

## **A semiring approach to equivalences, bisimulations and control**

**Roland Glück, Bernhard Möller, Michel Sintzoff**

### **Angaben zur Veröffentlichung / Publication details:**

Glück, Roland, Bernhard Möller, and Michel Sintzoff. 2009. "A semiring approach to equivalences, bisimulations and control." Lecture Notes in Computer Science 5827: 134–49. [https://doi.org/10.1007/978-3-642-04639-1\\_10](https://doi.org/10.1007/978-3-642-04639-1_10).

### **Nutzungsbedingungen / Terms of use:**

**licgercopyright**

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under the following conditions:

**Deutsches Urheberrecht**

Weitere Informationen finden Sie unter: / For more information see:

<https://www.uni-augsburg.de/de/organisation/bibliothek/publizieren-zitieren-archivieren/publizieren>



# A Semiring Approach to Equivalences, Bisimulations and Control

Roland Glück<sup>1</sup>, Bernhard Möller<sup>1</sup> and Michel Sintzoff<sup>2</sup>

<sup>1</sup> Universität Augsburg

<sup>2</sup> Université catholique de Louvain

**Abstract.** Equivalences, partitions and (bi)simulations are usually tackled using concrete relations. There are only few treatments by abstract relation algebra or category theory. We give an approach based on the theory of semirings and quantales. This allows applying the results directly to structures such as path and tree algebras which is not as straightforward in the other approaches mentioned. Also, the amount of higher-order formulations used is low and only a one-sorted algebra is used. This makes the theory suitable for fully automated first-order proof systems. As a small application we show how to use the algebra to construct a simple control policy for infinite-state transition systems.

## 1 Introduction

Semirings have turned out to be useful for algebraic reasoning about relations and graphs, for example in [3]. Even edge-weighted graphs were successfully treated in this setting by means of fuzzy relations, as shown in [5] and [6]. Hence it is surprising that up to now no treatment of equivalence relations and bisimulations in this area has taken place, although a relational-algebraic approach was given in [11]. A recent, purely lattice-theoretic abstraction of bisimulations appears in [8]. The present paper was stimulated by [10], since the set-theoretic approach of that paper lends itself to a more compact treatment using modal semirings. This motivated the treatment of subsequent work by the third author by the same algebraic tools, as presented here. In Sect. 2 we consider partitions and equivalences. Sect. 3 explores equivalences in depth, while Sect. 4 is dedicated to bisimulations. As a short application in Sect. 5 a generic construction of a simple control policy is shown.

## 2 Semirings, Tests and Partitions

### 2.1 Idempotent Semirings and Tests

Semirings abstract the operations of choice and sequential composition.

**Definition 2.1** 1. An *idempotent semiring* is a structure  $S = (M, +, 0, \cdot, 1)$  such that  $0 \neq 1$ ,  $(M, +, 0)$  and  $(M, \cdot, 1)$  are monoids, choice  $+$  is commutative and idempotent, and composition  $\cdot$  distributes through  $+$  and is strict in both arguments.

2. The *natural order*  $\leq$  is given by  $x \leq y \Leftrightarrow_{df} x + y = y$ .
3. We call an element  $x \in N$  of a subset  $N \subseteq M$  *atomic in N* if  $x \neq 0$  and  $\forall y \in N : y \neq 0 \wedge y \leq x \Rightarrow y = x$ .
4. A subset  $N \subseteq M$  is *atomic* if every element  $x \in N$  is the supremum of the atoms of  $N$  below  $x$ .
5. A *quantale* is an idempotent semiring that is a complete lattice under the natural order and in which composition distributes over arbitrary suprema.

In an idempotent semiring the element 0 is +-irreducible, i.e.,  $x + y = 0 \Rightarrow x = 0 = y$ . Moreover, 0 is the least element w.r.t.  $\leq$ .

An example for a quantale is  $(\text{Rel}([0, 9]), \cup, \emptyset, ;, \text{id}_{[0, 9]})$ , where  $\text{Rel}([0, 9])$  denotes the set of all binary relations over the interval  $[0, 9] \subseteq \mathbb{R}$ ,  $\text{id}_X$  denotes the identity relation on  $X \subseteq [0, 9]$  and  $;$  denotes relational composition.

As a running example we will use a simple non-deterministic transition system the state of which is given by a single variable with values in  $[0, 9]$ . It is described by the following relation  $T$  between input states  $x$  and output states  $y$ :

$$xTy \Leftrightarrow_{df} (x \in [0, 2] \wedge y = x+4) \vee (x \in [4, 6] \wedge y = x+3) \vee (x \in [4, 6] \wedge y = x-4).$$

To model sets of states (or equivalently assertions about states) in the semiring setting one uses tests [7].

**Definition 2.2** The set  $\text{test}(S)$  of *tests* of an idempotent semiring  $S$  is the maximal Boolean subalgebra of the elements below 1. The complement of a test  $p$  w.r.t. 1 is denoted by  $\neg p$ ; it is the unique test  $q$  with  $p + q = 1$  and  $p \cdot q = 0$ . The set of atomic tests of  $S$ , i.e., of atoms in  $\text{test}(S)$ , is denoted by  $\text{atest}(S)$ .

The elements 1 and 0 are tests. Moreover, for tests  $p, q$  their composition  $p \cdot q$  coincides with their infimum. Hence  $p \leq q \Leftrightarrow p \cdot q = p$ . (1)

The tests in our running example are precisely the subrelations of the identity relation on  $[0, 9]$ , including the empty relation. They correspond in an obvious manner to subsets of  $[0, 9]$  and thus can be used to handle these without introducing a new sort. In this example the set  $\text{test}(S)$  is atomic and  $\text{atest}(S)$  is the set  $\{\{(x, x)\} \mid x \in [0, 9]\}$ .

For the remainder of this paper we assume  $\text{test}(S)$  to be atomic; an atomic test abstractly corresponds to a single state or graph node.

In the sequel we will often form sums of subsets of  $\text{test}(S)$ . For better readability we use the abbreviation  $\sum P =_{df} \sum_{p \in P} p$  for finite  $P \subseteq \text{test}(S)$ ; it coincides with the supremum of  $P$ . If the underlying semiring is a quantale we therefore denote by  $\sum P$  the supremum of an arbitrary  $P \subseteq \text{test}(S)$ .

By +-irreducibility of 0 we have

$$\sum P \neq 0 \Leftrightarrow \exists p \in P : p \neq 0 \tag{2}$$

## 2.2 Partitions

We now define the familiar concept of partition in terms of the tests of an idempotent semiring.

**Definition 2.3** A finite subset  $P \subseteq \text{test}(S)$  is called a *partition* if  $\sum P = 1$  and for all  $p, q \in P$  the equivalence  $p \cdot q = 0 \Leftrightarrow p \neq q$  holds.

Hence  $\{1\}$  is a partition, as is  $\text{atest}(S)$ , since  $\text{test}(S)$  is assumed to be atomic. Moreover, every element of a partition is a test different from 0. For a subset  $P' \subseteq P$  of a partition  $P$  we have  $\neg \sum P' = \sum(P - P')$ . Hence the complement  $\neg p$  of  $p \in P$  satisfies

$$\neg p = \sum(P - \{p\}) . \quad (3)$$

In our running example  $\{\text{id}_{[0,6]}, \text{id}_{]6,9]}\}$  and  $\{\text{id}_{[0,9] \cap \mathbb{Q}}, \text{id}_{[0,9] - \mathbb{Q}}\}$  are partitions.

**Definition 2.4** We say that partition  $Q$  *refines* partition  $P$ , in signs  $Q \leq_r P$ , if every element of  $P$  can be written as the sum of suitable elements of  $Q$ . When  $Q \leq_r P$  we say also that  $P$  is *coarser* than  $Q$ . Clearly,  $\leq_r$  is an order.

**Lemma 2.5** *Assume that partition  $Q$  refines partition  $P$ . Then for all  $q \in Q$  and  $p \in P$  we have  $q \cdot p \neq 0 \Rightarrow q \leq p$ .*

*Proof.* By assumption there is a subset  $Q' \subseteq Q$  with  $p = \sum Q'$ . By distributivity,  $q \cdot p = q \cdot \sum Q' = \sum_{q' \in Q'} q \cdot q'$ . By (2) there must be a  $q' \in Q'$  with  $q \cdot q' \neq 0$ . Since  $Q$  is a partition this implies  $q = q'$  and hence  $q \cdot q' = q$  and  $q \leq p$ .  $\square$

**Lemma 2.6** *A partition  $Q$  refines a partition  $P$  iff for all  $q \in Q$  there is a unique  $p \in P$  with  $p \cdot q \neq 0$ .*

*Proof.* ( $\Rightarrow$ ) For an arbitrary  $q \in Q$  we show first the existence of a  $p \in P$  with  $p \cdot q \neq 0$ . This is seen by  $q = 1 \cdot q = (\sum P) \cdot q = \sum_{p \in P} (p \cdot q)$ . Since  $q \neq 0$ , by (2) there must be a  $p \in P$  with  $p \cdot q \neq 0$ .

To show uniqueness we assume that there are two different  $p, p' \in P$  such that  $p \cdot q \neq 0$  and  $p' \cdot q \neq 0$  hold. By Lemma 2.5 this implies  $q \leq p$  and  $q \leq p'$ . Hence  $0 \neq q = q \cdot q \leq p \cdot p'$ , contradicting  $p \neq p'$ .

( $\Leftarrow$ ) Consider an arbitrary  $p \in P$  and set  $Q' = \{q \in Q \mid p \cdot q \neq 0\}$ . We claim  $p = \sum Q'$ . First,  $p = p \cdot \sum Q = p \cdot (\sum Q' + \sum(Q - Q')) = p \cdot \sum Q'$ . By (1) this is equivalent to  $p \leq \sum Q'$ .

The reverse inequality  $\sum Q' \leq p$  holds iff  $\forall q \in Q' : q \leq p$ . Suppose  $q \not\leq p$  for some  $q \in Q'$ . By (3) this is equivalent to  $0 \neq q \cdot \neg p = q \cdot \sum(P - \{p\}) = \sum_{p' \in P - \{p\}} q \cdot p'$ . By (2) there must be a  $p' \in P - \{p\}$  with  $q \cdot p' \neq 0$ . But this is a contradiction to  $q \cdot p \neq 0$  and the uniqueness assumption.  $\square$

**Lemma 2.7** *Let  $P$  and  $Q$  be partitions with  $Q \leq_r P$  and assume  $p \in P$  and  $p = \sum Q'$  for some  $Q' \subseteq Q$ . Then for all  $q \in Q$  we have  $p \cdot q \neq 0 \Leftrightarrow q \in Q'$ .*

*Proof.* ( $\Rightarrow$ ) Because of  $q \cdot p = q \cdot \sum_{q' \in Q'} q' = \sum_{q' \in Q'} (q \cdot q') \neq 0$  there has to be a  $q' \in Q'$  with  $q \cdot q' \neq 0$ . According to the definition of a partition this implies  $q = q'$  and hence  $q \in Q'$ .

( $\Leftarrow$ ) Let  $q \in Q'$ . Then  $q \leq p$  and therefore  $p \cdot q = q$ . The claim follows from  $q \neq 0$ , because  $q \neq 0$  holds for all  $q \in Q$ .  $\square$

We now focus on binary relations  $R$  which do not connect different sets in a given partition  $P$ : for all  $p \in P$  and for all  $x, y$  such that  $x R y$  we have  $x \in p \Leftrightarrow y \in p$ . For example,  $R$  may be an equivalence and  $P$  may be the set of its equivalence classes. This is captured by the following abstract definition.

**Definition 2.8** An element  $r \in M$  respects a partition  $P$  if  $r = \sum_{p \in P} p \cdot r \cdot p$ .

**Lemma 2.9** Let  $r \in M$  respect the partition  $P$  and let  $p, p' \in P$  such that  $p \neq p'$ . Then  $p \cdot r \cdot p' = 0$ .

*Proof.* Due to the definition of a partition we have for all  $p'' \in P$  that  $p \cdot p'' = 0$  or  $p' \cdot p'' = 0$ . Now, by respectance and distributivity,

$$p \cdot r \cdot p' = p \cdot (\sum_{p'' \in P} p'' \cdot r \cdot p'') \cdot p' = \sum_{p'' \in P} p \cdot p'' \cdot r \cdot p'' \cdot p' = \sum_{p'' \in P} 0 = 0. \quad \square$$

An easy consequence of this is the following.

**Corollary 2.10** Let  $r \in M$  respect the partition  $P$ . Then for all  $p \in P$  one has  $p \cdot r \cdot \neg p = 0 = \neg p \cdot r \cdot p$ .

*Proof.* By (3), respectance, distributivity and Lemma 2.9,

$$p \cdot r \cdot \neg p = p \cdot r \cdot \sum (P - \{p\}) = \sum_{p' \in P - \{p\}} p \cdot r \cdot p' = \sum_{p' \in P - \{p\}} 0 = 0. \quad \square$$

The above lemma is used to prove another important property.

**Theorem 2.11** Let partition  $Q$  refine partition  $P$ . If  $r \in M$  respects  $Q$  then it respects  $P$ , too.

*Proof.* For every  $p \in P$  we denote by  $Q_p \subseteq Q$  the unique subset of  $Q$  with  $\sum Q_p = p$ . Because of the partition properties  $\bigcup_{p \in P} Q_p = Q$  holds. Then by definition of  $Q_p$ , distributivity, splitting the sum, Lemma 2.9 and since  $\bigcup_{p \in P} Q_p = Q$  and  $r$  respects  $Q$ ,

$$\begin{aligned} \sum_{p \in P} p \cdot r \cdot p &= \sum_{p \in P} ((\sum Q_p) \cdot r \cdot (\sum Q_p)) = \sum_{p \in P} (\sum_{q, q' \in Q_p} (q \cdot r \cdot q')) \\ &= \sum_{p \in P} ((\sum_{q \in Q_p} q \cdot r \cdot q) + (\sum_{q, q' \in Q_p, q \neq q'} q \cdot r \cdot q')) \\ &= \sum_{p \in P} (\sum_{q \in Q_p} q \cdot r \cdot q) = \sum_{q \in Q} q \cdot r \cdot q = r \end{aligned} \quad \square$$

### 2.3 Modal Semirings and Symmetry

In the sequel the concept of symmetry will play an important role. To define it we use modal operators.

**Definition 2.12** A modal (idempotent) semiring  $(M, +, 0, \cdot, 1, |\cdot|, \langle \cdot |)$  consists of an idempotent semiring  $S = (M, +, 0, \cdot, 1)$  and the forward and backward diamond operators  $|\cdot|, \langle \cdot | : M \rightarrow (\text{test}(S) \rightarrow \text{test}(S))$ , characterised by the following axioms (e.g. [4]): for all  $x, y \in M$  and  $p, q \in \text{test}(S)$ ,

$$|x\rangle q \leq \neg p \Leftrightarrow p \cdot x \cdot q \leq 0 \Leftrightarrow \langle x|p \leq \neg q, \quad (4)$$

$$|x\rangle(|y\rangle q) = |x \cdot y\rangle q \quad \langle x|(\langle y|q) = |y \cdot x\rangle q \quad (5)$$

By these definitions,  $\langle x|q$  and  $|x\rangle q$  abstractly describe the image and the inverse image of  $q$  under  $x$ , resp. From (4) we obtain, for all  $p, q \in \text{test}(S)$ ,

$$|p\rangle q = p \cdot q = \langle p|q . \quad (6)$$

The operators enjoy many further properties, e.g., strictness  $|x\rangle 0 = 0 = \langle x|0$  and additivity  $|x + y\rangle q = |x\rangle q + |y\rangle q$  and  $|x\rangle (q + r) = |x\rangle q + |x\rangle r$ . This also entails that they are isotone in both arguments.

In our example we have  $|T\rangle \text{id}_{[7,8]} = \text{id}_{[4,5]}$  and  $\langle T| \text{id}_{[5,6]} = \text{id}_{[1,2]} \cup \text{id}_{[8,9]}$ .

Corresponding box operators can be defined as standard de Morgan duals of the diamonds, but we do not need them for the present paper. For details see again [4].

As mentioned above, the diamonds distribute through  $+$  in both arguments; in a quantale they even distribute through arbitrary sums. Moreover, by shunting we obtain from (4) that  $p \cdot |x\rangle q \leq 0 \Leftrightarrow p \cdot x \cdot q \leq 0 \Leftrightarrow q \cdot \langle x|p \leq 0$ . Therefore, for atomic  $p$ ,

$$p \cdot x \cdot q \neq 0 \Leftrightarrow p \leq |x\rangle q . \quad (7)$$

A symmetric property holds for  $\langle \cdot |$ .

Frequently, reasoning can be made more compact by lifting the order on  $\text{test}(S)$  pointwise to functions  $f, g : \text{test}(S) \rightarrow \text{test}(S)$  by setting

$$f \leq g \Leftrightarrow_{df} \forall p \in \text{test}(S) : f(p) \leq g(p)$$

E.g.,  $\langle x| \leq \langle y|$  abbreviates  $\forall p \in \text{test}(S) : \langle x|p \leq \langle y|p$ . An analogous convention applies to the equality of such functions.

In relation algebra, symmetry of a relation  $R$  is expressed as  $R^\smile \subseteq R$  or, equivalently, as  $R^\smile = R$ , where  $R^\smile$  is the converse of  $R$ . Since in semirings there is no converse operation, we have to find express symmetry differently.

Assuming temporarily an abstract converse  $x^\smile$  of an element  $x$  we would certainly expect  $p \cdot x^\smile \cdot q = 0 \Leftrightarrow q \cdot x \cdot p = 0$  for all  $p, q \in \text{test}(S)$ . By Axiom (4) this means  $|x^\smile\rangle = \langle x|$  and  $\langle x^\smile| = |x\rangle$ . Therefore if we consider just the behaviour of an element w.r.t. tests we can avoid the converse by passing to the respective mirror diamond. This motivates the following.

**Definition 2.13** An element  $x$  of a modal semiring is *symmetric* if  $\langle x| = |x\rangle$ .

It is straightforward to check that the set of symmetric elements is closed under  $+$ . In a quantale it is even closed under arbitrary sums.

Our example relation is not symmetric: We have  $|T\rangle\{(5, 5)\} = \{(1, 1)\}$ , but  $\langle T|\{(5, 5)\} = \{(1, 1), (8, 8)\}$ . If we restrict it to the relation  $T' = T;(\text{id}_{[0,2]} \cup \text{id}_{[4,6]})$  we obtain a symmetric relation, as is easily verified.

It turns out that in a special class of semirings this notion has interesting equivalent characterisations.

**Definition 2.14** Assume a modal semiring  $S$  with a greatest element  $\top$ . Then  $S$  satisfies the *Tarski rule* if  $x \neq 0 \Leftrightarrow \top \cdot x \cdot \top = \top$ .

The Tarski rule holds, for instance, in the modal semiring of binary relations. Since  $0$  is an annihilator for  $\cdot$ , this rule is equivalent to

$$\top \cdot x \cdot \top = \top \cdot y \cdot \top \Leftrightarrow (x = 0 \Leftrightarrow y = 0) \Leftrightarrow (x \leq 0 \Leftrightarrow y \leq 0). \quad (8)$$

A useful consequence of the Tarski rule is

$$\top \cdot x \cdot \top \cdot y \cdot \top = 0 \Leftrightarrow (x \leq 0 \vee y \leq 0) \quad (9)$$

which, in turn, implies  $\top \cdot x \cdot \top \cdot y \cdot \top = 0 \Leftrightarrow \top \cdot y \cdot \top \cdot x \cdot \top = 0$  and hence

$$\top \cdot x \cdot \top \cdot y \cdot \top = \top \cdot y \cdot \top \cdot x \cdot \top. \quad (10)$$

For the remainder of this section we assume that the Tarski rule holds.

**Lemma 2.15** *The following statements for an element  $x$  are equivalent:*

1.  $\forall p, q \in \text{test}(S) : \top \cdot p \cdot x \cdot q \cdot \top = \top \cdot q \cdot x \cdot p \cdot \top.$
2.  $\forall p, q \in \text{test}(S) : p \cdot x \cdot q \leq 0 \Leftrightarrow q \cdot x \cdot p \leq 0.$
3.  $x$  is symmetric.

*Proof.* The equivalence of Parts 1 and 2 is just a special case of (8). Therefore it suffices to show the equivalence of Parts 2 and 3. For an arbitrary  $x \in M$  we argue as follows:

$$\begin{aligned} & \forall p, q \in \text{test}(S) : p \cdot x \cdot q \leq 0 \Leftrightarrow q \cdot x \cdot p \leq 0 \\ \Leftrightarrow & \quad \{ \text{by (4)} \} \\ & \forall p, q \in \text{test}(S) : |x\rangle q \leq \neg p \Leftrightarrow \langle x|q \leq \neg p \\ \Leftrightarrow & \quad \{ \text{substitution } p \mapsto \neg p, \text{ bijectivity of negation} \} \\ & \forall p, q \in \text{test}(S) : |x\rangle q \leq p \Leftrightarrow \langle x|q \leq p \\ \Leftrightarrow & \quad \{ \text{indirect equality} \} \\ & \forall q \in \text{test}(S) : |x\rangle q = \langle x|q \end{aligned}$$

□

An immediate consequence of this lemma is the following:

**Lemma 2.16** *If  $s$  is symmetric and  $p \in \text{test}(S)$  then  $p \cdot s \cdot p$  is symmetric, too.*

*Proof.* For arbitrary  $q, q' \in \text{test}(S)$  we have, by associativity of multiplication, its commutativity on tests and symmetry of  $s$ ,

$$\begin{aligned} \top \cdot q \cdot (p \cdot s \cdot p) \cdot q' \cdot \top &= \top \cdot (q \cdot p) \cdot s \cdot (p \cdot q') \cdot \top = \top \cdot (p \cdot q') \cdot s \cdot (p \cdot q) \cdot \top \\ &= \top \cdot (q' \cdot p) \cdot s \cdot (p \cdot q) \cdot \top = \top \cdot q' \cdot (p \cdot s \cdot p) \cdot q \cdot \top \quad \square \end{aligned}$$

This implies

**Corollary 2.17** *For all  $p \in \text{test}(S)$  the product  $p \cdot \top \cdot p$  is symmetric; in particular,  $\top$  is symmetric.*

*Proof.* Symmetry of  $\top$  is immediate from (10) and Lemma 2.15. Then symmetry of  $p \cdot \top \cdot p$  is a consequence of Lemma 2.16. □

Finally we show a consequence of the Tarski rule for diamonds.

**Lemma 2.18**

1.  $|\top\rangle 1 = 1 = \langle \top|1$ .
2. If  $p \neq 0$  then  $|\top\rangle p = 1 = \langle \top|p$ .

*Proof.*

1. This follows already without the Tarski rule by setting  $p = q = 1$  in (6) and using isotony of the diamonds in their first argument.
2. We only show the property for the forward diamond. We have, using (6), Part 1, (5), the Tarski rule and Part 1 again,

$$|\top\rangle p = |\top\rangle |p\rangle 1 = |\top\rangle |p\rangle |\top\rangle 1 = |\top \cdot p \cdot \top\rangle 1 = |\top\rangle 1 = 1. \quad \square$$

### 3 Equivalences

#### 3.1 Equivalences and Fixpoints

**Definition 3.1** An element  $x \in M$  is called *reflexive* if  $1 \leq x$  and *transitive* if  $x \cdot x \leq x$ . A reflexive and transitive element is called a *preorder* and a symmetric preorder is an *equivalence*.

More liberally, one could define  $x$  to be reflexive and transitive if  $|1\rangle \leq |x\rangle$  and  $\langle x\rangle |x\rangle \leq \langle x\rangle$ , resp. These conditions are equivalent to  $\langle 1| \leq \langle x|$  and  $\langle x|\langle x| \leq \langle x|$ . As an example of the difference to the above formulation, consider the modal semiring of sets of paths in a graph under path concatenation. The element 1 there is the set of all single-node paths. The condition  $1 \leq x$  hence means that the set  $x$  of paths includes all these paths, whereas  $|1\rangle p \leq |x\rangle p$  means that  $x$  must for every node from  $p$  contain a path from that node to some node in  $p$ , but not necessarily a single-node one. However, for the current treatment we found it more convenient to omit the diamonds.

For an equivalence  $x$  and an atomic test  $p$  the test  $|x\rangle p$  (which by symmetry of  $x$  coincides with  $\langle x|p$ ) will play the role of the equivalence class of  $p$  under  $x$ . If  $p$  is a general test then  $|x\rangle p = \langle x|p$  will correspond to the union of the equivalence classes of the elements in  $p$ . This will be made precise later.

**Lemma 3.2** *Let  $x$  be a preorder.*

1.  $|x\rangle$  is a closure operator.
2. If  $p$  is a test then  $|x\rangle p$  is a fixed point of  $|x\rangle$  and  $\langle x|p$  is a fixed point of  $\langle x|$ .
3. The sets of fixed points of  $|x\rangle$  and  $\langle x|$  each are closed under composition  $\cdot$ .

*Proof.*

1. We have to show isotony, extensivity and idempotence. Isotony holds for all diamonds. Extensivity follows from  $1 \leq x$  and isotony. For idempotence we have, by transitivity of  $x$  and isotony of  $|\cdot\rangle$ ,  $|1\rangle = id$  and (5), reflexivity of  $x$  and isotony of  $|\cdot\rangle$  again, that  $|x\rangle |x\rangle = |x \cdot x\rangle \leq |x\rangle = |x\rangle |1\rangle \leq |x\rangle |x\rangle$ .

2. First,  $|x\rangle(|x\rangle p) = |x \cdot x\rangle p \leq |x\rangle p$  by (5), transitivity of  $x$  and isotony of diamonds. Second,  $|x\rangle p = |1\rangle(|x\rangle p) \leq |x\rangle(|x\rangle p)$  by (6), reflexivity of  $x$  and isotony of diamonds. The statement about  $\langle x|p$  is proved symmetrically.
3. The claim follows from the two previous claims as shown in more general context in [2].  $\square$

If  $x$  is an equivalence the above lemma means that unions of equivalence classes of  $x$  are saturated w.r.t.  $x$ .

**Lemma 3.3** *Let  $r$  be an equivalence and  $p$  a fixed point of the function  $\langle r|$ . Then  $\neg p$  is a fixed point of  $\langle r|$ , too. (For a similar result see [9], p. 33.)*

*Proof.* Reflexivity of  $r$  yields  $\langle r|\neg p \geq \neg p$ . The reverse inequation follows using (4) twice, symmetry of  $r$  and that  $\langle r|p = p$  by assumption:

$$\langle r|\neg p \leq \neg p \Leftrightarrow \neg p \cdot r \cdot p \leq 0 \Leftrightarrow |r\rangle p \leq p \Leftrightarrow \langle r|p \leq p \Leftrightarrow \text{true} . \quad \square$$

### 3.2 Equivalences and Partitions

**Lemma 3.4** *Let  $r$  be an equivalence. Assume that the set  $F$  of all fixed points of  $\langle r|$  is atomic and let  $A \subseteq F$  be the set of all its atoms. Then  $A$  is a partition.*

*Proof.* First we show that  $\sum A = 1$ . Assume  $\sum A < 1$ . Then by Lemma 3.3  $\neg \sum A$  is also a fixed point of  $f$  and it is different from 0. So there has to be an atomic fixed point below  $\neg \sum A$ , which leads to a contradiction.

For disjointness of the elements of  $A$  we consider arbitrary  $p, q \in A$  with  $p \neq q$ . By Lemma 3.2,  $p \cdot q$  is again a fixed point below  $p$  and  $q$ . Since  $p$  and  $q$  are assumed to be two different atomic fixed points of  $f$ , this implies  $p \cdot q = 0$ .  $\square$

**Definition 3.5** For an equivalence  $r$  we call the set of the atomic fixed points of the function  $\langle r|$ , denoted by  $Pa(r)$ , the *equivalence classes of  $r$* .

**Lemma 3.6** *Assume the Tarski rule and let  $P$  be a partition. Then  $Eq(P) =_{df} \sum_{p \in P} p \cdot \top \cdot p$  is an equivalence. It is called the equivalence induced by  $P$ .*

*Proof.* For transitivity we have, using distributivity, that  $p \cdot p' = 0 \Leftrightarrow p \neq p'$  for  $p, p' \in P$ , idempotence of multiplication on tests and associativity as well as  $p \in P \Rightarrow p \neq 0$  and the Tarski rule,

$$\begin{aligned} \sum_{p \in P} p \cdot \top \cdot p \cdot (\sum_{p \in P} p \cdot \top \cdot p) &= \sum_{p, p' \in P} p \cdot \top \cdot p \cdot p' \cdot \top \cdot p' \\ &= \sum_{p \in P} p \cdot \top \cdot p \cdot p \cdot \top \cdot p = \sum_{p \in P} p \cdot (\top \cdot p \cdot \top) \cdot p = \sum_{p \in P} p \cdot \top \cdot p . \end{aligned}$$

Reflexivity can be shown, using  $\top \geq 1$ , idempotence of multiplication on tests and the definition of a partition, by

$$\sum_{p \in P} p \cdot \top \cdot p \geq \sum_{p \in P} p \cdot 1 \cdot p = \sum_{p \in P} p = 1 .$$

Symmetry of  $\sum_{p \in P} p \cdot \top \cdot p$  follows easily from the distributivity of  $|\cdot\rangle$  and  $\langle \cdot|$  over summation and the symmetry of  $p \cdot \top \cdot p$  for all  $p \in P$  (cf. Corollary 2.17).  $\square$

**Lemma 3.7** For an equivalence  $r$  and  $p, q \in Pa(r)$  we have  $p \cdot r \cdot q = 0 \Leftrightarrow p \neq q$ .

*Proof.* Because of (4) the claim  $p \cdot r \cdot q = 0$  is equivalent to  $\langle r | p \leq \neg q$ . Due to the fixed point property of  $p$  this is equivalent to  $p \leq \neg q$ . By shunting we obtain the equivalent statement  $p \cdot q = 0$ . From Lemma 3.4 we know that  $Pa(r)$  is a partition, which gives us the equivalence to  $p \neq q$ .  $\square$

**Lemma 3.8** An equivalence  $r \in M$  respects the partition  $Pa(r)$  induced by itself.

*Proof.* We have, by  $Pa(r)$  being a partition, distributivity, splitting the sum and Lemma 3.7,

$$\begin{aligned} r &= \left( \sum Pa(r) \right) \cdot r \cdot \left( \sum Pa(r) \right) = \sum_{p, p' \in Pa(r)} p \cdot r \cdot p' \\ &= \left( \sum_{p \in Pa(r)} p \cdot r \cdot p \right) + \left( \sum_{p, p' \in Pa(r), p \neq p'} p \cdot r \cdot p' \right) = \sum_{p \in Pa(r)} p \cdot r \cdot p \quad \square \end{aligned}$$

**Lemma 3.9** For a partition  $P$  and arbitrary test  $q$  we have

$$|Eq(P)\rangle q = \sum_{p \in P \wedge p \cdot q \neq 0} p \cdot$$

*Proof.* Using the definition of  $Eq$ , additivity of the diamond, (5), (6), strictness of the diamonds, Lemma 2.18.2 and (6) again we calculate

$$\begin{aligned} |Eq(P)\rangle q &= \left| \sum_{p \in P} p \cdot \top \cdot p \right\rangle q = \sum_{p \in P} |p \cdot \top \cdot p\rangle q = \sum_{p \in P} |p\rangle | \top \rangle | p \rangle q \\ &= \sum_{p \in P} |p\rangle | \top \rangle (p \cdot q) = \sum_{p \in P \wedge p \cdot q \neq 0} |p\rangle | \top \rangle (p \cdot q) \\ &= \sum_{p \in P \wedge p \cdot q \neq 0} |p\rangle 1 = \sum_{p \in P \wedge p \cdot q \neq 0} p \cdot \quad \square \end{aligned}$$

Now we can show the connection between the operations  $Eq$  and  $Pa$ .

**Theorem 3.10**

1. For an equivalence  $r$  we have  $r \leq Eq(Pa(r))$ .
2. For a partition  $P$  we even obtain  $P = Pa(Eq(P))$ .

In particular,  $Pa$  and  $Eq$  form a Galois connection.

*Proof.*

1. By Lemma 3.8 and isotony we have

$$r = \sum_{p \in Pa(r)} p \cdot r \cdot p \leq \sum_{p \in Pa(r)} p \cdot \top \cdot p = Eq(Pa(r)) \cdot$$

2. First, by Lemma 3.9 and since  $P$  is a partition, every  $p \in P$  is a fixpoint of  $|Eq(P)\rangle$ . Second, we show that the elements of  $P$  are atomic fixpoints of  $|Eq(P)\rangle$ . To this end we consider some  $p \in P$  and some  $q \neq 0$  with  $q < p$ . Then, again by Lemma 3.9, we have  $|Eq(P)\rangle q = p \neq q$ , i.e.,  $q$  is not a fixpoint of  $|Eq(P)\rangle$ . Finally we show that every atomic fixpoint of  $|Eq(P)\rangle$  is an element of  $P$ . Let  $q$  be a fixpoint of  $|Eq(P)\rangle$ . Then by Lemma 3.9

$$q = |Eq(P)\rangle q = \sum_{p \in P \wedge p \cdot q \neq 0} p \cdot$$

This holds, in particular, for atomic fixpoints of  $|Eq(P)\rangle$ . But since atoms are sum-irreducible, the respective sums have to be singleton sums, i.e., the atomic fixpoints all coincide with elements of  $P$ .

The Galois property follows from these two properties via isotony.  $\square$

In the relational semiring Part 1 of this theorem strengthens to an equality. In general, however, it does not. Consider a graph with a single node  $x$  only and a looping arc on  $x$ . In the associated path semiring we have  $1 = \{x\}$  is an equivalence and  $P =_{df} \{1\}$  is the only partition possible. Then  $Eq(Pa(1)) = \top \neq 1$ , since  $\top$  is the set of all finite constant paths  $xxx \dots$ .

### 3.3 Atomic Tests and Equivalence Classes

Next we want to investigate the relationship between atomic tests and equivalence classes. We will see that atomic tests in a certain sense are generators of equivalence classes.

The following lemma states that two elements in the same equivalence class of  $r$  are connected to each other, whereas two elements in different equivalence classes are not connected under  $r$ .

**Lemma 3.11** *Let  $r$  be an equivalence and  $p, q$  be atomic tests. Then*

$$p \cdot r \cdot q \neq 0 \Leftrightarrow |r\rangle p = |r\rangle q$$

*Proof.* ( $\Rightarrow$ ) By atomicity of  $p$  and (7), isotony and transitivity of  $r$ ,

$$p \leq |r\rangle q \Rightarrow |r\rangle p \leq |r\rangle |r\rangle q \Rightarrow |r\rangle p \leq |r\rangle q .$$

Symmetrically we obtain  $\langle r|q \leq \langle r|p$ , which by symmetry of  $r$  is equivalent to  $|r\rangle q \leq |r\rangle p$ . Now the claim follows by antisymmetry of  $\leq$ .

( $\Leftarrow$ ) By reflexivity of  $r$  we have  $p \leq |r\rangle p = |r\rangle q$  and hence  $p \cdot r \cdot q$  by (7) and atomicity of  $p$ .  $\square$

This yields an important relationship between equivalences and partitions:

**Theorem 3.12** *Equivalence  $r \in M$  respects partition  $P$  iff  $Pa(r)$  refines  $P$ .*

*Proof.* ( $\Rightarrow$ ) For the sake of contradiction we assume that  $Pa(r)$  does not refine  $P$ . According to Lemma 2.6 there are  $p \in Pa(r)$  and distinct elements  $q, q' \in P$  with  $p \cdot q \neq 0$  and  $p \cdot q' \neq 0$ . We consider now two atomic tests  $at_1$  and  $at_2$  with  $at_1 \leq p \cdot q$  and  $at_2 \leq p \cdot q'$ . Because the equivalence classes of  $at_1$  and  $at_2$  under  $r$  coincide (both are  $p$ ) we can apply Lemma 3.11 and obtain  $at_1 \cdot r \cdot at_2 \neq 0$ . Isotony yields  $q \cdot r \cdot q' \neq 0$ . But then  $r$  cannot respect  $P$  because of Lemma 2.9. ( $\Leftarrow$ ) Lemma 3.8 states that  $r$  respects  $Pa(r)$ . According to Theorem 2.11  $r$  respects  $P$ , too.  $\square$

Now we are ready to prove the main result of this section:

**Theorem 3.13** *Let  $r$  be an equivalence and  $p$  an atomic test. Then  $|r\rangle p$  is an atom in the set of fixed points of  $|r\rangle$ . It is called the equivalence class of  $p$  under  $r$  and is denoted by  $[p]_r$ .*

*Proof.* Suppose  $0 \neq |r\rangle q \leq |r\rangle p$  for some test  $q$ . By strictness of  $|r\rangle$  we must have  $q \neq 0$  and hence, by atomicity of  $\text{test}(S)$ , there is a nonempty set  $Q' \subseteq \text{atest}(S)$  with  $q = \sum Q'$ . The assumption  $|r\rangle q \leq |r\rangle p$  is, by distributivity of  $|r\rangle$ , equivalent to  $\forall q' \in Q' : |r\rangle q' \leq |r\rangle p$ . Reflexivity of  $r$  implies  $\forall q' \in Q' : q' \leq |r\rangle p$ . By (7) we get  $\forall q' \in Q' : q' \cdot r \cdot p \neq 0$  and hence by lemma 3.11  $\forall q' \in Q' : |r\rangle q' = |r\rangle p$ . But then also  $|r\rangle q = \sum_{q' \in Q'} |r\rangle q' = |r\rangle p$  and we are done.  $\square$

## 4 Bisimulations

A simulation for a relation  $\rightarrow \subseteq X \times X$  (such as a transition relation) in the usual sense is a relation  $R \subseteq X \times X$  such that

$$x R x' \wedge x \rightarrow y \Rightarrow \exists y' : y R y' \wedge x' \rightarrow y' .$$

In relation algebra this is written more compactly as  $R \smile ; \rightarrow \subseteq \rightarrow ; R \smile$ , where  $;$  denotes relational composition.

A bisimulation for  $\rightarrow$  is a simulation the converse of which is again a simulation for  $\rightarrow$ . Translated into relation algebra this becomes

$$R ; \rightarrow \subseteq \rightarrow ; R \wedge R \smile ; \rightarrow \subseteq \rightarrow ; R \smile .$$

Using the same method as in Sect. 2.3 we can give the following converse-free definition, where  $b$  replaces  $R$  and  $g$  replaces  $\rightarrow$ :

**Definition 4.1** An element  $b \in M$  is called a *bisimulation* for  $g \in M$  iff

$$|b\rangle|g\rangle \leq |g\rangle|b\rangle \wedge \langle b||g\rangle \leq \langle g||b\rangle .$$

For an element  $g \in M$  the set of all bisimulations for  $g$  is denoted by  $\text{bisim}_g$ . Note that  $0 \in \text{bisim}_g$ .

**Lemma 4.2** For all  $g \in M$  the set  $\text{bisim}_g$  is closed under sum and product. If the underlying modal semiring is a quantale then it is closed under arbitrary sums.

*Proof.* The closedness under sum follows easily from the distributivity properties of the diamonds. Closedness under product follows from Axiom (5).  $\square$

For our further purposes it turns out that it is sufficient to require only the existence of a pseudoconverse.

**Definition 4.3** We call  $y \in M$  a *pseudoconverse* of  $x \in M$  iff  $|x\rangle = \langle y|$ ; in this case we write  $\text{pscon}(x, y)$ .

Note that a symmetric element is a pseudoconverse of itself. We now require for all  $x \in M$  the existence of a (not necessarily unique) pseudoconverse  $y$ .

**Lemma 4.4** Let  $x, y \in M$  such that  $\text{pscon}(x, y)$ . Then also  $\text{pscon}(y, x)$ .

*Proof.* We only show the inequality  $\langle x | \leq |y\rangle$ ; the reverse inequality is shown analogously. We have, by (4) twice, the assumption  $|x\rangle \leq |y\rangle$ , (4) twice and reflexivity of  $\leq$ ,

$$\begin{aligned} \langle x | p \leq |y\rangle p &\Leftrightarrow p \cdot x \cdot (\neg |y\rangle p) \leq 0 \Leftrightarrow |x\rangle (\neg |y\rangle p) \leq \neg p \Leftarrow \langle y | (\neg |y\rangle p) \leq \neg p \\ &\Leftrightarrow \langle y | (\neg |y\rangle p) \cdot y \cdot p \leq 0 \Leftrightarrow |y\rangle p \leq |y\rangle p \Leftrightarrow \text{true} . \quad \square \end{aligned}$$

**Lemma 4.5** *The sum of an element  $x \in M$  and an arbitrary pseudoconverse  $y \in M$  of  $x$  is symmetric.*

*Proof.* Let  $x, y \in M$  be arbitrary with  $\text{pscon}(x, y)$  and let  $p \in \text{test}(S)$  be an arbitrary test. Then we calculate, using distributivity of  $\langle \cdot |$  over  $+$ ,  $\text{pscon}(x, y)$  and Lemma 4.4, distributivity of  $\langle \cdot |$  over  $+$  and commutativity of  $+$ ,

$$\langle x + y | p = \langle x | p + \langle y | p = |y\rangle p + |x\rangle p = |x + y\rangle p . \quad \square$$

**Lemma 4.6** *Let  $g \in M$  be arbitrary and  $x \in \text{bisim}_g$  and  $\text{pscon}(x, y)$ . Then  $y \in \text{bisim}_g$ .*

*Proof.* Immediate from the definition of bisimulation and pseudoconverse.  $\square$

By definition of  $\text{bisim}_g$  for an arbitrary  $g \in M$  it is obvious that in a quantale there is a coarsest bisimulation for  $g$ , namely  $\hat{g} =_{df} \sum_{b \in \text{bisim}_g} b$ . This element has another interesting property:

**Theorem 4.7** *For all  $g \in M$  the coarsest bisimulation  $\hat{g}$  for  $g$  is an equivalence.*

*Proof.* Reflexivity and transitivity follow quickly from Lemma 4.2. For symmetry we observe that for every element  $b \in \text{bisim}_g$  every pseudoconverse  $b'$  of  $b$  lies again in  $\text{bisim}_g$ . Due to commutativity, associativity and idempotence the equality  $\sum_{b \in \text{bisim}_g} b = \sum_{b \in \text{bisim}_g} (b + b')$  holds. This means that  $\hat{g}$  can be written as a sum of symmetric elements of  $M$  and hence is symmetric itself.  $\square$

The equivalence classes of  $\hat{g}$  have an important property wrt. to  $g$ : If from a nonempty part of an equivalence class  $p$  one can reach, via  $g$ , a second (or even the same) equivalence class  $q$  then it is possible to get from *every* nonempty part of  $p$  via  $g$  to  $q$ . This stability property is formally stated in the next theorem.

**Theorem 4.8 (Stability)** *Let  $g \in M$  be arbitrary and  $p, q \in \text{atest}(S)$  be atomic tests. If  $p \cdot g \cdot q \neq 0$  then for all  $p' \leq [p]_{\hat{g}}$  with  $p' \neq 0$  we have  $p' \cdot g \cdot [q]_{\hat{g}} \neq 0$ .*

*Proof.* Due to the atomicity of  $\text{test}(S)$  it suffices to show the claim for all atomic  $p'$ . Because  $\hat{g}$  is an equivalence (Theorem 4.7) we obtain  $p' \cdot \hat{g} \cdot p \neq 0$  from Lemma 3.11. Hence (7) shows  $p' \leq |\hat{g}\rangle p$ . Similarly, the assumption  $p \cdot g \cdot q \neq 0$  and atomicity of  $p$  yield by (7) that  $p \leq |g\rangle q$ . Now, by isotony and since  $\hat{g}$  is a symmetric bisimulation, we get

$$0 \neq p' \leq |\hat{g}\rangle p \leq |\hat{g}\rangle |g\rangle q \leq |g\rangle |\hat{g}\rangle q = |g\rangle \langle \hat{g} | q = |g\rangle [q]_{\hat{g}}$$

and hence, by (7),  $p' \cdot g \cdot [q]_{\hat{g}} \neq 0$  as required.  $\square$

By this result,  $\hat{g}$  determines the coarsest partition that is  $g$ -stable.

## 5 Generating Control Policies

We now sketch a generic method of control design and show how to handle it algebraically. As an illustration a simple control policy for our running example is generated.

### 5.1 Generic Control Synthesis Using Bisimulations

We are given a transition graph  $G = (V, R)$ , where  $V$  is the set of nodes and  $R$  is the transition relation, and a control objective  $C$  like cycle-freeness, transitivity or various liveness properties. As a further property we request that the desired control objective can be achieved by a suitable restriction of  $G$ . In other words, any controlled transition graph is a subgraph of the uncontrolled one. Most known algorithms generating control policies require that the transition graphs are finite. These algorithms are impracticable in the case of large-scale systems. In the case of infinite state spaces, algorithms have been developed only for a few particular control properties. We propose to construct control policies for large-scale systems by a generic method based on bisimulations; given a control objective, it is assumed that an algorithm  $A_{cp}$  generating control policies for that objective and finite systems is available. Relationships between bisimulation equivalence and logical equivalences (e.g. [1]) should help.

The idea is to reduce the huge given graph  $G = (V, R)$  to a small finite graph  $G_1 = (V_1, R_1)$ , called the (*bisimulation*) *quotient* of  $G$ . The nodes in  $V_1$  are the equivalence classes of the coarsest bisimulation for  $G$ , while the transitions in  $R_1$  are the corresponding set-level liftings of the transitions in  $R$ . The part  $V_1$  can be constructed by an algorithm  $A_{eq}$  (e.g. [1]). To this, hopefully finite, graph we apply algorithm  $A_{cp}$  and obtain a subgraph  $G'_1$  of  $G_1$  with the required control property. Then a subgraph  $G'$  of  $G$  is obtained by inverting the set-level liftings.

The **crucial assumption** is that the given graph  $G$  belongs to the class of graphs for which the number of equivalence classes of its coarsest bisimulation is finite. Then the generic synthesis algorithm looks as follows:

- Input** Transition Graph  $G = (V, R)$ , Control Objective  $C$ .
- Step 1** Use algorithm  $A_{eq}$  to construct the quotient graph  $G_1 = (V_1, R_1)$ , where  $V_1$  is the set of the equivalence classes of the coarsest bisimulation for  $G$  and  $R_1$  is the quotient of  $R$  w.r.t.  $V_1$ .
- Step 2** Use  $A_{cp}$  to construct the subgraph  $G'_1 = (V'_1, R'_1)$  of  $G_1$ . Hence  $G'_1$  satisfies  $C$ .
- Step 3** Generate the controlled graph  $G' = (V', R')$  by flattening  $V'_1$  into  $V'$  (i.e.,  $V'$  is the union of the sets in  $V'_1$ ) and  $R'_1$  into  $R'$  (by the corresponding flattening of the transition relation).
- Output** The Controlled Transition Graph  $G' = (V', R')$ , which satisfies  $C$ .

In each special case to which this generic algorithm is applied it remains to show that the generated graph  $G'$  satisfies the required control objective  $C$ . A generic proof of the correctness of Step 3 depends essentially on the formalisation of a significant family of control objectives.

The method elaborated in [10] for optimal control basically generates equivalence sets where states have an equal value. In fact, these sets are composed of equivalence classes of a coarsest bisimulation. So, that particular method is an instance of the proposed approach. In the present paper we illustrate the generic method of bisimulation-based control synthesis with a simple control objective.

## 5.2 Application to a Simple Control Objective

Now we will demonstrate the proof of the correctness of Step 3 for a simple control objective, namely a liveness property. We require that if a node has an ingoing edge it has to offer an outgoing one, too. A relational formulation could be the predicate  $\forall x, y : x R y \Rightarrow (\exists z : y R z)$ . In other words, if the pre-image of a node set is non-empty then its image has to be non-empty, too. This motivates the following definition in a general modal semiring  $S = (M, +, 0, \cdot, 1)$ :

**Definition 5.1** An element  $g \in M$  is called *live* iff for all  $p \in \text{test}(S)$  the implication  $|g\rangle p \neq 0 \Rightarrow \langle g|p \neq 0$  holds. For an element  $g \in M$  an element  $g' \in M$  is called a *live part* of  $g$  iff  $g'$  is live and  $g' \leq g$ .

Obviously 0 is live. Moreover, due to distributivity of the diamonds over sums the sum of arbitrary live elements is live, too. So for a  $g \in M$  there is a greatest live part, denoted by  $\text{glp}_g$ .

By atomicity of  $\text{test}(S)$ , distributivity of the diamonds over arbitrary sums and  $+$ -irreducibility of 0, an element  $g$  is live iff the implication  $|g\rangle p \neq 0 \Rightarrow \langle g|p \neq 0$  holds for all atomic tests  $p \in \text{atest}(S)$ .

As an important concept we introduce a so-called *marker*  $\delta_g(p, q)$  of an element  $g \in M$  and tests  $p, q \in \text{test}(S)$ . It can be understood as a sign whether  $g$  admits a transition from  $p$  to  $q$ . In this case it is a restriction of  $\top$ , otherwise it equals 0. The precise definition is as follows:

**Definition 5.2** For an element  $g \in M$  the *marker* function  $\delta_g(\cdot, \cdot) : \text{test}(S) \times \text{test}(S) \rightarrow M$  is defined by  $\delta_g(p, q) = p \cdot \top \cdot q$  if  $p \cdot g \cdot q \neq 0$ , and is 0 otherwise.

We will use this construction to express the above schematic algorithm in our algebraic setting. First we have to model the construction of the graph  $G_1$  from the above description. The nodes correspond to equivalence classes, so a first idea could be to set  $g_1 = \sum_{p, q \in Pa(\hat{g})} \delta_g(p, q)$ , where  $Pa(\hat{g})$  is the set of equivalence classes of the coarsest bisimulation for  $g$ . This models the property that  $G_1$  admits a transition from one node to another iff there is a transition in  $G$  between two elements of the equivalence classes corresponding to the nodes in  $G_1$ . However, it turns out to be more convenient to abstract from this construction by means of a system of representatives (analogously to the classical use) and to reduce this quotient to a quotient witness:

**Definition 5.3** A *system of representatives (SOR)* for an equivalence  $r$  is a set  $\text{Rep}$  of atomic tests such that  $\sum_{p \in \text{Rep}} [p]_r = 1$  and  $p, q \in \text{Rep} \wedge p \neq q \Rightarrow [p]_r \cdot [q]_r = 0$ . For an element  $g \in M$  an element  $h \in M$  is called a *quotient*

witness of  $g$  if there is a SOR Rep of  $\hat{g}$  such that  $h = \sum_{p,q \in \text{Rep}} p \cdot \delta_g([p]_{\hat{g}}, [q]_{\hat{g}}) \cdot q$ . Rep is called the *associated* SOR of  $h$ , and the elements  $(p, q)$  from  $\text{Rep}^2$  with  $p \cdot h \cdot q \neq 0$  are called its *edges*, denoted by  $\text{edges}_h$ . The set of all quotient witnesses of  $g$  is denoted by  $\text{qw}(g)$ .

Let now  $h \in \text{qw}(g)$  be arbitrary. Assume we can determine the  $\text{glp}_h$ . Our goal now is to construct from  $\text{glp}_h$  the greatest live part  $\text{glp}_g$  of  $g$ . To this end we set  $g' = \sum_{(p,q) \in \text{edges}_{\text{glp}_h}} [p]_{\hat{g}} \cdot g \cdot [q]_{\hat{g}}$  ( $\text{edges}_{\text{glp}_h}$  is defined analogously to Definition 5.3) and obtain an element  $g' \in M$  with the desired property:

**Theorem 5.4** *Let  $g'$  be constructed as above. Then  $g' = \text{glp}_g$ .*

*Proof.* The property  $g' \leq g$  follows immediately from isotony of multiplication and  $p \leq 1$  for all  $p \in P$  for an arbitrary partition  $P$ . By atomicity of  $\text{test}(S)$ , distributivity of the diamonds over arbitrary sums and  $+$ -irreducibility of  $0$ , it suffices to show the second claim for all atomic tests. So let  $p$  be an arbitrary atomic test with  $|g'|p \neq 0$ . By  $q$  we denote the representative of  $[p]_{\hat{g}}$  in Rep. Due to the construction of  $g'$  there has to be a pair  $(q, q') \in \text{edges}_{\text{glp}_h}$  with  $q \cdot \text{glp}_h \cdot q' \neq 0$ . Because of  $\text{glp}_h \leq h$  and the construction of  $h$  the inequality  $q \cdot g \cdot q' \neq 0$  holds. According to Theorem 4.8 for every atomic test  $p'$  with  $p' \leq [q]_{\hat{g}}$  the inequality  $p' \cdot g \cdot [q']_{\hat{g}} \neq 0$  has to hold. Because  $p$  and  $p'$  are contained in the same equivalence class we have also  $p \cdot g \cdot [q']_{\hat{g}} \neq 0$ . But then by construction of  $g'$  also  $\langle g'|p \neq 0$  holds.

Hence  $g'$  is a live part of  $g$ . Assume now that  $g' < \text{glp}_g$ . Then we consider the element  $\tilde{h} = \sum_{p,q \in \text{Rep}} p \cdot \delta_{\text{glp}_g}([p]_{\hat{g}}, [q]_{\hat{g}}) \cdot q$ . Because of  $\text{glp}_g \leq g$  we have  $\tilde{h} \leq h$ . On the other hand, due to the construction of  $g'$  and  $g' < \text{glp}_g$  there has to be  $p, q \in \text{Rep}$  such that  $(p, q) \notin \text{edges}_{\text{glp}_h}$  and  $[p]_{\hat{g}} \cdot \text{glp}_g \cdot [q]_{\hat{g}} \neq 0$ . Consider now an arbitrary  $p \in \text{Rep}$  with  $|\tilde{h}\rangle p \neq 0$ . Then by construction  $|\text{glp}_g\rangle [p]_{\hat{g}} \neq 0$  and hence  $|\text{glp}_g\rangle [p]_{\hat{g}} \neq 0$ . But then we have also  $\langle \tilde{h}|p \neq 0$ . This means that  $\tilde{h}$  is live and  $\tilde{h} \leq \text{glp}_h$  does not hold, which is a clear contradiction.  $\square$

Let us now apply this construction to our running example. The coarsest bisimulation is here given by  $[0, 2]^2 \cup [4, 6]^2 \cup (]2, 4[ \cup ]6, 9])^2$ , and it has three equivalence classes, namely  $[0, 2]$ ,  $[4, 6]$  and  $]2, 4[ \cup ]6, 9]$ . As a quotient witness we can choose the relation  $\{(1, 4), (4, 8), (4, 1)\}$ . The greatest live part of this is  $\{(1, 4), (4, 1)\}$ . If we play this back to the original relation by means of the above construction we obtain the infinite relation  $\{(x, y) \in \mathbb{R}^2 \mid (x \in [0, 2] \wedge y = x + 4) \vee (x \in [4, 6] \wedge y = x - 4)\}$ , which is the greatest live part of the original relation according to Theorem 5.4.

Admittedly, the present algebraic modelling of system control is basic and primitive. The application of the generic method for other control objectives, e.g. optimality, may well require the use of labelled transition systems. For such cases, the algebraic framework needs to be refined.

## 6 Conclusion and Further Work

We have shown how equivalences, partitions and bisimulations can be conveniently described in the setting of modal semirings and quantales. With these tools we were also able to give a generic algorithm for constructing a simple policy for an infinite transition system.

Future work has several directions: First, we shall extend our methods to cover also labelled transition systems. Quantales for describing them are already known from the literature. The second focus will be to consider more significant goals than the simple liveness property given in Sect. 5.2. So we plan to tackle properties like acyclicity, termination or even (probabilistic) shortest path problems. A more general challenge would be to identify the subclass of control objectives for which the algorithm from Sect. 5.1 works correctly.

## References

1. C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008.
2. G. Birkhoff. *Lattice Theory*, volume XXV of *Colloquium Publications*. American Mathematical Society, 3rd edition, 1967.
3. B. Carré. *Graphs and Networks*. Oxford Univ. Press, 1979.
4. J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM Transactions on Computational Logic*, 7:798–833, 2006.
5. R. Glück and B. Möller. Circulations, fuzzy relations and semirings. In P. Audebaud and C. Paulin-Mohring, editors, *Mathematics of Program Construction — MPC 2008*, volume 5133 of *Lecture Notes in Computer Science*, pages 134–152. Springer, 2008.
6. Y. Kawahara. On the cardinality of relations. In R. Schmidt, editor, *Relations and Kleene Algebra in Computer Science (RelMiCS/AKA 06)*, volume 4136 of *Lecture Notes in Computer Science*, pages 251–265, 2006.
7. E. Manes and D. Benson. The inverse semigroup of a sum-ordered semiring. *Semigroup Forum*, 31:129–152, 1985.
8. D. Pous. Complete lattices and up-to techniques. In S. Zhong, editor, *Programming Languages and Systems, 5th Asian Symposium, APLAS 2007, Singapore, November 29-December 1, 2007*, volume 4807 of *Lecture Notes in Computer Science*, pages 351–366. Springer, 2007.
9. G. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists*. Springer, 1993.
10. M. Sintzoff. Synthesis of optimal control policies for some infinite-state transition systems. In P. Audebaud and C. Paulin-Mohring, editors, *Mathematics of Program Construction — MPC 2008*, volume 5133 of *Lecture Notes in Computer Science*, pages 336–359. Springer, 2008.
11. M. Winter. A relation-algebraic theory of bisimulations. *Fundam. Inf.*, 83(4):429–449, 2008.