Some Uses of Modal Semirings

Bernhard Möller[1(✉)] and Jules Desharnais[2(✉)]

[1] Universität Augsburg, Bavaria, Germany
bernhard.moeller@informatik.uni-augsburg.de
[2] Université Laval, Québec, Canada
jules.desharnais@ift.ulaval.ca

Abstract. We survey one branch of algebraic logic, namely modal semirings. They provide compact algebraic definitions of actions, with choice $+$ and sequential composition $\cdot$, together with modal operators box and diamond, parametrised by actions, that allow reasoning about successors and predecessors of states/worlds. Particular instances are homogeneous binary relations or sets of finite and infinite non-empty traces under fusing concatenation. As main examples of applications we present obstacle analysis for geographic wayfinders, Hoare Logic, O'Hearn's Incorrectness Logic, General Correctness Logic, as well as the temporal logic CTL* and its sublogics CTL and LTL. We also give glimpses at Epistemic Logics of belief and knowledge, pointer structures plus Separation Logic and preference database queries. Finally, we briefly discuss some related algebraic approaches.

1 Introduction

The aim of *algebraic logic* is to compact series of small steps of general logical inference into larger (in)equational steps. Another goal is to replace tedious model-theoretic argumentation, in particular, element-wise argumentation, by more abstract and compact reasoning.

We exemplify this using the algebraic structure of *modal semirings*. The theme is to algebraically generalise many pertinent computer science concepts within that one single framework. The approach is also suitable for off-the-shelf general theorem provers such as Prover9/Mace4 [25], Isabelle (e.g., [35]), etc.

Modal semirings provide compact algebraic definitions of actions, with choice $+$ and sequential composition $\cdot$, together with modal operators box and diamond, parametrised by actions, that allow reasoning about successors and predecessors of states/worlds. Particular instances are homogeneous binary relations or sets of finite and infinite non-empty traces under fusing concatenation.

The paper is intended as a survey; hence there are not many new results. The underlying theory and some essential references are found in the report [28]; the monograph [29] presents plenty of further material. Selected parts of that book have been checked/developed using the system Prover9/Mace4. This is an automated theorem prover coupled with a counterexample finder. It fully supports first-order predicate logic, in particular, propositional and equational logic.

2 Modal Operators

As a preparation for the abstract algebraic treatment, we introduce the modal operators in the concrete setting of binary relations.

2.1 Definitions

Assume a set Σ of states or possible worlds, more abstractly called *points*. We use the modal forward and backward diamond operators (e.g. [39]) that compute the inverse image $|R\rangle Q$ and the image $\langle R|P$ of sets $Q, P \subseteq \Sigma$ under some binary relation $R \subseteq \Sigma \times \Sigma$:

$$|R\rangle Q =_{df} \{x \,|\, \exists\, y \in Q : x\, R\, y\} \;, \quad \langle R|P =_{df} \{y \,|\, \exists\, x \in P : x\, R\, y\} \;. \tag{1}$$

Hence they are existential quantifiers about successor and predecessor points.

Let us explain the notation. In many modal logics one considers only one direction of transitions and then uses a notation like $\langle R\rangle$ for the diamond of R. However, we are interested in both directions and hence use the above asymmetric notations. Beware: the notations $|R\rangle$ and $\langle R|$ should not be confused with the analogous ones used in quantum theory.

Using the De Morgan duality $(\forall\, z : P(z)) \;\Leftrightarrow\; \neg(\exists\, z : \neg P(z))$ between existential and universal quantifiers, one defines corresponding box operators as

$$|R]Q =_{df} \overline{|R\rangle \overline{Q}} \;, \quad [R|P =_{df} \overline{\langle R|\, \overline{P}} \;,$$

where $\overline{X}$ is the complement of X. Therefore

$$|R]Q =_{df} \{x \,|\, \forall\, y : x\, R\, y \;\Rightarrow\; y \in Q\} \;, \quad [R|P =_{df} \{y \,|\, \forall\, x : x\, R\, y \;\Rightarrow\; x \in P\} \;.$$

Diamond and box can also mirror the deontic concepts of "may" and "must".

2.2 Application I: Space-Time Diagrams and Obstacle Analysis

As our first—and somewhat unorthodox—example of the use of modal operators we present an application from geo-informatics. This section is based on [27].

A *wayfinder* is an entity that moves through a space-time continuum with possible obstacles. Therefore one important task is to determine regions of space-time which the wayfinder may safely traverse without running the risk of getting stuck in front of an obstacle (obstacles are considered impenetrable). Besides obstacles, which must be avoided, one is also interested in space-time regions that must be reached; these are called *compulsions*.

In describing such phenomena we take up an approach by Hendricks et al. [15]. Central concepts there are modalities such as "may" and "must" when describing movement in space-time. Examples are

– "We *may* use a bus or a train."
– "We *must* reach the plane before it leaves."

– "We *must not* pass through road X because of construction work."

While the treatment in the original paper [15] is only semi-formal, we show how to model these notions relationally with box and diamond operators. One advantage of this treatment is that for a large part our results are independent of the number of spatial (or even temporal) dimensions and of metric considerations.

Points and Reachability. For the formalisation we assume, for simplicity, a set S of *spatial coordinates* taken from a vector space with a norm $\| \|$, such as $\mathbb{R}, \mathbb{R}^2$ or $\mathbb{R}^3$. Second, we assume a linearly ordered set T of *temporal coordinates*, for simplicity an interval of $\mathbb{R}$. With this, now a *point* is a pair $(s,t) \in S \times T$, and a *region* is a set of points.

We want to describe the possible movements of a wayfinder. Without any restrictions one could not predict where the wayfinder might be at a given time. Therefore one uses, for each period of time considered, an upper bound on the velocity and analyses how far away the wayfinder can get from its starting position staying below this speed bound during the whole period.

For a non-negative bound v the *reachability relation* R_v between points is

$$(s,t)\, R_v\, (s',t') \Leftrightarrow_{df} t \leq t' \wedge \|s' - s\| \leq v \cdot (t' - t)\ .$$

This means that (s',t') can be reached from starting point (s,t) by travelling for time $t' - t$ with maximal velocity v. Having v as a parameter allows modelling switches between varying velocities, e.g., shifting to a lower gear in a steeper region. Using the triangle inequality for the norm, it is straightforward to show that R_v is a partial order.

Reachability and Modalities. Now we want to characterise regions of spatio-temporal reachability. The diagrams to follow are similar to the light cones introduced by Minkowski within the Theory of Relativity [24]. In this section we

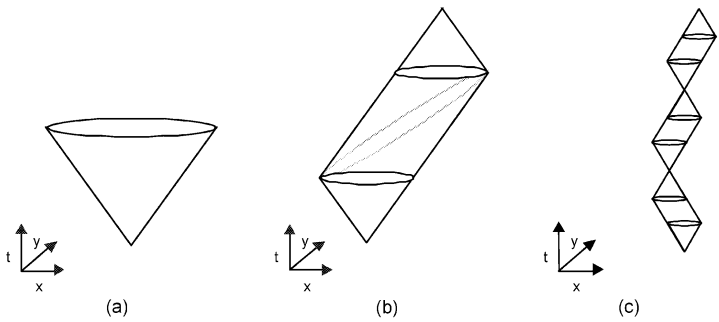
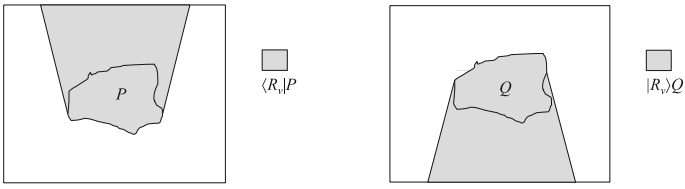


Fig. 1. Characteristic space-time diagrams

restrict ourselves to the case of two spatial dimensions to allow simple depictions. The illustrations in this section are taken from [15]; time progresses upwards. The cone in (a) models the case where the wayfinder starts at the space-time point at the tip of the cone. Since we study the points reachable under a certain maximal speed v, the further time progresses the farther the wayfinder can move away (in every spatial direction) from the spatial coordinate of its starting point. In (b) we find the situation where both a departure point and a destination point are given. The downward open cone at the top models the region from which the destination can be reached under maximal speed v; it is also known as a *past cone*. Dually, a cone such as the one in (a) is called a *future cone*. For a fixed speed limit and given start and end points, the possible region of travel for the wayfinder is the intersection of the (infinitely extended) future and past cones; it is called a *prism* [13,15]. Finally, in (c) there is a sequence of space-time points that the wayfinder has to meet; they are connected by prisms. Such a structure is called a *necklace*.

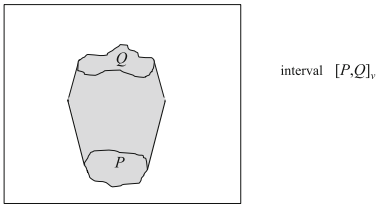
We now describe some of these constructions in terms of modal operators. To simplify notation we identify singleton sets with their only element. With this, the future and past cones for a starting point x, a target point y and maximal velocity v are given by $\langle R_v|x$ and $|R_v\rangle y$, resp. Therefore, the modal notation can serve as a "calculus of diagrams". As in (1) the notation can also be used for regions P, Q by forming $\langle R_v|P$ and $|R_v\rangle Q$:



The prism between x, y (cf. Part (b) in Fig. 1) is simply the *interval* $[x, y]_v =_{df} \langle R_v|x \cap |R_v\rangle y$ between x, y w.r.t. the partial order R_v, i.e.,

$$[x, y]_v = \{r \mid x\, R_v\, r \wedge r\, R_v\, y\} \ .$$

Note that by reflexivity of R_v we have $x, y \in [x, y]_v$ (and hence $[x, y]_v \neq \emptyset$) whenever $x\, R_v\, y$. For regions P, Q we set $[P, Q]_v =_{df} \langle R_v|P \cap |R_v\rangle Q$:



Compulsions and Barriers. Diamonds and boxes express possible and guaranteed reachability under some speed bound v, resp.:

$$\left.\begin{array}{l} - \; x \in |R_v\rangle Q \text{ iff under } v \text{ it is possible to reach from } x \text{ some point in } Q; \\ - \; y \in \langle R_v| P \text{ iff under } v \text{ it is possible to reach } y \text{ from some point in } P; \\ - \; x \in |R_v] Q \text{ iff under } v \text{ all points reachable from } x \text{ lie in } Q; \\ - \; y \in [R_v| P \text{ iff under } v \text{ all points from which } y \text{ is reachable lie in } P. \end{array}\right\} \quad (2)$$

With this we can model *compulsions* or *barriers*, i.e., regions that must be reached or avoided. In Fig. 2, again taken from [15], we restrict ourselves to one spatial dimension. Region M_1 consists of a single space-time point. M_2 is a spatially extended region which exists only for one single instant of time. M_3–M_5 are singleton regions in space which each exist for a certain interval of time. M_6 is a spatially extended region which exists only for an interval of time. Finally, M_7 and M_8 are regions that, during a time interval, move from one place in space to another. While M_7 at each time during the interval occupies a singleton region in space, the spatial extent of M_8 shrinks during its time interval.

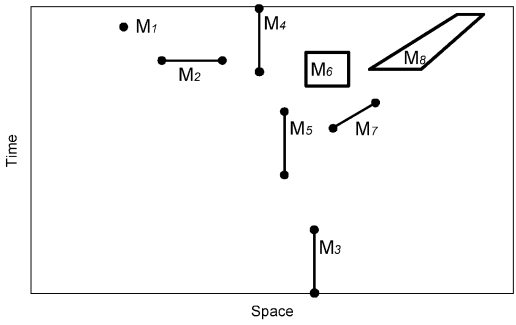


Fig. 2. Sample regions

By (2), the region from which the wayfinder can avoid a barrier B in the future direction is $|R_v]\,\overline{B}$. An analogous expression models this for the past direction. The region from which the wayfinder is guaranteed to reach compulsion C is $|R_v]C$.

Frequently, one will want barriers or compulsions to be "connected". For this one can use the notion of convexity: a region P is R_v-*convex* if for any two subsets $Q, Q' \subseteq P$ also all intermediate points belong to P, i.e., $[Q, Q']_v \subseteq P$. For transitive relation R and region B the sets $|R\rangle B$ and $\langle R|B$ are convex: with $Q, Q' \subseteq |R\rangle B$ we obtain, by set theory, $Q' \subseteq |R\rangle B$ plus isotony of diamond and transitivity of R,

$$[Q, Q'] = \langle R|Q \cap |R\rangle Q' \subseteq |R\rangle Q' \subseteq |R\rangle|R\rangle B \subseteq |R\rangle B \; .$$

The reasoning for $\langle R|B$ is symmetric. Next, by definition and set theory, convex sets are closed under intersection, and hence, in particular, intervals are convex.

Further Topics. The paper [27] continues this treatment by proving a number of properties of obstacles with a bounded avoidance region. The latter has a more elaborate definition than $|R_v]\,\overline{B}$ above. Therefore determining the avoidance region for a union of regions is non-trivial; it turns out that in case of a partial overlap this may be larger than just the union of the avoidance regions. Finally, that paper presents an abstract algebraic notion of coordinates, with which further boundedness assertions become possible.

3 Algebraic Abstraction

The relational treatment in the previous section already allows abstracting from the particular space/time structure in which the movements occur: all that matters is the reachability relation, which simply can be treated as a parameter of the whole approach. The only general requirement is that reachability be transitive.

However, we abstract even further by generalising the setting of concrete relations to the algebraic structure of *modal semirings*. This is a well established theory (see [7] for an overview) with many concrete instantiations, in particular relations. Using it makes our theory apply to a much larger class of models. Additionally it becomes amenable to (semi-)automatic proofs more easily (see [18] for a pioneering paper on this and [11] for a more recent survey).

3.1 IL-Semirings

An *idempotent left semiring* (briefly *IL-semiring*) is a structure $(S, +, \cdot, 0, 1)$ with the following properties.

1. The reduct $(S, +, 0)$ is a commutative monoid with idempotent $+$, while $(S, \cdot, 1)$ is a monoid.
2. The operator $\cdot$ right-distributes over $+$, i.e., $(a + b) \cdot c = a \cdot c + b \cdot c$, and is *left-strict*, i.e., $0 \cdot a = 0$, for all $a, b, c \in S$.
3. With the *natural order* $a \leq b \Leftrightarrow_{df} a + b = b$, abstracting inclusion/implication, $\cdot$ is right-isotone, i.e., $b \leq c \Rightarrow a \cdot b \leq a \cdot c$.

An IL-semiring is *left-distributive* when it also satisfies $a\cdot(b+c) = a\cdot b+a\cdot c$. An *I-semiring* is a left-distributive IL-semiring with *right-strict* $\cdot$, i.e., with $a\cdot 0 = 0$. An IL-Semiring is *Boolean* if its natural order induces a Boolean algebra.

Semiring elements abstractly represent actions, with $a+b$ and $a\cdot b$ representing choice between and sequential composition of actions a, b. The units 0 and 1 represent the empty and idle actions.

Further, the natural order $\leq$ abstractly represents inclusion and $+$ is the supremum operator of an upper semilattice with least element 0. This implies $a, b \leq a + b$.

We present some classical examples.

Example 3.1. Assume a set Σ of points and let Σ^* and Σ^ω be the set of all finite and infinite sequences of points, resp.

1. The structure $\mathsf{REL}(\Sigma) =_{df} (\mathcal{P}(\Sigma \times \Sigma), \cup, ;, \emptyset, \Delta_\Sigma)$, where ; is relation composition and Δ_Σ is the identity relation on Σ, is called the *relational semiring*.
2. The structure $\mathsf{LAN}(\Sigma) =_{df} (\mathcal{P}(\Sigma^*), \cup, ., \emptyset, \{\varepsilon\})$, where . is concatenation and ε is the empty sequence, is called the *language semiring* and is familiar from the algebra of regular languages.
3. The structure $\mathsf{PAT}(\Sigma) =_{df} (\mathcal{P}(\Sigma^+ \cup \Sigma^\omega), \cup, \cdot, \emptyset, \Sigma)$, where $\Sigma^+ =_{df} \Sigma^* - \{\varepsilon\}$ and $\cdot$ is fusing concatenation, is called the *path semiring*. It is instrumental for the semantics of temporal logics.

Of these, the first two are I-semirings, while the third is only an IL-semiring. All three are Boolean.

3.2 Tests

A *test* [8,21,22] in an IL-semiring S is a $p \in S$ with a *complement* $\neg p$ relative to 1, namely $p + \neg p = 1$ and $p \cdot \neg p = 0 = \neg p \cdot p$. Note that the symbol p is not a propositional variable; rather it stands for a predicate characterising a set of points. The complement $\neg p$ is unique when it exists. The set $\mathsf{test}(S)$ of all tests in S has least and greatest elements 0 and 1, with $\neg 0 = 1$ and $\neg 1 = 0$. They represent the everywhere false and the everywhere true predicate, resp. On tests the natural order abstractly represents implication.

Under suitable extra conditions $\mathsf{test}(S)$ forms a Boolean algebra, and $p \cdot q$ and $p + q$ represent conjunction and disjunction of tests p, q.

Example 3.2. In the relational semiring (cf. Ex. 3.1.1) the tests are the subrelations of the identity relation, which are in one-to-one correspondence with sets of points. In the path semiring (cf. Ex. 3.1.3) the element 1 is the set of all single-point traces; hence tests are sets of points.

For test p and action a we obtain input and output *restrictions* of a to p as

$$p \cdot a \quad \text{and} \quad a \cdot p \,. \tag{3}$$

Our approach differs from KAT (Kleene algebra with tests [21]) in that the algebra of tests cannot be freely chosen but always consists of the maximal complemented set of subidentities.

3.3 Modal Operators

For transition system a and test q, the *forward diamond* $|a\rangle q$ is a test characterising the points with at least one immediate a-successor in q. It abstractly represents the inverse image of q under a as defined in (1) of Sect. 2.1. *Forward*

box is the De Morgan dual of forward diamond, while the test $\ulcorner a$ represents the *domain*, i.e., the set of starting points of a. We axiomatise this by

$$\begin{array}{ll} |a\rangle q \leq p \;\Leftrightarrow\; a \cdot q \leq p \cdot a \;\; (\mathit{Prediamond}) \;, & |a \cdot b\rangle q = |a\rangle(|b\rangle q) \;\; (\mathit{Composition}) \;, \\ |a]q \;=_{df}\; \neg|a\rangle\neg q \;, & \ulcorner a \;=_{df}\; |a\rangle 1 \;. \end{array}$$

A purely equational axiomatisation is possible, too. The box $|a]q$ corresponds to Dijkstra's weakest liberal precondition $\mathsf{wlp}.a.q$. Domain and diamond are interdefinable: we have $|a\rangle q = \ulcorner(a \cdot q)$. As noted in (3), $a \cdot q$ restricts a to the transitions that end in a q-point; the inverse image of q consists of the starting points of that.

Backward diamond, *backward box* and *codomain* can be defined almost symmetrically; some extra axioms compensate the lack of left-distributivity and right-strictness of $\cdot$. The backward diamond $\langle a|p$ yields the image of p under a.

We call an IL-semiring with forward and backward diamond and box *premodal* when these operators satisfy (the backward analogues of) (*Prediamond*) and *modal* when also (the backward analogues of) (*Composition*) hold.

The modal operators in a left-distributive IL-semiring are unique if they exist. They satisfy many useful laws. First, there are the Galois connections

$$\langle a|p \leq q \quad\Leftrightarrow\quad p \leq |a]q \;, \qquad\qquad |a\rangle p \leq q \quad\Leftrightarrow\quad p \leq [a|q \;. \tag{4}$$

As further samples we mention

$$\left.\begin{array}{rlrl} |a\rangle(p+q) &= |a\rangle p + |a\rangle q \;, & |a](p \cdot q) &= |a]p \cdot |a]q \;, \\ |a+b\rangle p &= |a\rangle p + |b\rangle p \;, & |a+b]p &= |a]p \cdot |b]p \;, \\ |p\rangle q &= p \cdot q \;, & |p]q &= p \to q \;. \end{array}\right\} \tag{5}$$

The latter implies $|1]q = q = |1\rangle q$ as well as $|0]p = 1$ and $|0\rangle p = 0$. Moreover, $|a]$ and $|a\rangle$ are isotone. Further, box is antitone and diamond is isotone in its action argument, i.e., $a \leq b \;\Rightarrow\; \forall p : |b](p) \leq |a](p) \wedge |a\rangle(p) \leq |b\rangle(p)$. If $\cdot$ is right-strict then we additionally get

$$|a]1 \;=\; 1 \;, \qquad\qquad |a\rangle 0 \;=\; 0 \;. \tag{6}$$

What is the difference to PDL? In PDL [14], actions and propositions are separate entities. Mostly no axioms for actions are given; these are more or less viewed syntactically. Their semantics is defined "observationally" via modal operators.

The connection between actions and propositions is achieved by "transfer" operators (e.g., $p?$, which turns proposition p into an action that behaves like a test).

In modal semirings, actions and propositions live in the same sort, hence no transfer operators are necessary. Actions have direct semantics and enjoy the algebraic semiring properties. Finally, since the modalities are internalised as regular operators, they may be freely nested, which is not possible in PDL.

4 Application II: Logics for Sequential Imperative Programs

Our next application specifies three types of semantics of imperative programs; the points here are program states.

4.1 Algebraic Model

Programs are represented by general elements $a, b, c \ldots$ of an IL-semiring, with choice $a+b$, sequential composition $a \cdot b$ and finite iteration in form of the *Kleene star* a^*. The latter is specified by the classical axioms [20]

$$1 + a \cdot a^* \leq a^* , \qquad 1 + a^* \cdot a \leq a^* , \qquad (\textit{Star Unfold})$$
$$b + a \cdot c \leq c \Rightarrow a^* \cdot b \leq c , \qquad b + c \cdot a \leq c \Rightarrow b \cdot a^* \leq c . \qquad (\textit{Star Induction})$$

We call a (pre)modal IL-semiring with star a *(pre)modal Kleene algebra*. Pleasantly, the star axioms induce corresponding laws for the modal operators without the need for stipulating additional axioms: in a premodal Kleene algebra,

$$p + \langle a|q \leq q \;\Rightarrow\; \langle a^*|p \leq q \; ; \qquad (\textit{Diamond Star Induction})$$

if the Kleene algebra is even modal, then also

$$p + \langle a|\langle a^*|p \leq \langle a^*|p \; . \qquad (\textit{Diamond Star Unfold})$$

Dual laws hold for the forward diamond and for the backward and forward boxes.

For a more intuitive notation, we define

$$\mathsf{abort} =_{df} \mathsf{false} =_{df} 0 , \qquad \mathsf{skip} =_{df} \mathsf{true} =_{df} 1 .$$

Moreover, as in [21], we introduce if and while operators:

$$\mathsf{if}\ p\ \mathsf{then}\ a\ \mathsf{else}\ b\ \mathsf{fi} =_{df} p \cdot a + \neg p \cdot b , \quad \mathsf{while}\ p\ \mathsf{do}\ a\ \mathsf{od} =_{df} (p \cdot a)^* \cdot \neg p . \qquad (7)$$

The latter is the least solution w of the standard recursion equation

$$w = \mathsf{if}\ p\ \mathsf{then}\ a \cdot w\ \mathsf{else}\ \mathsf{skip} = p \cdot a \cdot w \;+\; \neg p \cdot \mathsf{skip} .$$

We now illustrate how the algebraic semantics for the while loop copes with the phenomenon of non-termination. In the case where $\cdot$ is right-strict,

$$\mathsf{while}\ \mathsf{true}\ \mathsf{do}\ a\ \mathsf{od} = (1 \cdot a)^* \cdot \neg 1 = \; 0 = \mathsf{abort} .$$

This reflects the expected observable behaviour well, in the following sense: by observing a running program one cannot distinguish a non-terminating loop from a blocked program or from a program that terminates without visible output. Further, the star axioms entail $a \leq 1 \;\Rightarrow\; a^* = 1$. Hence

$$\mathsf{while}\ p\ \mathsf{do}\ \mathsf{skip}\ \mathsf{od} = (p \cdot 1)^* \cdot \neg p = p^* \cdot \neg p = 1 \cdot \neg p = \neg p .$$

That, too, meets intuition very well: a loop whose body does not modify any variables will terminate only if it is never entered. Similarly, since $p \cdot \mathsf{abort} \leq \mathsf{abort} \leq 1$, even without right strictness of $\cdot$,

$$\mathsf{while}\ p\ \mathsf{do}\ \mathsf{abort}\ \mathsf{od} = \neg p .$$

4.2 Hoare Logic

We now deal with Hoare logic for such programs, largely following [30,32]. Using modal operators and the Galois connections (4) we can give two algebraic versions of Hoare triples:

$$\{p\}\ a\ \{q\} \Leftrightarrow_{df} p \leq |a]q \Leftrightarrow \langle a|p \leq q\ . \tag{8}$$

Both express that all points a-reachable from p are guaranteed to satisfy q (cf. also (2)). The proof rules for these triples are shown in Fig. 3.

Divergence	*Skip*	*Assume*
$\dfrac{}{\{p\}\ 0\ \{q\}}$	$\dfrac{}{\{p\}\ 1\ \{p\}}$	$\dfrac{q \in \mathsf{test}(A)}{\{p\}\ q\ \{p \cdot q\}}$
Choice	*Sequencing*	*Iteration*
$\dfrac{\forall i \in \{1,2\} :\ \{p\}\ a_i\ \{q\}}{\{p\}\ a_1 + a_2\ \{q\}}$	$\dfrac{\{p\}\ a\ \{r\} \quad \{r\}\ b\ \{q\}}{\{p\}\ a \cdot b\ \{q\}}$	$\dfrac{\{p\}\ a\ \{p\}}{\{p\}\ a^*\ \{p\}}$
Disjunction	*Consequence*	*Atom*
$\dfrac{\{p_1\}\ a\ \{q_1\} \qquad \{p_2\}\ a\ \{q_2\}}{\{p_1 + p_2\}\ a\ \{q_1 + q_2\}}$	$\dfrac{p' \leq p \quad \{p\}\ a\ \{q\} \quad q \leq q'}{\{p'\}\ a\ \{q'\}}$	$\dfrac{a \text{ an atomic program}}{\{p\}\ a\ \{\langle a|p\}}$

Fig. 3. Proof Rules for the Hoare Calculus

The conclusion of the (*Atom*) rule may look a bit strange at first sight, since by (8) it is a mere tautology. To relate it to standard rules, we transform the triple in its conclusion as follows: by (8), logic twice and (8) again,

$$\{p\}\ a\ \{\langle a|p\} \Leftrightarrow \langle a|p \leq \langle a|p \Leftrightarrow \mathsf{TRUE} \Leftrightarrow |a]p \leq |a]p \Leftrightarrow \{|a]p\}\ a\ \{p\}\ . \tag{9}$$

In the case of a language with assignments, the standard rule $\{p[e/x]\}\ x := e\ \{p\}$ has precisely this latter form. In Fig. 3 we have used the form with the diamond operator for technical convenience.

As a final remark, to achieve relative completeness (see Th. 4.1) it is crucial that the underlying assertion language be *sufficiently expressive*. This means that, for all programs α and preconditions φ considered, there is an assertion ψ that expresses the strongest liberal postcondition for φ under α, i.e., there are tests p, q representing φ, ψ and a program element a representing α such that $q = \langle a|p$.

Theorem 4.1 (Soundness and Completeness of the Hoare Calculus). *Assume a left-distributive premodal Kleene algebra.*

1. *Using (Diamond Star Induction) one shows that the proof rules for the Hoare calculus are sound.*
2. *If the algebra is even modal then using (Diamond Star Unfold) one shows that they also satisfy relative completeness, i.e., every valid triple is provable.*

As for most logical calculi, the proof of soundness is straightforward.

For relative completeness we denote by $\vdash \{p\}\ a\ \{q\}$ that $\{p\}\ a\ \{q\}$ is derivable using the rules of Fig. 3. First, one shows by induction on the structure of statement a that

$$\vdash \{p\}\ a\ \{\langle a|p\}\ . \tag{10}$$

(Semantically, by (8), as for atomic programs, this triple is just a tautology.) The induction base is provided by the rules (*Divergence*), (*Skip*) and (*Atom*), the induction step by (*Choice*), (*Sequencing*) and (*Iteration*). This technique is presented in a concrete setting, e.g., in [1].

Now assume that $\{p\}\ a\ \{q\}$ holds. Then $\langle a|p \leq q$ by (8). Using (10) we obtain $\vdash \{p\}\ a\ \{\langle a|p\}$. Now the conclusion $\vdash \{p\}\ a\ \{q\}$ follows by the rule (*Consequence*).

The recently introduced TopKats [42] (the concept of which was known long before, cf. the Galois Connection $\ulcorner a \leq q \Leftrightarrow a \leq q \cdot \top$ in (56) of [8]) allow mimicking modal operators that satisfy only (*Prediamond*) and hence cannot establish relative completeness.

As an example of the use of the calculus we derive the standard while rule

$$\frac{\{q\}\ p \cdot a\ \{q\}}{\{q\}\ \mathsf{while}\ p\ \mathsf{do}\ a\ \mathsf{od}\ \{q \cdot \neg p\}}$$

Recall Definition (7), i.e., $\mathsf{while}\ p\ \mathsf{do}\ a\ \mathsf{od} =_{df} (p \cdot a)^* \cdot \neg p$. From the premise of the while rule we infer $\{q\}\ (p \cdot a)^*\ \{q\}$ by (*Iteration*). Moreover, by (*Assume*) we obtain $\{q\}\ \neg p\ \{q \cdot \neg p\}$, so that (*Sequencing*) yields the conclusion of the while rule.

4.3 Incorrectness Logic

Dually to Hoare Logic, which is used to show *absence* of errors, O'Hearn's Incorrectness Logic [37,40] allows reasoning about their *occurrence*. In its treatment we again follow [30]. The corresponding triples take the form

$$[p]\,a\,[q] \Leftrightarrow_{df} q \leq \langle a|p$$

Hence if q represents erroneous states, all of these are reachable from p states. The essential proof rules are shown in Fig. 4; for further ones see [30].

$$\frac{}{[p]\,0\,[0]}\ \textit{Divergence} \qquad \frac{}{[p]\,1\,[p]}\ \textit{Skip} \qquad \frac{q \in \mathsf{test}(A)}{[p]\,q\,[p \cdot q]}\ \textit{Assume}$$

$$\frac{\exists i \in \{1,2\}:\ [p]\,a_i\,[q]}{[p]\,a_1 + a_2\,[q]}\ \textit{Choice} \qquad \frac{[p]\,a\,[r] \quad [r]\,b\,[q]}{[p]\,a \cdot b\,[q]}\ \textit{Sequencing} \qquad \frac{\forall n \in \mathbb{N} : [p_n]\,a\,[p_{n+1}]}{[p_0]\,a^*\,[\bigsqcup_{n\in\mathbb{N}} p_n]}\ \textit{Iteration}$$

$$\frac{[p_1]\,a\,[q_1] \qquad [p_2]\,a\,[q_2]}{[p_1 + p_2]\,a\,[q_1 + q_2]}\ \textit{Disjunction} \qquad \frac{p \le p' \quad [p]\,a\,[q] \quad q' \le q}{[p']\,a\,[q']}\ \textit{Consequence} \qquad \frac{a \text{ an atomic program}}{[p]\,a\,[\langle a|p]}\ \textit{Atom}$$

Fig. 4. Proof Rules for Incorrectness Logic

For soundness and relative completeness, here we need an additional assumption about the algebra of tests. IL-semiring S is called *countably test-complete (CTC)* if every countable subset $S' \subseteq \mathsf{test}(S)$ has a lub $\bigsqcup S'$. (This is equivalent to stipulating that every countable chain of tests has a lub.)

Theorem 4.2 (Soundness and Completeness of Incorrectness Logic). *Assume a left-distributive premodal and CTC Kleene algebra.*

1. *Using (Diamond Star Induction) one shows that the rules in Fig. 4 satisfy relative completeness.*
2. *If the algebra is even modal then using (Diamond Star Unfold) one shows that they are also sound (preserve validity).*

The proofs are analogous to the Hoare case.

4.4 General Correctness Logic

While Sect. 4.2 showed how to model partial correctness in (pre)modal Kleene algebras, we now turn to total correctness, largely following [33]. For this, the transition behaviour must be enriched by information about presence/absence of non-termination. The basic idea in relational/logical approaches (e.g., [34,38]) is to model a command as a pair (a, p) consisting of an action element a that relates pre-/post-states and a set p of states from which termination is guaranteed; these states are called *non-diverging*. All states in $\neg p$ are considered to lead to the pseudo-state "looping" next to any proper successor states under a.

To make this idea work, we assume that the actions are modelled by elements of an I-semiring S (for an explanation see below). The set $\mathsf{COM}(S) =_{df} S \times \mathsf{test}(S)$ is then the set of all *commands* over S.

Now we can give algebraic definitions of Dijkstra's operators wlp and wp. For postcondition $q \in \mathsf{test}(S)$ and command (a,p) we set

$$\mathsf{wlp}.(a,p).q \;=_{df}\; |a]q\;, \qquad \mathsf{wp}.(a,p).q \;=_{df}\; p \cdot \mathsf{wlp}.(a,p).q\;.$$

Since we assume that S is an I-semiring, we have $|a]1 = 1$ by (6) and can retrieve the termination set of command (a,p) as $p = \mathsf{wp}.(a,p).1$. Hence all commands k satisfy Nelson's *pairing condition* $\mathsf{wp}.k.q = \mathsf{wp}.k.1 \cdot \mathsf{wlp}.k.q$.

We now define the basic commands and composition operators.

$$\begin{array}{c} \mathsf{loop} \;=_{df}\; (0,0)\;, \quad \mathsf{skip} \;=_{df}\; (1,1)\;, \quad \mathsf{fail} \;=_{df}\; (0,1)\;, \\ (a,p) \,[]\, (b,q) \;=_{df}\; (a+b,\, p \cdot q)\;, \\ (a,p)\,;\,(b,q) \;=_{df}\; (a \cdot b,\, p \cdot |a]q)\;. \end{array}$$

The command loop offers no transitions and terminates from no state; it models total blocking/divergence, similar to abort in Sect. 4.1. Command skip offers the identity transition, i.e., does not alter the state, and terminates from every state. Command fail is introduced because of its pleasant properties, like being a neutral element w.r.t. choice $[]$. It offers no transitions, but terminates from every state. Demonic choice $[]$ offers the union of the transitions of both operands but guarantees termination only for those states for which both operands do so. Sequential composition ; offers the composition of the transitions of the operands; termination can only be guaranteed for those states for which the first operand does so and for which all transitions offered by the first operand lead to states for which the second operand guarantees termination.

Theorem 4.3. *The structure* $\mathsf{COM}(S) \;=_{df}\; (\mathsf{COM}(S),\, []\,,;,\mathsf{fail},\mathsf{skip})$ *over an I-semiring* S *is a left-distributive IL-semiring, with* $[]\,,;,\mathsf{fail},\mathsf{skip}$ *playing the roles of* $+,\cdot,0,1$ *of IL-semirings. However,* $\mathsf{COM}(S)$ *is not an I-semiring. The associated natural order is* $(a,p) \leq (b,q) \;\Leftrightarrow\; a \leq b \wedge p \geq q$. *Finally,* $\mathsf{test}(\mathsf{COM}(S)) = \mathsf{test}(S) \times \{1\}$, *so that* $\mathsf{test}(\mathsf{COM}(S))$ *and* $\mathsf{test}(S)$ *are isomorphic.*

To see that $\mathsf{COM}(S)$ is not an I-semiring, we need to show that the left zero fail w.r.t. ; is not also a right zero. For instance,

$$\mathsf{loop}\,;\mathsf{fail} = (0,0)\,;(0,1) = (0,0) = \mathsf{loop} \neq \mathsf{fail}\;.$$

There is even more structure.

Theorem 4.4 (wp is wlp). $\mathsf{COM}(S)$ *admits a modal forward box, namely*

$$|k](q,1) \;=\; (\mathsf{wp}.k.q, 1)\;.$$

The theorem means that wp is nothing but wlp in the left-distributive modal semiring of commands. Therefore the standard properties of wlp and wp come for free by (5), since both are box operators in left-distributive modal semirings (for readability we abbreviate $(p,1)$ to just p, etc.):

$$\left.\begin{array}{c} \mathsf{w(l)p}.\mathsf{fail}.r = 1\,,\; \mathsf{w(l)p}.\mathsf{skip}.r = r\,, \\ \mathsf{w(l)p}.(k \,[]\, l).r = \mathsf{w(l)p}.k.r \cdot \mathsf{w(l)p}.l.r\,,\; \mathsf{w(l)p}.(k\,;\,l).r = \mathsf{w(l)p}.k.(\mathsf{w(l)p}.l.r)\,, \end{array}\right\} \qquad (11)$$

where w(l)p stands for either wlp or wp. The only command for which wlp and wp do not behave uniformly is loop, which does not have a counterpart in S:

$$\mathsf{wlp}.\mathsf{loop}.r = 1\ , \qquad \mathsf{wp}.\mathsf{loop}.r = 0\ . \tag{12}$$

But this is no wonder, since the whole idea of the wp operator is to distinguish between loop and fail, which wlp does not.

Another pleasant fact concerns a calculus for generalised correctness. Since we have seen that wp is wlp in a left-distributive modal IL-semiring, we can use the general soundness and relative completeness result for Hoare logic from Sect. 4.2, since its proof nowhere uses right-strictness of the underlying IL-semiring. The essential fact used in that proof was that the Hoare triple $\{p\}\ a\ \{\langle a|p\}$ is derivable for every command a and every test p. To use Th. 4.4 we deploy again the equivalences (8). From that and (11), (12) we read off the following axioms for the atomic commands:

$$\{1\}\ \mathsf{fail}\ \{q\}\ , \qquad \{0\}\ \mathsf{loop}\ \{q\}\ , \qquad \{q\}\ \mathsf{skip}\ \{q\}\ .$$

The rules for choice and sequencing become

$$\frac{\{p\}\ k\ \{r\} \qquad \{q\}\ l\ \{r\}}{\{p \cdot q\}\ k \,[\!]\, l\ \{r\}}\ , \qquad \frac{\{p\}\ k\ \{r\} \qquad \{r\}\ l\ \{q\}}{\{p\}\ k\,;l\ \{q\}}\ .$$

We conclude with a brief look at iteration.

Theorem 4.5. *The modal left semiring* $\mathsf{COM}(S)$ *of commands over a modal I-semiring* S *is a left-distributive modal Kleene algebra with* $(a, p)^* = (a^*, |a^*]p)$.

However, mimicking the while definition (7) yields a command that shows the adequate transition behaviour but is too lax w.r.t. termination information. This can be remedied, but the details (cf. [29,33]) would take up too much space.

5 Application III: Temporal Logics

The logic CTL^* allows reasoning about sets of (infinite) traces, also called *paths*. To represent these algebraically one may use special IL-semirings called *left quantales* (e.g. [41]). There the order $\leq$ induces a complete lattice and $\cdot$ distributes over arbitrary lubs in its right argument. The path semiring $\mathsf{PAT}(\Sigma)$ from Ex. 3.1.3 is a Boolean left quantale.

Notation 5.1. For a path σ we denote by σ_j $(j \in \mathbb{N})$ the point number j of σ and by σ^j the remainder of σ after removal of its first j points.

This section is based on [6].

5.1 Full CTL*

The CTL* formulas are given by the grammar

$$\Psi \ ::= \ \bot \mid \Phi \mid \Psi \to \Psi \mid \mathsf{E}\Psi \mid \mathsf{X}\Psi \mid \Psi \mathsf{U} \Psi \ , \tag{13}$$

where $\bot$ denotes falsity, Φ is a set of atomic formulas that characterise points, $\to$ is logical implication, E is the existential quantifier on paths, and X and U are the next-time and until operators.

We briefly recall the standard semantics, which tells when a path satisfies a formula. Path σ satisfies an atomic formula $\pi \in \Phi$ iff π holds for the first point of σ. Path σ satisfies $\mathsf{E}\varphi$ iff there is a path τ that satisfies φ and has the same first point as σ. Path σ satisfies $\mathsf{X}\varphi$ iff σ^1 satisfies φ. Path σ satisfies $\varphi \mathsf{U} \psi$ iff after a finite number (including zero) j of X steps the remaining path σ^j satisfies ψ and all path pieces σ^k with $k < j$ satisfy φ.

The logical connectives $\neg, \top, \wedge, \vee, \mathsf{A}$ are defined, as usual, by $\neg\varphi =_{df} \varphi \to \bot$, $\top =_{df} \neg\bot$, $\varphi \wedge \psi =_{df} \neg(\varphi \to \neg\psi)$, $\varphi \vee \psi =_{df} \neg\varphi \to \psi$ and $\mathsf{A}\varphi =_{df} \neg\mathsf{E}\neg\varphi$. Moreover, the "finally" operator F and the "globally" operator G are defined by

$$\mathsf{F}\psi =_{df} \top \mathsf{U} \psi \qquad \text{and} \qquad \mathsf{G}\psi =_{df} \neg\mathsf{F}\neg\psi \ . \tag{14}$$

Informally, $\mathsf{F}\psi$ holds if after a finite number of steps the remainder of the trace satisfies ψ, while $\mathsf{G}\psi$ holds if after every finite number of steps ψ still holds.

The sublanguages Ξ of *state formulas* and Π of *path formulas* denote sets of points and sets of computation traces, resp. Following [9], p. 1013, they are given by

$$\begin{aligned} \Xi \ &::= \bot \mid \Phi \mid \Xi \to \Xi \mid \mathsf{E}\Pi \mid \mathsf{A}\Pi, \\ \Pi \ &::= \Xi \mid \Pi \to \Pi \mid \mathsf{X}\Pi \mid \Pi \mathsf{U} \Pi \ . \end{aligned} \tag{15}$$

To give an algebraic semantics, we assign to each CTL* formula φ an element $[\![\varphi]\!]$ of a Boolean quantale, representing the set of paths $\{\sigma \mid \sigma \models \varphi\}$. The notation $\sigma \models \varphi$ means that path σ satisfies formula φ.

Atomic formulas in Φ are represented by tests. A quantale element n ("next") stands for the underlying one-step transition system of the logic under consideration. The precise requirements on n are developed in [29], but to get a feel for what it may be, consider a concrete semantics based on the path semiring $\mathsf{PAT}(\Sigma)$ from Ex. 3.1.3. Then n may be represented by a set of paths with exactly two nodes (i.e., *edges*), thus constituting a transition graph. The algebraic semantics $\mathsf{n} \cdot [\![\varphi]\!]$ for $\mathsf{X}\varphi$ given below is then simply the set of paths $x.\sigma$ (where . is standard, non-fusing concatenation as in Ex. 2.2), with $\sigma \in [\![\varphi]\!]$ and $x.\sigma_0 \in \mathsf{n}$. A different instance of n is given in Sect. 5.3.

To ease understanding we present the definition in classical first-order logic side by side with the algebraic one. In this, π is an arbitrary formula in Φ and Σ_π is the set of all points for which π holds.

$$
\begin{array}{lll}
\sigma \not\models \bot & & \\
\sigma \models \pi & \Leftrightarrow \sigma_0 \in \Sigma_\pi & \\
\sigma \models \varphi \to \psi & \Leftrightarrow \sigma \models \varphi \text{ implies } \sigma \models \psi & \\
\sigma \models \mathsf{E}\varphi & \Leftrightarrow \exists \tau \in \Sigma^\omega : \tau_0 = \sigma_0 \text{ and } \tau \models \varphi & \\
\sigma \models \mathsf{X}\,\varphi & \Leftrightarrow \sigma^1 \models \varphi & \\
\sigma \models \varphi\,\mathsf{U}\,\psi & \Leftrightarrow \exists j \geq 0 : \ \sigma^j \models \psi \text{ and } & \\
 & \qquad \forall k < j : \ \sigma^k \models \varphi &
\end{array}
$$

$$
\begin{aligned}
[\![\bot]\!] &= 0 \\
[\![p]\!] &= p \cdot \top \\
[\![\varphi \to \psi]\!] &= \overline{[\![\varphi]\!]} + [\![\psi]\!] \\
[\![\mathsf{E}\varphi]\!] &= \lceil [\![\varphi]\!] \cdot \top \ , \\
[\![\mathsf{X}\,\varphi]\!] &= \mathsf{n} \cdot [\![\varphi]\!] \ , \\
[\![\varphi\,\mathsf{U}\,\psi]\!] &= \bigsqcup_{j \geq 0} (\mathsf{n}^j \cdot [\![\psi]\!] \ \sqcap \ \prod_{k<j} \mathsf{n}^k \cdot [\![\varphi]\!])
\end{aligned}
$$

The expression $p \cdot \top$ denotes a *test ideal*, i.e., the set of all traces that start with p-points.

The semantics establishes soundness of the usual laws. From it we derive for the sublanguages CTL and LTL simpler semantics, involving the modal operators.

5.2 From CTL* to CTL

For a number of applications the sublogic CTL of CTL* suffices. According to [9], p.1013, syntactically CTL consists of those CTL* state formulas that only use path formulas of the restricted form (compare (15))

$$\Pi \ ::= \ \mathsf{X}\Xi \mid \Xi\mathsf{U}\Xi \ . \tag{16}$$

Hence, by (15), the full CTL grammar is

$$\Xi ::= \bot \mid \Phi \mid \Xi \to \Xi \mid \mathsf{EX}\Xi \mid \mathsf{AX}\Xi \mid \mathsf{E}(\Xi\mathsf{U}\Xi) \mid \mathsf{A}(\Xi\mathsf{U}\Xi) \ . \tag{17}$$

It turns out that the semantics of each state formula is a test ideal and hence directly corresponds to a test, i.e., an abstract representation of a set of points.

Theorem 5.2. *Let φ be a state formula of* CTL*.*

1. $[\![\varphi]\!]$ *is a test ideal, namely* $[\![\varphi]\!] = \lceil [\![\varphi]\!] \cdot \top$.
2. $[\![\mathsf{E}\varphi]\!] = [\![\varphi]\!]$ *and* $[\![\mathsf{A}\varphi]\!] = [\![\varphi]\!]$.

Hence for state formula φ we define the simplified semantics (the $\mathrm{index}_\mathsf{d}$ standing for "domain")

$$[\![\varphi]\!]_\mathsf{d} \ =_{df} \ \lceil [\![\varphi]\!] \ . \tag{18}$$

This enables us to calculate solely with tests.

One can derive an inductive representation of $[\![\,]\!]_\mathsf{d}$. For this, the modal operators diamond and box can conveniently be used. Additionally, we use an *omega* operator $^\omega$ (e.g. [2]) for infinite iteration. It is specified by the axioms

$$a^\omega \ = \ a \cdot a^\omega \ , \qquad \textit{(Omega Unfold)}$$

$$c \leq b + a \cdot c \ \Rightarrow \ c \leq a^\omega + a^* \cdot b \ . \qquad \textit{(Omega Co-Induction)}$$

In left quantales the omega operator always exists.

Theorem 5.3.

1. $[\![\bot]\!]_{\mathsf{d}} = 0$, $[\![p]\!]_{\mathsf{d}} = p$, $[\![\neg\varphi]\!]_{\mathsf{d}} = \neg[\![\varphi]\!]_{\mathsf{d}}$, $[\![\varphi \to \psi]\!]_{\mathsf{d}} = [\![\varphi]\!]_{\mathsf{d}} \to [\![\psi]\!]_{\mathsf{d}}$, $[\![\top]\!]_{\mathsf{d}} = 1$.
2. $[\![\mathsf{EX}\varphi]\!]_{\mathsf{d}} = |\mathsf{n}\rangle[\![\varphi]\!]_{\mathsf{d}}$, $[\![\mathsf{AX}\varphi]\!]_{\mathsf{d}} = |\mathsf{n}][\![\varphi]\!]_{\mathsf{d}} = [\![\mathsf{AXA}\varphi]\!]_{\mathsf{d}}$.
3. $[\![\mathsf{E}(\varphi\mathsf{U}\psi)]\!]_{\mathsf{d}} = |([\![\varphi]\!]_{\mathsf{d}} \cdot \mathsf{n})^*\rangle[\![\psi]\!]_{\mathsf{d}}$.
4. $[\![\mathsf{A}(\varphi\mathsf{U}\psi)]\!]_{\mathsf{d}} = \neg\lceil(\neg[\![\psi]\!]_{\mathsf{d}} \cdot \mathsf{n})^\omega \cdot |(\neg[\![\psi]\!]_{\mathsf{d}} \cdot \mathsf{n})^*](([\![\varphi]\!]_{\mathsf{d}} + [\![\psi]\!]_{\mathsf{d}})$.

The properties in No. 1 are self-evident. The ones in No. 2 mean that the existential and universal quantifiers of CTL are semantically reflected as the existential and universal modal operators diamond and box.

Property 3 means that the starting points of the traces in $[\![\mathsf{E}(\varphi\mathsf{U}\psi)]\!]_{\mathsf{d}}$ are precisely those from which after finitely many X steps through φ points a ψ point can be reached (remember that by (3) $[\![\varphi]\!]_{\mathsf{d}} \cdot \mathsf{n}$ is the restriction of n to $[\![\varphi]\!]_{\mathsf{d}}$ points).

Property 4 characterises $[\![\mathsf{A}(\varphi\mathsf{U}\psi)]\!]_{\mathsf{d}}$ as the set of those points from which it is not possible to iterate indefinitely on non-ψ points and after any finite number of iterations on non-ψ points a point that satisfies φ or ψ must be reached.

Note that all supremum and infimum operators $\bigsqcup/\bigsqcap$ have disappeared. In particular, the representation of the until operator in Property 3 is much much simpler than in the general semantics. This result shows that for CTL we do not need the full power of quantales; rather an omega algebra suffices.

5.3 From CTL* to LTL

According to [9], p.1002, LTL is the fragment of CTL* that does not have path quantifiers. More precisely, LTL has no state formulas and the path formulas are given by

$$\Pi ::= \Phi \mid \bot \mid \Pi \to \Pi \mid \mathsf{X}\Pi \mid \Pi\mathsf{U}\Pi \ .$$

Semantically its formulas φ behave like the state formulas $\mathsf{A}\varphi$ in CTL*.

For the precise semantics we want, in particular, an analogue of the simple CTL representation from Th. 5.3.3, namely

$$[\![\mathsf{E}(\varphi\mathsf{U}\psi)]\!]_{\mathsf{d}} = |([\![\varphi]\!]_{\mathsf{d}} \cdot \mathsf{n})^*\rangle[\![\psi]\!]_{\mathsf{d}} \ .$$

This is not immediate, since LTL has no state formulas and $[\![\,]\!]_{\mathsf{d}}$ cannot be used.

Therefore we present another semantics for LTL, based on the concrete IL-semiring $S = \mathcal{P}(\Sigma^+ \cup \Sigma^\omega)$ for some set Σ of points. The operators are union for $+$ and pointwise path concatenation for $\cdot$. Here we use the subalgebra of S with carrier set $\mathrm{INF}(S) =_{df} \mathcal{P}(\Sigma^\omega)$ and all operators restricted to $\mathrm{INF}(S)$. For brevity we denote this subalgebra again by $\mathrm{INF}(S)$. Its top element is Σ^ω. Now we embed $\mathrm{INF}(S)$ into the algebra $\mathsf{REL}(\Sigma^\omega)$ of binary relations over Σ^ω by a function $h : \mathrm{INF}(S) \to \mathsf{REL}(\Sigma^\omega)$ with $h(U) =_{df} \{(\sigma,\sigma) \mid \sigma \in U\}$, the partial identity relation corresponding to U. With this we define for path formula φ another semantic mapping

$$[\![\varphi]\!]_{\mathsf{L}} =_{df} h([\![\varphi]\!] \cap \mathrm{INF}(S)) \ .$$

In particular, $[\![\top]\!]_{\mathsf{L}} = h(\Sigma^\omega)$ is the identity relation on Σ^ω.

Next, we represent the semantic element n by a relation N (standing for "next"), namely $N =_{df} \{(\sigma, \sigma^1) \mid \sigma \in \Sigma^\omega\}$ (remember Notation 5.1). For $U \subseteq \Sigma^\omega$ we have $h(\mathsf{n} \cdot U) = |N\rangle h(U)$. Now we obtain

$$[\![\bot]\!]_{\mathsf{L}} = \emptyset\ , \qquad [\![p]\!]_{\mathsf{L}} = h(p \cdot \Sigma^\omega)\ , \qquad [\![\varphi \to \psi]\!]_{\mathsf{L}} = [\![\varphi]\!]_{\mathsf{L}} \to [\![\psi]\!]_{\mathsf{L}}\ ,$$
$$[\![\mathsf{X}\varphi]\!]_{\mathsf{L}} = |N\rangle [\![\varphi]\!]_{\mathsf{L}}\ , \qquad [\![\varphi \mathsf{U} \psi]\!]_{\mathsf{L}} = |([\![\varphi]\!]_{\mathsf{L}}\ ; N)^*\rangle [\![\psi]\!]_{\mathsf{L}}\ ,$$

i.e., the desired analogue of Th. 5.3.3. Consequently, $[\![\mathsf{F}\psi]\!]_{\mathsf{L}} = |N^*\rangle [\![\psi]\!]_{\mathsf{L}}$ and $[\![\mathsf{G}\psi]\!]_{\mathsf{L}} = |N^*][\![\psi]\!]_{\mathsf{L}}$.

This shows that for LTL we can weaken the requirements on the underlying semantic algebra even further, viz. to those of a modal Kleene algebra.

6 Sketches of Further Applications

Besides the above applications we now give glimpses at some other ones to further demonstrate the wide applicability of the modal semiring approach.

Epistemic Logics. This material bases on and extends [26]. Epistemic logics are special modal logics, dealing with belief and knowledge (e.g. [19]). They base on the well-known Kripke structures that each consist of a set of possible worlds and access relations between them. As in Sect. 3 these are modelled by elements of a left-distributive modal Kleene algebra, where tests represent sets of possible worlds.

We deal with multi-agent systems, where each agent may have her own belief/knowledge. Suppose there are agents i $(1 \leq i \leq n)$, each endowed with an access element a_i. Then, for a test p, a world w satisfies the predicate $\mathsf{K}_i p$ (i.e., belongs to the test $\mathsf{K}_i p$), where K_i is the knowledge operator for agent i, iff all neighbours of w under access element a_i lie in p. According to Sect. 3 this is faithfully reflected by defining $\mathsf{K}_i p =_{df} |a_i]p$. The everyone-knows operator E can then be defined as $\mathsf{E}p =_{df} \prod_{i=1}^{n} \mathsf{K}_i p$. By (5) this is equivalent to $\mathsf{E}p = |a]p$, where $a = \sum_{i=1}^{n} a_i$. The common knowledge operator C ("everyone knows that everyone knows that everyone knows...") is simply realised as $\mathsf{C}p =_{df} |a^+]p$.

Now epistemic reasoning can be done in equational logic. In [26,29] the approach is illustrated with the Wise Men and Muddy Children Puzzles. Moreover, there we briefly show how to algebraically model knowledge propagation and knowledge update.

Pointer Structures and Separation Logic. Based on and substantially extending [3], in [29], we model linked data structures and their typical associated phenomena. The semiring elements this time represent *meshes*, namely collections of direct edge-like connections, labelled by selector names, corresponding to pointers between nodes. The tests represent sets of nodes, where a *node* is an atomic test. As in general order theory, test p is atomic if for all tests q we have

$q \leq p \Rightarrow q = 0 \vee q = p$. A special node $\Box$ represents `nil` in PASCAL or `null` in JAVA. For mesh a the test $\ulcorner a$ characterises the nodes from which actually links emanate. We only consider meshes a with $\Box \cdot \ulcorner a = 0$, meaning that $\Box$ cannot be "dereferenced". Therefore, $\Box$ can serve as a "terminator" in pointer structures, e.g., for marking the end of a list or a leaf in a tree.

The set of nodes reachable from some set p of nodes along links from a is $reach(p, a) =_{df} \langle a^* | p$. Here is a typical localisation property that can be proved algebraically: If $reach(p, a) \cdot \ulcorner b = 0$, then $reach(p, a + b) = reach(p, a)$. In words: if none of the starting nodes of b is reachable from p via a links then all of b is unimportant for reachability from p via $a + b$, the union of a and b.

Among other things, our treatment characterises meshes that are forests or trees; operators for splitting trees/forests into smaller pieces are provided.

Standard Separation Logic (SL) [36] deals with reasoning about parts of an overall mesh. Meshes a, b are *weakly separate*, in symbols $a * b$[1], if $\ulcorner a \cdot \ulcorner b = 0$.

In [29] we use the notion of *strong separatedness*, namely

$$a \circledast b \Leftrightarrow_{df} reach(\ulcorner a, a + b) \cdot reach(\ulcorner b, a + b) \leq \Box \ .$$

This means that a and b span regions within the union $a + b$ that are disjoint except possibly for the terminator node $\Box$. With this notion we can prove frame rules analogous to the ones in standard SL.

Viability of the approach is shown by the examples of in-situ list reversal, tree rotation and an implementation of binary trees threaded for quicker and stack-less infix traversal.

Preference Database Queries. This material bases on and substantially extends [31]. Preferences (e.g., "I like blue cars better than red ones") allow more flexible and personalised queries in relational database systems. Evaluation of such queries means to select the maximal tuples from the database w.r.t. a preference "better than", which is a strict partial order. In [29,31] we represent preference relations by elements of an I-semiring, whereas tests represent sets of database tuples. The *best* or *maximal* tuples w.r.t. preference a and test p are represented by the test

$$\mathsf{max}_a\, p =_{df} p - |a\rangle p \ ,$$

where $q - r =_{df} q \cdot \neg r$ represents the (set) difference between q and r. This can be understood as follows: the tuples in $|a\rangle p$ each are a-below (dominated by) some tuple in p. Therefore $\mathsf{max}_a\, p$ consists of those tuples of p that are not dominated by any other tuple in p and hence are a-maximal within p.

In a practical system, complex preferences can be built out of simpler ones using, e.g., *Pareto composition* (closely related to the direct product) or *prioritisation* (closely related to the lexicographic product) of strict partial orders. In [29] we present an algebraic calculus of such constructions and exemplify its use in proving laws about preferences that can be used in query optimisation.

[1] The notational clash between $*$ and the Kleene star * is unfortunate, but standard.

7 Outlook

Some Related Algebraic Approaches. While it would be a hopeless task to survey the whole field of algebraic techniques, we briefly discuss a few other papers which are close in spirit to our style of treatment.

In [23] the authors introduce pKA, a probabilistic Kleene-style algebra, based on a widely accepted model of probabilistic/demonic computation. Separation theorems simplify reasoning about distributed systems, where with purely algebraic reasoning one can reduce complicated interleaving behaviour to "separated" behaviours each of which can be analysed on its own. The paper presents two case studies. The first treats a simple voting mechanism in the algebraic style. The second—based on Rabin's mutual exclusion with bounded waiting—rectifies some subtle flaws in the original presentation. The approach admits clear expositions of assumptions relating probability and secrecy and, in some cases, even simple characterisations of these in spite of their intricacy. Finally it is shown how the algebraic proofs can be automated using a modification of Aboul-Hosn and Kozen's KAT-ML.

The paper [12] studies two generalisations of KAT able to express programs as weighted transitions and tests with outcomes in non-necessarily bivalent truth spaces: graded Kleene algebra with tests (GKAT) and a variant where tests are also idempotent (I-GKAT). Fuzzy structures form special instances of this; applications include program verification and transformation.

In [17] the authors deal with an algebraic formulation of weighted graphs to connection paths in wireless networks. It uses matrices over an I-semiring of weights. These matrices carry not just the weights but even more information, such as the next "hop" on a path towards a destination. The matrices form again an I-semiring. They can be used not only for determining path lengths, but also to reconstruct the paths themselves, hop by hop.

The paper [5] studies how modal operators can be defined for fuzzy relations. These are mappings from pairs of elements into the interval $[0, 1]$ of real numbers. The values can be interpreted as transition probabilities or as capacities, and in various other ways. As a replacement for the complement operation one can use the mapping that sends x to $1 - x$. Together with the concepts of t-norm and t-conorm a weak form of Boolean algebra can be defined. Domain and codomain in a certain sense "measure" enabledness in transition systems. The paper presents a new axiomatisation of two variants of these operators in the setting of IL-semirings; it avoids complementation and hence is applicable to fuzzy relations. It is also shown how the notions of (pre)domain and modal operators can be lifted to the matrix level. Some applications to network flow problems, inspired by Kawahara's seminal paper on cardinality (see also the next paper), are sketched as well.

In [10] the authors deal with Stone relation algebras. These model weighted graphs and generalise relation algebras which capture only unweighted graphs. Previous work has axiomatised the cardinality operator in relation algebras, which counts the number of edges of an unweighted graph. The authors generalise the axioms for cardinality to Stone relation algebras where that oper-

ator forms the sum of the weights. They study the relationships between various axiom systems for cardinality. This results in simpler cardinality axioms also for relation algebras. The paper gives sufficient conditions for the representability of Stone relation algebras and for Stone relation algebras to be relation algebras.

And What About Concurrency? Since concurrency is a quite important topic, we want to make a few remarks about it.

All our examples in Sects. 4–6 involve some notion of "global state", and the modal operators map sets of states to sets of states.

A description of a form of concurrency with something like a global state is provided by Petri nets. There the place marking is a global entity, which enables a modal treatment [4].

But in other approaches to true, i.e., non-interleaving, concurrency this kind of global state does not exist; at best local states occur and can be handled.

This occurs also in the widely discussed framework of *Concurrent Kleene Algebras* [16]. These form I-semirings, and hence have, as all IL-semirings, the tests 0 and 1—but only these! So the test algebra is trivial and the modal operators are not interesting.

Therefore it remains an open problem whether a viable (pre)modal algebra for the concurrent case can be found.

Acknowledgements. We are grateful to Peter O'Hearn and the organisers of WADT 2024 for making this invited paper possible. We also thank the referees for their helpful comments.

References

1. Apt, K.R., Olderog, E.R.,: Verification of sequential and concurrent programs. 2nd edition, Springer (1997). https://doi.org/10.1007/978-1-84882-745-5
2. Cohen, E.: Separation and reduction. In: Backhouse, R., Oliveira, J.N. (eds.) MPC 2000. LNCS, vol. 1837, pp. 45–59. Springer, Heidelberg (2000). https://doi.org/10.1007/10722010_4
3. Dang, H.-H., Möller, B.: Extended transitive Separation Logic. J. Log. Alg. Meth. Program **84**(3), 303–325 (2015)
4. Dang, H.H., Möller, B.: Modal algebra and Petri nets. Acta Inf. **52**(2-3), 109–132 (2015)
5. Desharnais, J., Möller, B.: Fuzzifying modal algebra. In: Höfner, P., Jipsen, P., Kahl, W., Müller, M.E. (eds.) RAMICS 2014. LNCS, vol. 8428, pp. 395–411. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-06251-8_24
6. Desharnais, J., Möller, B.: Non-associative Kleene algebra and temporal logics. In: Höfner, P., Pous, D., Struth, G. (eds.) RAMICS 2017. LNCS, vol. 10226, pp. 93–108. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-57418-9_6
7. Desharnais, J., Möller, B., Struth, G.: Modal Kleene algebra and applications – a survey. J. Rel. Meth Comp. Sci. **1**, 93–131 (2004)
8. Desharnais, J., Möller, B., Struth, G.: Kleene algebra with domain. ACM Trans. Comp. Log. **7**, 798–833 (2006)
9. Emerson, E.: Temporal and modal logic. In: Jan van Leeuwen (ed.): Handbook of Theoretical Computer Science. Vol. B: Formal Models and Semantics. Elsevier, pp. 995–1072 (1990)

10. Furusawa, H., Guttmann, W.: Cardinality and representation of stone relation algebras. CoRR abs/2309.11676 (2023). https://doi.org/10.48550/arXiv.2309.11676
11. Gomes, V., Guttmann, W., Höfner, P., Struth, G., Weber, T.: Kleene algebras with domain. Arch. Formal Proofs (2016). https://isa-afp.org/entries/KAD.html
12. Gomes, L., Madeira, A., Barbosa, L.: Generalising KAT to verify weighted computations. Sci. Ann. Comp. Sci. **29**(2), 141–184 (2019)
13. Hägerstrand, T.: What about people in regional science? Pap. Reg. Sci. **24**(1), 7–24 (1970)
14. Harel, D., Kozen, D., Tiuryn, J.: Dynamic Logic. MIT Press (2000)
15. Hendricks, M.D., Egenhofer, M.J., Hornsby, K.: Structuring a Wayfinder's dynamic space-time environment. In: Kuhn, W., Worboys, M.F., Timpf, S. (eds.) COSIT 2003. LNCS, vol. 2825, pp. 75–92. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-39923-0_6
16. Hoare, T., Möller, B., Struth, G., Wehrman, I.: Concurrent Kleene algebra and its foundations. J. Log. Algebr. Program **80**(6), 266–296 (2011)
17. Höfner, P., McIver, A.: Hopscotch – reaching the target hop by hop. J. Log. Algebraic Methods Program **83**(2), 212–224 (2014)
18. Höfner, P., Struth, G.: Automated reasoning in Kleene algebra. In: Pfenning, F. (ed.) CADE 2007. LNCS (LNAI), vol. 4603, pp. 279–294. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73595-3_19
19. Huth, M., Ryan, M.: Logic in computer science: modelling and reasoning about systems. Cambridge University Press, 2nd edition (2004)
20. Kozen, D.: A completeness theorem for Kleene algebras and the algebra of regular events. Inf. Comput. **110**, 366–390 (1994)
21. Kozen, D.: Kleene algebras with tests. ACM Trans. Program. Lang. Syst. **19**, 427–443 (1997)
22. Manes, E., Benson, D.: The inverse semigroup of a sum-ordered semiring. Semigroup Forum **31**, 129–152 (1985)
23. McIver, A., Gonzalia, C., Cohen, E., Morgan, C.: Using probabilistic Kleene algebra PKA for protocol verification. J. Logic Alg. Prog. **76**, 90–111 (2008)
24. Minkowski, H.: Raum und Zeit. Physikalische Zeitschrift, vol. 10, pp. 104–111 (1909). English translation in Petkov, V., (ed.): Minkowski, H., Space and Time: Minkowski's papers on relativity. Minkowski Institute Press (2012) http://www.minkowskiinstitute.org/mip/books/minkowski.html
25. McCune, W.: Prover9 and Mace4. https://www.cs.unm.edu/~mccune/prover9/
26. Möller, B.: Modal knowledge and game semirings. Comp. J. **56**(1), 53–69 (2013)
27. Möller, B.: Geographic Wayfinders and space-time algebra. J. Log. Alg. Meth. Prog. **104**, 274–302 (2019)
28. Möller, B., Desharnais, J: Basics of modal semirings and of Kleene/omega algebras. Report 2019-03. Universität Augsburg (2019). https://opus.bibliothek.uni-augsburg.de/opus4/files/63988/TR-2019-03.pdf
29. Möller, B., Desharnais, J.: Modal semirings and applications. Accepted for the series Trends in Logic. Springer (2025) (to appear)
30. Möller, B., O'Hearn, P., Hoare, T.: On algebra of program correctness and incorrectness. In: Fahrenberg, U., Gehrke, M., Santocanale, L., Winter M., (eds.): Relational and algebraic methods in computer science. LNCS 13027, pp. 325 – 343. Springer ?(2021)
31. Möller, B., Roocks, P.: An algebra of database preferences. J. Log. Algebr. Meth. Program **84**(3), 456–481 (2015)
32. Möller, B., Struth, G.: Algebras of modal operators and partial correctness. Theo. Comp. Sci. **351**, 221–239 (2006)

33. Möller, B., Struth, G.: wp is wlp. In: MacCaull, W., Winter, M., Düntsch, I. (eds.) RelMiCS 2005. LNCS, vol. 3929, pp. 200–211. Springer, Heidelberg (2006). https://doi.org/10.1007/11734673_16
34. Nelson, G.: A generalization of Dijkstra's calculus. ACM Trans. Prog. Lang. Syst. **11**(4), 517–561 (1989)
35. Nipkow, T., Wenzel, M., Paulson, L.C. (eds.): Isabelle/HOL - a proof assistant for higher-order logic. LNCS, vol. 2283. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45949-9
36. O'Hearn, P.W.: Separation logic. Commun. ACM **62**(2), 86–95 (2019)
37. O'Hearn, P.: Incorrectness logic. PACML (POPL) **4**, 10:1–10:32 (2020)
38. Parnas, D.: A generalised control structure and its formal definition. Commun. ACM **26**, 572–581 (1983)
39. Popkorn, S.: First steps in modal logic. Cambridge University Press (1994)
40. Raad, A., Berdine, J., Dang, H.-H., Dreyer, D., O'Hearn, P., Villard, J.: Local reasoning about the presence of bugs: incorrectness separation logic. In: Lahiri, S.K., Wang, C. (eds.) CAV 2020. LNCS, vol. 12225, pp. 225–252. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-53291-8_14
41. Rosenthal, S.: Quantales and their applications. Pitman Research Notes in Mathematics Series, Vol. 234. Longman Scientific and Technical (1990)
42. Zhang, C., de Amorim, A.A., Gaboardi, M., : On incorrectness logic and Kleene algebra with top and tests. Proc. ACM Princ. Prog. Langs. **6** (POPL), 1–30 (2022)