardinalities of relations are used to prove the approximation ratio of the program presented in [2]. Furthermore, we study the application of the proof assistants Coq and Isabelle/HOL in this context. Therefore, we first use the library developed in [5] for mechanising the correctness proof in Coq. Our implementation in Isabelle/HOL builds on a library for untyped relations (see [17]). Thus, we modify Y. Kawahara's definition of a cardinality operation and present a new theoretical framework for dealing with cardinalities in homogeneous relation algebras. For this framework we develop a library that is eventually applicable for the mechanisation of the programs' correctness proof. As in [2], we compare the advantages and disadvantages of the usability of both tools in this context.

Our Coq proof script and Isabelle/HOL theories are available here [18].

2 Preliminaries

First, we recall the basic principles of relation algebra based on the heterogeneous approach of [6,15,16]. Set-theoretic relations form the standard model of relation algebras. We assume the basic operations on set-theoretic relations, viz. union, intersection, complementation, transposition and composition, in the remainder denoted by $R \cup S$, $R \cap S$, $\overline{R}$, R^T and RS for relations R, S of appropriate type. Furthermore, we consider the predicates $R \subseteq S$ (inclusion) and $R = S$ (equality)and the empty, universal and identity relation denoted by O, L and I.

Those operations and constants form a (heterogeneous) *relation algebra* in the sense of [15,16], with typed relations as elements. We write $R : X \leftrightarrow Y$ if R is a relation with source X and target Y and denote the type of R by $X \leftrightarrow Y$. In the case of typed relations we frequently overload the symbols O, L and I, if their type can be inferred from the context. If necessary we use indices as e.g., L_{XY} for L of type $X \leftrightarrow Y$. The axioms of a relation algebra are

(1) the axioms of a Boolean lattice for all same typed relations under the Boolean operations $\cup$, $\cap$ and $\overline{\ }$, $\subseteq$ and L and O,
(2) the associativity of composition and that identity relations are neutral w.r.t. composition,
(3) the *Schröder rule*, i.e., that for all relations Q, R and S with appropriate types it holds $QR \subseteq S \iff Q^\mathsf{T}\overline{S} \subseteq \overline{R} \iff \overline{S}R^\mathsf{T} \subseteq \overline{Q}$
(4) the *Tarski rule*, i.e., that for all relations R and all universal relations with appropriate types it holds $R \neq \mathsf{O} \iff \mathsf{L}R\mathsf{L} = \mathsf{L}$.

In the relation-algebraic proofs of this paper we only indicate applications of (3), (4) and consequences of the above axioms that are not obvious. Furthermore, we assume that complementation and transposition bind stronger than composition and composition binds stronger than union and intersection.

In the following we define some specific classes of relations, for more details we refer again to [15,16]. If R is *homogeneous*, i.e., of type $X \leftrightarrow X$, R is called *irreflexive* iff $R \subseteq \overline{\mathsf{I}}$ and *symmetric* iff $R = R^\mathsf{T}$. A homogeneous relation R is *reflexive* iff $\mathsf{I} \subseteq R$, *antisymmetric* iff $R \cap R^\mathsf{T} \subseteq \mathsf{I}$, and *transitive* iff $RR \subseteq R$. A reflexive, antisymmetric and transitive relation R is a *order relation* and if additionally $R \cup R^\mathsf{T} = \mathsf{L}$ holds, i.e., R is *linear*, then R is called a *linear order relation*. A relation R is *univalent* iff $R^\mathsf{T}R \subseteq \mathsf{I}$ and *total* iff $R\mathsf{L} = \mathsf{L}$. A *mapping* is a univalent and total relation.

A *vector* is a relation v with $v = v\mathsf{L}$. For a set-theoretic relation $v : X \leftrightarrow Y$ the equality $v = v\mathsf{L}$ means that v is of the form $v = Z \times Y$ with a subset Z of X. Then we say that v *models the subset* Z of X. Since for this purpose the target of a vector is irrelevant, we use the specific singleton set $\mathbf{1}$ as target. Moreover, a *point* p is a vector that is *injective* and *surjective*, i.e., $pp^\mathsf{T} \subseteq \mathsf{I}$ and $\mathsf{L}p = \mathsf{L}$.

We also assume the following version of the *Point Axiom* of [7] holding for set-theoretic relations, where $\mathcal{P}(v) := \{p \mid p \subseteq v \wedge p \text{ is point}\}$ for all vectors v.

Axiom 2.1. *For all objects X we have* $\mathsf{L}_{X\mathbf{1}} = \bigcup_{p \in \mathcal{P}(\mathsf{L}_{X\mathbf{1}})} p$.

Additionally we have the following lemma which states that this property can be generalised for arbitrary vectors (see [7]).

Lemma 2.1. *If $v : X \leftrightarrow \mathbf{1}$ is a vector, then* $v = \bigcup_{p \in \mathcal{P}(v)} p$. □

In [9], Kawahara investigates the cardinality of set-theoretic relations. The main result is a characterisation of the cardinalities of relations. Considering the properties of this characterisation as axiomatic specification of the cardinality operation $|\cdot|$ leads to the following definition:

Definition 2.1. *For all relations R we denote its cardinality by $|R|$. The following axioms specify the meaning of the cardinality operation, where Q, R and S are arbitrary relations with appropriate types:*

(C1) If R is finite, then $|R| \in \mathbb{N}$ and $|R| = 0$ iff $R = \mathsf{O}$.
(C2) $|R| = |R^\mathsf{T}|$.
(C3) If R and S are finite, then $|R \cup S| = |R| + |S| - |R \cap S|$.
(C4) If Q is univalent, then $|R \cap Q^\mathsf{T}S| \leq |QR \cap S|$ and $|Q \cap SR^\mathsf{T}| \leq |QR \cap S|$.
(C5) $|\mathsf{I}_\mathbf{1}| = 1$.

In (C1) and (C3) the occuring relations are assumed to be finite so that the cardinality $|R|$ can be regarded as a natural number, in (C2) and (C4) the notation $|R| = |S|$ (respectively $|R| \leq |S|$) is equivalent to the fact that there exists a bijection between R and S (respectively an injection from R to S) and (C5) says that the identity relation on the set $\mathbf{1}$ contains precisely one pair. In the present paper we assumes in case of an expression $|R|$ the sets of R's type to be finite and thus $|R| \in \mathbb{N}$.

Based on the above axioms in [9] a lot of laws for the cardinality operation are derived in a purely algebraic manner, for instance, the monotonicity of the cardinality operation, i.e., that $R \subseteq S$ implies $|R| \leq |S|$. Futhermore, they imply $|\bigcup_{R \in \mathcal{R}} R| = \sum_{R \in \mathcal{R}} |R|$, for all finite sets $\mathcal{R}$ of pairwise disjoint relations. Other consequences of the axioms we use in the remainder are the following:

Lemma 2.2.

1. *If R and S are univalent, then $|RS \cap Q| = \left|R \cap QS^{\mathsf{T}}\right|$.*
2. *If R is univalent and S is a mapping, then $|RS| = |R|$.*
3. *If R is univalent, then $|R^{\mathsf{T}}S| \leq |S|$.*

The cardinality of points and vectors of type $X \leftrightarrow \mathbf{1}$ can be studied by using the above results. The next lemma states that a point contains exactly one pair.

Lemma 2.3. *If $p : X \leftrightarrow \mathbf{1}$ is a point, then $|p| = 1$.*

Proof. Using cardinality axioms (C2) and (C5) and Lemma 2.2 ($\mathbb{1}_{\mathbf{11}}$ is univalent and $p^{\mathsf{T}} : \mathbf{1} \leftrightarrow X$ is a mapping), we have the following calculation:

$$|p| = |p^{\mathsf{T}}| = |\mathbb{1}_{\mathbf{11}} p^{\mathsf{T}}| = |\mathbb{1}_{\mathbf{11}}| = 1. \qquad \square$$

This lemma allows to show that the cardinality of a vector with target $\mathbf{1}$ is equal to the cardinality of the set of all points it contains.

Lemma 2.4. *For all $v : X \leftrightarrow \mathbf{1}$ we have $|v| = |\mathcal{P}(v)|$.*

Note that in the above lemma with $|\mathcal{P}(v)|$ we denote the usual cardinality of the set $\mathcal{P}(v)$. For more details, in particular omitted proofs, and results concerning the cardinality operation as well as applications we refer to [1,3,9].

3 Approximating Minimal Vertex Colorings

In [2] the authors present a relational program for computing vertex colorings in undirected (and loop-free) graphs. The verification tasks arising by applying the assertion-based verification method are supported by the automated theorem prover Prover9 and the proof assistants Coq and Isabelle/HOL. By this example the advantages and disadvantages of these tools are studied and compared.

The presented program is based on the well-known Greedy algorithm that assigns sequentially a proper color to each vertex, i.e., a color that is not already assigned to one of its neighbours. This procedure does not consider the fact that one is usually interested in computing a minimal and not an arbitrary coloring of a graph. Thus, one usually assumes the colors to be ordered so that the algorithm chooses a minimal color for each vertex. By this approach a minimal vertex coloring is approximated with a ratio of $\Delta + 1$, where Δ is the maximum degree of the given graph.

In [2] the approximation ratio is not treated at all. Thus, in the remainder of this section we prove the ratio of the following program with the modified choice of the color q using the results about the cardinality operation presented in Sect. 2:

$C := \mathsf{O}$;
while $C\mathsf{L} \neq \mathsf{L}$ **do**
  let $p = point(\overline{C\mathsf{L}})$;
  let $q = point(\overline{C^{\mathsf{T}}Ep} \cap \overline{\overline{M}\,\overline{C^{\mathsf{T}}Ep}})$;
  $C := C \cup pq^{\mathsf{T}}$ **od**

The input relations of this program are an *adjacency relation* $E : X \leftrightarrow X$, modelling a given graph G with a set of vertices X, and a linear order relation $M : F \leftrightarrow F$ on a set of colors F. The output relation of the program is $C : X \leftrightarrow F$ representing the vertex coloring, i.e., a mapping so that in addition $CC \subseteq \overline{E}$ holds. The latter condition is called the coloring property. Furthermore, all occuring universal relations in the program have target $\mathbf{1}$. As in [2] we assume the deterministic operation *point* selecting a point to a given nonempty vector v such that $point(v) \subseteq v$. For more details we refer to [2] since the only difference to our program is the choice of the point q. In [2], q is choosen as $point(\overline{C^\mathsf{T}Ep})$, i.e., q is not used for one of p's neighbours. If we choose q as $point(\overline{C^\mathsf{T}Ep} \cap \overline{M}\,\overline{C^\mathsf{T}Ep})$ instead we also ensure that q is minimal since $\overline{C^\mathsf{T}Ep} \cap \overline{M}\,\overline{C^\mathsf{T}Ep}$ is the vector of all minimal colors w.r.t. the order relation M, see, e.g., [16] for further information.

To formally verify the correctness of the above program we apply the assertion-based verification method. Thus, we first specify the programs' pre- and postcondition. The precondition is the conjunction of the following formulae specifying E as an adjacency relation, i.e., an irreflexive and symmetric relation, and M as a linear, reflexiv and antisymmetric relation (transitivity is not needed here).

$$Pre(E, M) \;:\Longleftrightarrow\; E = E^\mathsf{T} \wedge E \subseteq \bar{\mathsf{I}} \wedge \mathsf{I} \subseteq M \wedge M \cap M^\mathsf{T} \subseteq \mathsf{I} \wedge M \cup M^\mathsf{T} = \mathsf{L}_{FF}$$

In the remainder we furthermore use the abbreviation $\Delta_v := \max\{|Ex| \mid x \in \mathcal{P}(v)\}$ for all vectors v and $\Delta := \Delta_\mathsf{L}$ for the maximum degree of a given graph modelled by E. If we do not specify a universal or empty relation's type in this section we assume its target to be $\mathbf{1}$.

The postcondition is a conjuction of three formulae stating that C is a vertex coloring, i.e., an univalent and total relation fulfilling the coloring property, and a formula saying that the number of used colors is at most $\Delta + 1$:

$$Post(C, E) \;:\Longleftrightarrow\; C^\mathsf{T}C \subseteq \mathsf{I} \wedge C\mathsf{L} = \mathsf{L} \wedge CC^\mathsf{T} \subseteq \overline{E} \wedge |C^\mathsf{T}\mathsf{L}| \leq \Delta + 1$$

The invariant is a conjunction of four formulae, where the first two ensure that C is univalent and fulfills the coloring property and the latter two are essential for proving the desired approximation ratio:

$$Inv(C, E, M) \;:\Longleftrightarrow\; C^\mathsf{T}C \subseteq \mathsf{I} \wedge CC^\mathsf{T} \subseteq \overline{E} \wedge C^\mathsf{T}\mathsf{L} \subseteq \overline{\overline{M}\,\overline{C^\mathsf{T}\mathsf{L}}} \wedge |C^\mathsf{T}\mathsf{L}| \leq \Delta_{C\mathsf{L}} + 1$$

As usual the following proof obligations have to be proved for partial correctness:

(PO1) $Pre(E, M) \Longrightarrow Inv(E, M, \mathsf{O})$
(PO2) $Inv(E, M, C) \wedge C\mathsf{L} = \mathsf{L} \Longrightarrow Post(E, C)$
(PO3) $Pre(E, M) \wedge Inv(E, M, C) \wedge C\mathsf{L} \neq \mathsf{L} \Longrightarrow Inv(E, M, C \cup pq^\mathsf{T})$ (where p and q are defined as in the given program).

Since $Pre(E, M), Post(E, C)$ and $Inv(E, M, \mathsf{O})$ are conjunctions of various formulae the three obligations can be splitted into single statements for each formula. In the remainder we only consider the statements involving cardinalities.

For the omitted proofs we refer to Sects. 4 and 5 and the appendix. Here, we start with proving the first proof obligation (PO1), i.e., the establishment of the last formula of the invariant.

Lemma 3.1. *For all relation E and M it holds $Inv(E, M, \mathsf{O})$.*

Proof. The last formula of the invariant is shown by using cardinality axiom (C1) two times: $|\mathsf{O}^\mathsf{T}\mathsf{L}| = 0 \leq 1 \leq \Delta_{\mathsf{OL}} + 1$. □

Next, we prove (PO2), i.e., that the invariant and the negation of the loop-condition imply the postcondition. Again we concentrate on the last formula involving cardinalities.

Lemma 3.2. *Let E, C, M be relations such that E is symmetric and irreflexive, M is reflexive, antisymmetric and linear and $C\mathsf{L} = \mathsf{L}$ and $Inv(E, C, M)$ holds. Then $Post(E, C)$ holds.*

Proof. Using $Inv(E, C, M)$ in the first and $C\mathsf{L} = \mathsf{L}$ in the second step we have the following inequality: $|C^\mathsf{T}\mathsf{L}| \leq \Delta_{C\mathsf{L}} + 1 = \Delta_\mathsf{L} + 1 = \Delta + 1$. □

For proving (PO3), i.e., the maintenance of the last formula of the invariant, we need the following auxiliary result.

Lemma 3.3. *Let R be a reflexive, anstisymmetric and linear relation. Then $R^\mathsf{T} = \mathsf{I} \cup \overline{R}$ holds.*

Proof. Using the antisymmetry of R we have:

$$R \cap R^\mathsf{T} \subseteq \mathsf{I} \iff R \cap R^\mathsf{T} \cap \bar{\mathsf{I}} \subseteq \mathsf{O} \iff R^\mathsf{T} \subseteq \overline{R \cap \bar{\mathsf{I}}} \iff R^\mathsf{T} \subseteq \mathsf{I} \cup \overline{R}.$$

By the linearity and reflexivity of R we show:

$$R \cup R^\mathsf{T} = \mathsf{L} \iff \overline{R \cup R^\mathsf{T}} \subseteq \mathsf{O} \iff \overline{R} \cap \overline{R^\mathsf{T}} \subseteq \mathsf{O} \iff \overline{R} \subseteq R^\mathsf{T} \Longrightarrow \mathsf{I} \cup \overline{R} \subseteq R^\mathsf{T}. \quad \square$$

Using the latter Lemma we show the maintenance of the invariants' last formula:

Lemma 3.4. *Let E, C and M be relations so that $Pre(E, M)$ and $Inv(E, M, C)$ hold and p, q points with $p \subseteq \overline{C\mathsf{L}}$, $q \subseteq \overline{C^\mathsf{T}Ep} \cap \overline{M}\,\overline{C^\mathsf{T}Ep}$. Then $|(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L}| \leq \Delta_{(C \cup pq^\mathsf{T})\mathsf{L}} + 1$ holds.*

Proof. Since p and q are points it holds $qp^\mathsf{T}\mathsf{L} = q$ and thus $|(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L}| = |C^\mathsf{T}\mathsf{L} \cup q|$. For the same reasons we have $pq^\mathsf{T}\mathsf{L} = p$ which implies $\Delta_{(C \cup pq^\mathsf{T})\mathsf{L}} = \Delta_{C\mathsf{L} \cup p}$ Hence we have to show $|C^\mathsf{T}\mathsf{L} \cup q| \leq \Delta_{C\mathsf{L} \cup p} + 1$.

Using (C3) and Lemma 2.3 we have the following equality:

$$|C^\mathsf{T}\mathsf{L} \cup q| = |C^\mathsf{T}\mathsf{L}| + |q| - |C^\mathsf{T}\mathsf{L} \cap q| = |C^\mathsf{T}\mathsf{L}| + 1 - |C^\mathsf{T}\mathsf{L} \cap q|.$$

If $q \subseteq C^\mathsf{T}\mathsf{L}$ it holds $|C^\mathsf{T}\mathsf{L} \cap q| = |q| = 1$. In this case the claim follows immediately with the assumption $Inv(C, E, M)$, in particular the last formula of it, and the fact that $\Delta_{C\mathsf{L}} \leq \Delta_{(C \cup pq^\mathsf{T})\mathsf{L}}$.
Hence, we consider the case that $q \subseteq \overline{C^\mathsf{T}\mathsf{L}}$. Then $C^\mathsf{T}\mathsf{L} \cap q = \mathsf{O}$ and it follows$|C^\mathsf{T}\mathsf{L} \cup q| = |C^\mathsf{T}\mathsf{L}| + 1$. Thus, it is sufficient to show that $|C^\mathsf{T}\mathsf{L}| + 1 \leq \Delta_{C\mathsf{L} \cup p} + 1$ holds.So we show that $|C^\mathsf{T}\mathsf{L}| \leq \Delta_{C\mathsf{L} \cup p}$, and therefor, $|C^\mathsf{T}\mathsf{L}| \leq |Ep|$.

Because of $q \subseteq \overline{C\mathsf{L}}$ and the third formula of $Inv(E, M, C)$ we have

$$q \cup \overline{M}q \subseteq \overline{C^\mathsf{T}\mathsf{L}} \cup \overline{M}\,\overline{C^\mathsf{T}\mathsf{L}} \subseteq \overline{C^\mathsf{T}\mathsf{L}}$$

and thus

$$C^\mathsf{T}\mathsf{L} \subseteq \overline{q} \cap \overline{\overline{M}q}. \tag{1}$$

Next, we prove

$$\overline{q} \cap \overline{\overline{M}q} \subseteq C^\mathsf{T}Ep \tag{2}$$

by the following calculation:

$$\begin{aligned}
q \subseteq \overline{M\,\overline{C^\mathsf{T}Ep}} &\iff \overline{M}\,\overline{C^\mathsf{T}Ep} \subseteq \overline{q} \\
&\iff \overline{M^\mathsf{T}}q \subseteq C^\mathsf{T}Ep && \textit{Schröder rule} \\
&\iff \overline{\mathsf{I} \cup \overline{M}}q \subseteq C^\mathsf{T}Ep && \text{Lemma 3.3} \\
&\iff \overline{(\mathsf{I} \cup \overline{M})q} \subseteq C^\mathsf{T}Ep && q \text{ point} \\
&\iff \overline{q \cup \overline{M}q} \subseteq C^\mathsf{T}Ep \\
&\iff \overline{q} \cap \overline{\overline{M}q} \subseteq C^\mathsf{T}Ep.
\end{aligned}$$

Using (1), (2) and Lemma 2.2.1 (C is univalent because of $Inv(E, M, C)$) as well as the monotonicity of the cardinality operation we obtain the desired inequality:

$$|C^\mathsf{T}\mathsf{L}| \leq |\overline{q} \cap \overline{\overline{M}q}| \leq |C^\mathsf{T}Ep| \leq |Ep|.$$

□

4 Cardinalities in Coq

In [2] the proofs of the according obligations (PO1)–(PO3) presented in Sect. 3 are mechanised amongst others with the proof assistant Coq using the library *RelationAlgebra* which provides a model for heterogeneous relation algebra and many other related algebraic structures. The library is available via [13], and presented in [14]. For more general information about Coq we refer to [4,20].

In [5] the authors extend the mentioned library so that a reasoning about cardinalities is possible. *RelationAlgebra* is enriched by the module `relalg` containing the most important definitions of special classes of relations, e.g., those introduced in Sect. 2. For the tools concerning cardinalities a standalone library was developed. To preserve the modularity of *RelationAlgebra* this library provides a separate module for each algebraic structure we defined in Sect. 2. The hierarchy of the modules is illustrated in Fig. 1.

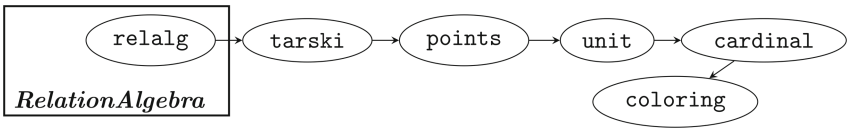

Fig. 1. Hierarchy of the Coq library

To simplify rewriting, the definitions are realized by using classes, for instance, being univalent is defined as follows:

```
Class is_univalent n m (x: X n m) := univalent: x^T * x <== 1.
```

Here, the variables `n` and `m` specify the type of the relation `x` and `X` provides the notions and operations of a relation algebra. The symbols ^{T},$*$ and $<==$ denote transposition, composition and inclusion. The type of the identity relation denoted by `1` is inferred automatically. In `points` the *Point Axiom* is assumed and several resulting facts are proved, especially those presented in Sect. 2. The definition of the cardinality operation is given in `cardinal` and follows the one presented in Sect. 2. A detailed description of each module and the notations can be found in [5].

In `cardinal` the proofs of all lemmata of Sect. 2 (and many more) are mechanised, for instance, Lemma 2.3 as follows:

```
Lemma card_point X (R: C X unit): is_point R → card R = 1.
Proof. rewrite ←cardcnv, ←dot1x. rewrite card_unimap. apply card1. Qed.
```

Here, `is_point` specifies the relation `R` as a point and `card` denotes the cardinality operation. The Coq proof follows exactly the one of Sect. 2 where `cardcnv`, `card_unimap` and `card1` correspond to (C2), Lemma 2.2 and (C5).

With the extended library all proofs of Sect. 3 can be done within Coq. In the following we show the formulations of the Lemmata 3.1, 3.4 and 3.2 where `inv` is the definition of the invariant as given in Sect. 3 (the adjacency and order relation are introduced at the beginning of our Coq module once and for all) and `minimal_elements M v` the vector of the minimal elements of a vector `v` w.r.t. a linear order relation `M`:

```
Lemma PO1: inv (zer n f).
Lemma PO2 (F: X n f) : inv F ∧ F*(top' f unit) == top → post (F ∪ p*q^T).
Lemma PO3 (F: X n f) (p: X n unit) (q: X f unit):
          is_point p → p <== !(F*top) →
          is_point q → q <== minimal_elements M (!(F^T*E*p)) →
          inv F → inv (F ∪ p*q^T).
```

Mainly, the proofs have to be done step by step. At some points we benefit at the one hand from the smart implementation of the specific relations that makes rewriting less difficult and on the other hand from the decision tactics provided by *RelationAlgebra*. A detailed description of those tactics can be found in [14].

5 Cardinalities in Isabelle/HOL

In this section we show how the proof assistant Isabelle/HOL can be used to prove the correctness of the program of Sect. 3. In particular, we develop the required theoretical framework for it.

Compared to the one of Coq the type system of Isabelle/HOL is less powerful. In the end the usage of multi-parameter classes is not possible whereby there is no trivial way to define heterogeneous relation algebras. Thus, our Isabelle/HOL theories built on an existing library, *Relation_Algebra*, for homogeneous relation algebras only, available via the *Archive of Formal Proofs*, see [17]. More general information about Isabelle/HOL can be found, for example, in [8,12].

This limitation makes it impossible to transfer the approach realised in Coq to Isabelle/HOL. Namely, if we consider points of type $X \leftrightarrow \mathbf{1}$, for instance, it was essential for the proofs of Sect. 3 that they have cardinality 1. This fact is mainly based on the cardinality axiom (C5) and the specific type $X \leftrightarrow \mathbf{1}$. When using the *Relation_Algebra* library we are not only restricted to homogeneous relation algebras, but to untyped relations.

Due to this, we have to modify the definition of the cardinality operation of Sect. 2. The first four axioms (C1)–(C4) can be adapted to untyped relations, but (C5) involves the special singleton set $\mathbf{1}$. Thus, we assume the following fifth axiom instead saying that the cardinality of the identity relation equals the number of points (in the relation algebra):

$$\text{(C5')}\ |\mathsf{I}| = |\mathcal{P}(\mathsf{L})|.$$

Note that there are equivalent formulations of (C5'), e.g., $|\mathsf{L}| = |\mathsf{I}|^2$, but for us, the given one is the most intuitive compared to (C5).

In the remainder we also assume a version of the *Point Axiom* for untyped relations. The only difference to Axiom 2.1 is that the occuring universal relation is untyped.

Axiom 5.1. *(Point Axiom). It holds* $\mathsf{L} = \bigcup_{p \in \mathcal{P}(\mathsf{L})} p$.

One can easily check that we get the following corresponding consequences as in Sect. 2.

Lemma 5.1.

1. *For all vectors* v *we have* $v = \bigcup_{p \in \mathcal{P}(v)} p$.
2. *We have* $\mathsf{I} = \bigcup_{p \in \mathcal{P}(\mathsf{L})} pp^\mathsf{T}$.

Furthermore, the Lemma 2.2 also holds in the case of untyped relations. The first important result which is significantly different, due to (C5'), is stated in the following lemma and gives us the cardinality of (untyped) points.

Lemma 5.2. *If* p *is a point, then* $|p| = |\mathsf{I}|$.

Proof. Using cardinality axioms (C2) and (C5') and Lemma 2.2 (I is univalent and p^T is a mapping) we have $|p| = |p^\mathsf{T}| = |\mathsf{I}p^\mathsf{T}| = |\mathsf{I}|$. □

Obviously, because of the above lemma, points and vectors are no longer suitable for modelling sets if their cardinalities are essential in the context. Thus, in the following and in particular for the formalisation is Isabelle/HOL we use *partial identities*, i.e., relations R with $R \subseteq \mathsf{I}$, instead of vectors to represent sets. In place of points we consider *atoms*, i.e., nonempty relations a with $a\mathsf{L}a^\mathsf{T} \subseteq \mathsf{I}$. We show that the cardinalities of those special relations correspond to the ones of vectors and points. Therefore, we start with a lemma about the cardinality of (untyped) vectors.

Lemma 5.3. *If v is a vector, then $|v| = |\mathcal{P}(v)| \cdot |\mathsf{I}|$.*

Proof. Because of Lemma 5.1, cardinality axioms (C3) and (C1) (the points in $\mathcal{P}(v)$ are pairwise disjoint) and Lemma 5.2 we obtain the claim by

$$|v| = \Big|\bigcup_{p \in \mathcal{P}(v)} p\Big| = \sum_{p \in \mathcal{P}(v)} |p| = \sum_{p \in \mathcal{P}(v)} |\mathsf{I}| = |\mathcal{P}(v)| \cdot |\mathsf{I}|. \qquad \square$$

Note that the above result holds in particular for $v = \mathsf{L}$ since L is a vector. This gives us $|\mathsf{L}| = |\mathsf{I}|^2$ because of (C5').

To prove that every atom has cardinality 1 we need the following technical lemma whose proof we omit due to the lack of space. It states that every atom is the composition of a point and a points' transposed (and vice versa), and that the universal relation can be written as the union of all atoms it contains. Here, we denote the set of all atoms (containted in L) as $\mathcal{A}(\mathsf{L})$.

Lemma 5.4.

1. *It holds $\mathcal{A}(\mathsf{L}) = \{p; q^\mathsf{T} | p, q \in \mathcal{P}(\mathsf{L})\}$.*
2. *It holds $\mathsf{L} = \bigcup_{a \in \mathcal{A}(\mathsf{L})} a$.*

From this we get the desired result about the cardinalities of atoms.

Lemma 5.5. *If a is an atom, then $|a| = 1$.*

Proof. For all atoms a it holds $a \neq \mathsf{O}$ and thus $|a| \geq 1$ with cardinality axiom (C1). We prove $|a| = 1$, for all atoms a, by contradiction. Thus, we assume that there exists an atom b with $|b| > 1$. Combining Lemmas 5.3 and 5.4.2 (for $v = \mathsf{L}$) we have $\mathcal{A}(\mathsf{L}) = |\mathsf{I}|^2$. Due to this and again Lemmas 5.3 and 5.4.2 we have

$$\begin{aligned} |\mathsf{I}|^2 = |\mathsf{L}| = |\bigcup_{a \in \mathcal{A}(\mathsf{L})} a| = \sum_{a \in \mathcal{A}(\mathsf{L})} |a| = |b| + \sum_{a \in \mathcal{A}(\mathsf{L}) \setminus \{b\}} |a| \\ > 1 + \sum_{a \in \mathcal{A}(\mathsf{L}) \setminus \{b\}} 1 = 1 + |\mathcal{A}(\mathsf{L}) \setminus \{b\}| = 1 + |\mathsf{I}|^2 - 1, \end{aligned}$$

which is a contradiction. $\square$

From this we get that partial points have cardinality 1 which makes them suitable for modelling single elements of sets.

Lemma 5.6. *If p is a partial point, then $|p| = 1$.*

Proof. By definition, p is an atom, thus the claim follows immediately with Lemma 5.5. □

We omit the corresponding proofs of the correctness of the program of Sect. 3, but refer to the Isabelle/HOL formalisation we describe in the remainder of this section and available via the web, see [18].

So far, the library *Relation_Algebra* provides several facts holding in untyped relation algebras as well as theories about functions and vectors with related facts, so that most of the specific relations mentioned in Sect. 2 are already defined. For instance, for vectors this is done in the following way

```
definition is_vector :: "'a ⇒ bool"
  where "is_vector x ≡ x = x;1"
```

In the library the symbols $+$, $\cdot$, $-$, ; and $\breve{}$ are used for union, intersection, complement, composition and transposition and 1, 0 and $1'$ for the universal, empty and identity relation. For our purpose we import additional theory, e.g., about natural numbers, so that we use $\sqcup$, $\sqcap$, and $^\cdot$ for the first three operations and *top*, *bot* and $1'$ for the constants L, O and I. As in the case of Coq neither the *Tarski rule* nor the *Point Axiom* is provided by the library so far. Follow the approach in Coq we develop a separate theory for each structure we define. The dependencies of the main theories are illustrated in Fig. 2.

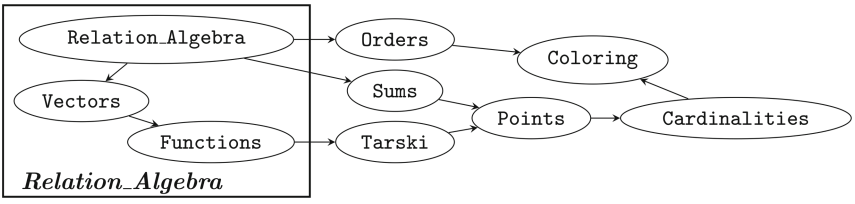

Fig. 2. Hierarchy of the Isabelle/HOL library

First, we extend the class *relation_algebra* by the *Tarski rule* using a class:

```
class relation_algebra_tarski = relation_algebra +
  assumes tarski: "x ≠ bot ⟷ top;x;top = top"
```

This is done in the theory *Relation_Algebra_Tarski* where we derive some fundametal properties of points, for instance the following one:

```
lemma points_surj: "is_point p ⟶ is_sur p"
```

The theory *Relation_Algebra_Points* is an extension of the latter providing the Axiom 5.1 and that the number of points is finite:

```
class relation_algebra_fin_points = relation_algebra_tarski +
  assumes finiteness:        "finite {x. is_point x}"
  and     pointaxiom [simp]: "⨆ {x. is_point x} = top"
```

Here, $\bigsqcup\{x.\ is\_point\ x\}$ is a notation for $\bigcup_{p \in \mathcal{P}(\mathsf{L})} p$ in Isabelle/HOL. In the theory *Relation_Algebra_Sums* we proved a several properties of these finite unions, e.g., monotonicity.

Finally, we have a theory called *Relation_Algebra_Cardinalities* where the cardinality operation is defined in the following way:

```
class cardinal =
  fixes cd :: "'a ⇒ nat" ("|_|" [30] 999)
class relation_algebra_card = cardinal + relation_algebra_fin_points +
  assumes card0      : "|x| = (0 :: nat) ⟷ x = bot"
  and cardcnv [simp] : "|x⌣| = |x|"
  and cardcup        : "|x ⊔ y| = |x| + |y| − |x ⊓ y)|"
  and cardded        : "is_p_fun x ⟶ |y ⊓ (x⌣; z)| ≤ |(x; y) ⊓ z|"
  and cardded'       : "is_p_fun x ⟶ |x ⊓ (z; y⌣)| ≤ |(x; y) ⊓ z|"
  and cardone        : "|1'| = card {x. is_point x}"
```

Here, *card* is the built-in operation for the cardinality of sets. With the given definition we are able to prove the mentioned results about cardinalities, for instance:

```
lemma cardunifun : assumes "is_p_fun x" and "is_fun y" shows "|x; y| = |x|"
lemma cardpoint : assumes "is_point x" shows "|x| = |1'|"
```

The proofs of these lemmata are found automatically by Sledgehammer. From this we get immediately that the cardinality of a point equals the cardinality of the identity relation. In the same way we formalise all lemmata of this section and many more where most of the proofs are heavily supported by Sledgehammer.

For the verification of the program of Sect. 3 we do not only use the above mentioned theories about relation algebra and cardinalities, but also a library for Hoare Logic in Isabelle/HOL, see [11]. This library provides the opportunity to write, for instance, while-programs as theorems as well as tactics generating the proof obligations for partial correctness automatically. Thus we can encode the program as follows.

```
theorem correctness: "VARS e m c p q
 { pre e m}
 c := bot;
 WHILE c • top ≠ top
   INV { inv e m c }
    DO p := point((c • top)ᶜ);
       q := point((c⌣ • e • p)ᶜ ⊓ (mᶜ • (c⌣ • e • p)ᶜ)ᶜ);
       c := c ⊔ p • q⌣
    OD
 { post e c }"
```

Unfortunately, we have to switch to another symbol for composition here since; is already defined in the theory for Hoare logic. Thus, we use $\bullet$ in this context. The pre- and postconditions and the invariant slightly differ from the ones presented in Sect. 3 since we have to use partial points and identities for proving the approximation bound.

definition "$pre\ e\ m \longleftrightarrow is\_irrefl\ e \wedge is\_symm\ e \wedge is\_lin\_order\ m$"
definition "$post\ e\ c \longleftrightarrow is\_fun\ c \wedge has\_color\_prop\ e\ c \wedge |c^\smile \bullet top \sqcap 1'| \leq \Delta_{top} + 1$"
definition "$inv\ e\ m\ c \longleftrightarrow pre\ e\ m \wedge is\_p\_fun\ c \wedge has\_color\_prop\ e\ c$
$\wedge\ c^\smile \bullet top \sqsubseteq (m^\mathsf{c} \bullet (c^\smile \bullet top)^\mathsf{c})^\mathsf{c} \wedge\ |c^\smile \bullet top \sqcap 1'| \leq \Delta_{c \bullet top} + 1$"

One of the big advantages of using the theory for Hoare Logic is that its provides tactis for verification condition generation. In the case of our program or theorem, respectively, we can apply the rule *vcg_simp*. With this rule the three proof obligations w.r.t. the given pre- and postconditions and the loop-invariant are generated as subgoals automatically. In the following we see the resulting subgoals after applying *vcg_simp*.

goal (3 subgoals):
1. $\bigwedge e\ m\ c\ p\ q.\ pre\ e\ m \Longrightarrow inv\ e\ m\ bot$
2. $\bigwedge e\ m\ c\ p\ q.\ inv\ e\ m\ c \wedge c \bullet top \neq top \Longrightarrow$
$inv\ e\ m\ (c \sqcup point((c \bullet top)^\mathsf{c}) \bullet point((c^\smile \bullet e \bullet p)^\mathsf{c} \sqcap (m^\mathsf{c} \bullet (c^\smile \bullet e \bullet p)^\mathsf{c})^\mathsf{c}))$
3. $\bigwedge e\ m\ c\ p\ q.\ inv\ e\ m\ c \wedge \neg c \bullet top \neq top \Longrightarrow post\ e\ c$

The three statements are shown stepwise by using the theories mentioned in this section. The proofs that are not found by Sledgehammer automatically are given as structured Isar proofs, see [18], so that the reader can follow the basic ideas.

Besides the results presented in this section our library contains over 150 lemmata about finite unions of relations, points and vectors, atoms, and cardinalities of relations. Furthermore, in *Relation_Algebra_Orders* we defined order related relations and proved several facts about them.

6 Comparison of the Implementations

In Sects. 4 and 5 we show how the proof assistants Coq and Isabelle/HOL can be used for formal program verfication and reasoning about relation algebras in general. In this section we want to summarise our experiences with both systems and highlight their advantages and disadvantages from our point of view.

For Coq, we used an existing library that already implements tools for proving results regarding cardinalities. One advantage of the library is that it extends a library including a model for heterogeneous relation algebras and related structures. Here, the implementation of typed relations is possible because of Coq's expressive type system based on the *predicative calculus of inductive constructions*. Such an expressive type system has many common advantages, for instance, it ensures that all expressions and formulae are well-typed. Thus, the Coq proofs mostly correspond to the handwritten ones we gave in this paper.

Coq, and in particular the used library, provides several automated theorem proving tactics and decision procedures, but most of them were not very helpful in our context. Thus, the proofs have mostly to be done step by step using Coqs standard tactics. Unfortunately, a direct link to automated theorem provers is still missing. Furthermore, the formalisation of the proof obligations of the presented program has to be done by hand since there are no tools for an automated generation. For non-experts the Coq code is quite hard to read without using an IDE illustrating proof steps and subgoals.

By contrast, Isabelle/HOL bridges the gap between interactive and automated theorem proving because of its integrated tool Sledgehammer. Due to the limited type system of Isabelle/HOL there is only an existing library for homogeneous relation algebras. For this reason an extension by the cardinality operation, as in the case of Coq, was not possible directly. Thus, we modified the axiomatisation of the operation to make it applicable for homogeneous relations in the first place. We formalised it in Isabelle/HOL and proved the correctness of the relational program heaviliy supported by Sledgehammer. Unlike Coq, Isabelle/HOL provides a library for Hoare Logic including tactics for generating proof obligations automatically. In our context we were able to avoid typed relations by adapting the cardinality operation. In general, reasoning about typed relations can be managed by using, for instance, predicates specifying the source and target of a relation. Such an approach often results in more complicated and longish proofs. In the future, one can benefit from our library containing most of the basic facts that are necessary when dealing with cardinalities. Certainly, invoking Sledgehammer does not always complete proofs successfully. As in Coq, one has to do steps by hand, but Isabelle/HOL supports the proof language Isar. Its intuitive syntax allows to write proofs structured and comprehensible for non-experts.

7 Concluding Remarks

We presented a correctness proof of a relational program for approximating vertex colorings in undirected (and loop-free) graphs. The proof of the approximation ratio we done by using an operation to reason algebraically about cardinalities in heterogeneous relation algebras.

Furthermore, all proofs were mechanised in both proof assistants Coq and Isabelle/HOL and build on existing libraries for relation algebras. In contrast to Coq, there were no tools to tackle cardinalities in Isabelle/HOL so far. To reuse a library for homogeneous relation algebras we presented a new theoretical framework for reasoning about untyped relations. In this context, we not only proved the programs' correctness in Isabelle/HOL, but also developed a library providing over 150 facts about, for instance, points, atoms and cardinalities.

For the future it would be helpful to have a tool for Hoare Logic in Coq so that the generation of a programs' proof obligations has not to be done by hand or external programs. A further investigation of the new axiomatisation of the cardinality operation is also conceivable to see how exhaustive this approach

is. In general, it would be interesting to study what is provable without the restriction to finite relations.

Acknowledgement. I thank Walter Guttmann and Damien Pous for their help concerning the use of proof assistants and Rudolf Berghammer for helpful discussions and his support, in general. I thank the unknown referees and Michael Winter for their comments and suggestions which helped to improve the paper.

Appendix

In this appendix we show that the third formula of the invariant $Inv(E, M, C)$ is maintained stated in the following lemma.

Lemma. *Let E, C and M be relations so that $Pre(E, M)$ and $Inv(E, M, C)$ hold and p, q points with $p \subseteq \overline{C\mathsf{L}}$, $q \subseteq \overline{C^\mathsf{T} E p} \cap \overline{\overline{M}\,\overline{C^\mathsf{T} E p}}$. Then $(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L} \subseteq \overline{\overline{M}\,\overline{(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L}}}$ holds.*

Proof. Since $Inv(E, M, C)$ holds, we have $C^\mathsf{T}\mathsf{L} \subseteq \overline{\overline{M}\,\overline{C^\mathsf{T}\mathsf{L}}}$ and hence

$$\overline{M}\,\overline{C^\mathsf{T}\mathsf{L}} \subseteq \overline{C^\mathsf{T}\mathsf{L}}. \tag{1}$$

The inclusion

$$\overline{M}\,\overline{C^\mathsf{T}\mathsf{L}} \subseteq \overline{q} \tag{2}$$

is shown by the following calculation:

$$\begin{aligned}
C^\mathsf{T} E p \subseteq C^\mathsf{T}\mathsf{L} &\iff \overline{C^\mathsf{T}\mathsf{L}} \subseteq \overline{C^\mathsf{T} E p} \\
&\implies \overline{M}\,\overline{C^\mathsf{T}\mathsf{L}} \subseteq \overline{M}\,\overline{C^\mathsf{T} E p} \\
&\iff \overline{\overline{M}\,\overline{C^\mathsf{T} E p}} \subseteq \overline{\overline{M}\,\overline{C^\mathsf{T}\mathsf{L}}} \\
&\implies q \subseteq \overline{\overline{M}\,\overline{C^\mathsf{T}\mathsf{L}}} && \text{since } q \subseteq \overline{C^\mathsf{T} E p} \cap \overline{\overline{M}\,\overline{C^\mathsf{T} E p}} \\
&\implies \overline{M}\,\overline{C^\mathsf{T}\mathsf{L}} \subseteq \overline{q}
\end{aligned}$$

Furthermore, we have the following:

$$(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L} \subseteq \overline{\overline{M}\,\overline{(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L}}} \iff \overline{M}\,\overline{(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L}} \subseteq \overline{(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L}}.$$

We now show that the inclusion above on the right-hand side is true where we use that p, q are points and thus $qp^\mathsf{T}\mathsf{L} = q$ again:

$$\begin{aligned}
\overline{M}\,\overline{(C \cup pq^\mathsf{T})^\mathsf{T}\mathsf{L}} &= \overline{M}\,\overline{C^\mathsf{T}\mathsf{L} \cup q} && qp^\mathsf{T}\mathsf{L} = q \\
&= \overline{M}\,(\overline{C^\mathsf{T}\mathsf{L}} \cap \overline{q})
\end{aligned}$$

$$
\begin{aligned}
&\subseteq \overline{M\,\overline{C^{\mathsf{T}}\mathsf{L}}} \cap \overline{M\bar{q}} \\
&\subseteq \overline{M\,\overline{C^{\mathsf{T}}\mathsf{L}}} \\
&\subseteq \overline{C^{\mathsf{T}}\mathsf{L}} \cap \bar{q} && \text{(1) and (2)} \\
&= \overline{C^{\mathsf{T}}\mathsf{L} \cup q} \\
&= \overline{(C \cup pq^{\mathsf{T}})^{\mathsf{T}}\mathsf{L}}. && qp^{\mathsf{T}}\mathsf{L} = q
\end{aligned}
$$

□

References

1. Berghammer, R., Danilenko, N., Höfner, P., Stucke, I.: Cardinality of relations with applications. Discret. Math. **339**(12), 3089–3115 (2016)
2. Berghammer, R., Höfner, P., Stucke, I.: Tool-based verification of a relational vertex coloring program. In: Kahl, W., Winter, M., Oliveira, J.N. (eds.) RAMICS 2015. LNCS, vol. 9348, pp. 275–292. Springer, Cham (2015). doi:10.1007/978-3-319-24704-5_17
3. Berghammer, R., Höfner, P., Stucke, I.: Cardinality of relations and relational approximation algorithms. J. Log. Algebraic Methods Program. **85**(2), 269–286 (2016)
4. Bertot, Y., Castéran, P., Huet, G., Paulin-Mohring, C.: Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of iInductive Constructions. Texts in Theoretical Computer Science. Springer, Heidelberg (2004)
5. Brunet, P., Pous, D., Stucke, I.: Cardinalities of finite relations in Coq. In: Blanchette, J.C., Merz, S. (eds.) ITP 2016. LNCS, vol. 9807, pp. 466–474. Springer, Cham (2016). doi:10.1007/978-3-319-43144-4_29
6. Freyd, P., Scedrov, A.: Categories, Allegories. Elsevier Science, Amsterdam (1990). North-Holland Mathematical Library
7. Furusawa, H.: Algebraic formalisations of fuzzy relations and their representation theorems. Ph.D. thesis, Department of Informatics, Kyushu University (1998)
8. Isabelle. https://isabelle.in.tum.de/
9. Kawahara, Y.: On the cardinality of relations. In: Schmidt, R.A. (ed.) RelMiCS 2006. LNCS, vol. 4136, pp. 251–265. Springer, Heidelberg (2006). doi:10.1007/11828563_17
10. Maddux, R.D.: Relation Algebras. Studies in Logic and the Foundations of Mathematics, vol. 150. Elsevier, Amsterdam (2006)
11. Nipkow, T.: Hoare logics in Isabelle/HOL. In: Schwichtenberg, H., Steinbrüggen, R. (eds.) Proof and System-Reliability, pp. 341–367. Kluwer, Dordrecht (2002)
12. Nipkow, T., Wenzel, M., Paulson, L.C.: Isabelle/HOL: A Proof Assistant for Higher-Order Logic. LNCS, vol. 2283. Springer, Heidelberg (2002)
13. Pous, D.: Relation Algebra and KAT in Coq. http://perso.ens-lyon.fr/damien.pous/ra/
14. Pous, D.: Kleene algebra with tests and Coq tools for while programs. In: Blazy, S., Paulin-Mohring, C., Pichardie, D. (eds.) ITP 2013. LNCS, vol. 7998, pp. 180–196. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39634-2_15
15. Schmidt, G.: Relational Mathematics, vol. 132. Cambridge University Press, Cambridge (2011). Encyclopedia of Mathematics and Its Applications

16. Schmidt, G., Ströhlein, T.: Relations and Graphs - Discrete Mathematics for Computer Scientists. EATCS Monographs on Theoretical Computer Science. Springer, Heidelberg (1993)
17. Struth, G., Weber, T.: Relation Algebra. Archive of Formal Proofs (2014). https://www.isa-afp.org/entries/Relation_Algebra.shtml
18. Stucke, I.: Reasoning about Cardinalities Supported by Proof Assistants, Proof Scripts. http://www.rpe.informatik.uni-kiel.de/en/Staff/ist/ramics-2017
19. Tarski, A.: On the calculus of relations. J. Symb. Log. **6**(3), 73–89 (1941)
20. The Coq Proof Assistant. https://coq.inria.fr