Universität Augsburg

Basics of Modal Semirings and of Kleene/Omega Algebras

Bernhard Möller, Jules Desharnais

Report 2019-03 October 2019

Institut für Informatik
D-86135 Augsburg

Preface

Algebraic structures, such as modal idempotent semirings or Kleene algebras, offer a large variety of applications, while requiring only a small set of operators and axioms. Such algebras abstractly capture so-called Kripke structures, i.e., access relations over a set of worlds or states. In addition they provide the associated multi-modal operators box and diamond that allow reasoning, e.g., about possible actions of agents in a system or about state transitions in general. Particular instances of modal semirings are provided by the algebra of homogeneous binary relations and by abstract relation algebras.

This setting allows many general considerations and results, ranging from epistemic logics with knowledge and belief [55] to propositional dynamic Hoare logic and resource-based settings such as separation logic [15]. Moreover, many further applications are covered, like abstract reasoning about bisimulations for model refinement [29], formal concept analysis, simple and concise correctness proofs for the optimisation of database preference queries [56], Petri nets [16] or generally applicable models of module hierarchies in a feature oriented software development process [6].

A large collection of such examples is treated in the forthcoming book *Modal semirings and applications* by the two authors, of which this report presents the first three chapters with the basic algebraic definitions and essential theorems about them. It serves as a reference for the current state of the theory.

Augsburg/Québec,
October 24, 2019

Bernhard Möller
Jules Desharnais

Acknowledgements

Many individuals have helped us with their comments and corrections, and partly also by substantial contributions to the presented material: Sven Apel, Don Batory, Rudolf Berghammer, Han-Hing Dang, Thorsten Ehm, Markus Endres, Roland Glück, Walter Guttmann, Anastasiya Grinenko, Tony Hoare, Peter Höfner, Ridha Khedri, Dominik Kölbl, Christian Lengauer, Martin E. Müller, Patrick Roocks, Martin Russling, Gunther Schmidt, Michel Sintzoff, Kim Solin, Georg Struth, Fairouz Tchier, Michael Winter, Andreas Zelend. We also want to thank Ewa Orłowska for initiating the writing of the book as well as Werner Kießling and Gunther Schmidt for temporarily furnishing positions for some of the above persons. Finally, we gratefully acknowledge partial funding of this work by the DFG projects *MO 690/7-1//-2* FeatureFoundation and *MO 690/9-1/9-2* AlgSep — *Algebraic Calculi for Separation Logic*, as well as by the Natural Sciences and Engineering Research Council of Canada.

Contents

1 Idempotent Left Semirings 1
1.1 Introduction 1
1.2 Preliminaries on Order Theory 2
1.2.1 Basic Notions 2
1.2.2 (Semi)Lattices 3
1.2.3 Kernel Operators 7
1.3 Basic Algebraic Structures 9
1.4 Idempotent Left Semirings 9
1.5 Examples of IL-Semirings 12

2 Tests, Domain and Modal Operators 17
2.1 Tests 17
2.2 Restriction 22
2.3 Tests as a Boolean Algebra 26
2.4 Predomain and Domain 28
2.5 Examples of Predomain and Domain Semirings 34
2.6 Precodomain and Codomain 36
2.7 Galois Connections 38
2.8 Modal Operators 41
2.9 Modal Operators as Semiring Elements 46

3 Iteration: Kleene and Omega Algebras 49
3.1 Elements of Fixed Point Theory 49
3.2 Finite Iteration: Left Kleene Algebras 51
3.3 Examples of Kleene Algebras 56
3.4 Infinite Iteration: Omega Algebras 58
3.5 Iteration, Tests and Modal Operators 63
3.6 Extremal Elements, Noetherity, Divergence and Convergence 65

References 70
References 70

Index 73

Chapter 1
Idempotent Left Semirings

I would use this semiring from a desire to do good...
— The Lord of the Semirings

1.1 Introduction

Semirings have a wide range of applications in computer science: in the theory of formal languages and automata (regular expressions) (e.g. [48]), logic of programs (e.g. [32, 45]) and many more [30, 33].

The elements of such algebras can be viewed as abstract representations of transition structures, such as relations between states, or paths (or more general partially ordered structures) that connect starting states to end states.

The characteristic operators of semirings are choice, denoted by $+$, and sequential composition, denoted by $\cdot$. Moreover, there are the constants 0, denoting the empty (or always blocking) transition system, and 1, representing identical transitions ("do nothing"). These are the neutral elements of $+$ and $\cdot$ respectively.

Classically, both operators are associative and $+$ is commutative. Moreover, as in school algebra, they satisfy the distributive laws and 0 is a left and right annihilator. To give $+$ really the character of a choice operator it is required to be idempotent.

This classical view is, however, not adequate when the phenomena of non-strictness or delay in choice are to be modelled. This is achieved by using *left semirings* in which 0 is only a left annihilator and $\cdot$ distributes through $+$ only from the right.

The theory of these structures and the presentation of many examples relevant for computer science form the main contents of the present chapter; before that we recall a number of facts from the theory of partial orders, which plays a central role as well.

We provide some remarks on notation. We write $\Leftrightarrow_{df}$ and $=_{df}$ for definitional equivalence and definitional equality. Also, we use the common abbreviation "iff" for "if and only if".

As customary, free variables in formulas are assumed to be universally quantified. Moreover, the range of a quantifier extends as far to the right as the parentheses allow.

1.2 Preliminaries on Order Theory

We repeat some definitions concerning partial orders that will be used throughout the report.

1.2.1 Basic Notions

Definition 1.2.1 A *partial order* on a set M is a reflexive, transitive and antisymmetric binary relation $\leq \subseteq M \times M$. Frequently, also the pair $(M, \leq)$ is referred to as a partial order. For a partial order $\leq$ we define the converse relation $\geq$, as usual, by $a \geq b \Leftrightarrow_{df} b \leq a$; it is a partial order again. The partial order is *linear* if any two elements are comparable, i.e., if for all $x, y \in M$ we have $x \leq y \vee y \leq x$. A subset $N \subseteq M$ is called a *chain* if $\leq$ is linear on N.

We now state four quite effective reasoning techniques for partial orders [25].

Lemma 1.2.2 *Consider a partial order $(M, \leq)$ and elements $a, b \in M$.*

1. $a \leq b \Leftrightarrow (\forall\, c : c \leq a \Rightarrow c \leq b)$. *(indirect inequality I)*
2. $a \leq b \Leftrightarrow (\forall\, c : b \leq c \Rightarrow a \leq c)$. *(indirect inequality II)*
3. $a = b \Leftrightarrow (\forall\, c : c \leq a \Leftrightarrow c \leq b)$. *(indirect equality I)*
4. $a = b \Leftrightarrow (\forall\, c : b \leq c \Leftrightarrow a \leq c)$. *(indirect equality II)*

Proof. We only show the first claim, the second one being symmetric and the third and fourth ones following from the first two using antisymmetry of $\leq$.

The direction $(\Rightarrow)$ holds by transitivity of $\leq$. For $(\Leftarrow)$ choose $c = a$ and use reflexivity of $\leq$. □

We define bounding elements by formulas similar to the ones in the above lemma.

Definition 1.2.3 Consider a partial order $(M, \leq)$ and a subset $N \subseteq M$.

1. We call l a *least element* of N if $l \in N \wedge \forall\, a \in N : l \leq a$. Within N least elements are unique if they exist.
2. Dually, we call g a *greatest element* of N if $g \in N \wedge \forall\, a \in N : a \leq g$. Within N greatest elements are unique if they exist.
3. We call s the *least upper bound* or *supremum* of N and write $s = \bigsqcup N$ when s is the least element in the set of all upper bounds of N in M, i.e.,

$$s \leq c \Leftrightarrow \forall\, a \in N : a \leq c\ .$$

The only free variable in this formula is c. Hence this formula is short for

$$\forall\, c \in M : s \leq c \Leftrightarrow (\forall\, a \in N : a \leq c)\ .$$

Note that s need not exist. It is customary to set $a \sqcup b =_{df} \bigsqcup \{a, b\}$ when it exists, where $\{a, b\} = \{a\}$ when $a = b$. The above characterisation of $\sqcup$ simplifies to

$$a \sqcup b \leq c \Leftrightarrow a \leq c \wedge b \leq c\ . \tag{1.1}$$

In particular, $a, b \leq a \sqcup b$.

4. Dually, we call i the *greatest lower bound* or *infimum* of N and write $i = \bigsqcap N$ when i is the supremum of N w.r.t. the converse order $\geq$. Its characterisation therefore reads

$$c \leq i \Leftrightarrow \forall\, a \in N : c \leq a\ .$$

It is customary to set $a \sqcap b =_{df} \bigsqcap \{a, b\}$. The above characterisation of $\sqcap$ simplifies to

$$c \leq a \sqcap b \Leftrightarrow c \leq a \wedge c \leq b\ .$$

In particular, $a \sqcap b \leq a, b$.

Let us explain the characterisation of the supremum. Setting in Part 3 $c = s$ makes the left hand side true and hence implies $\forall\, a \in N : a \leq s$, so that s is indeed an upper bound for N. The direction ($\Leftarrow$) means that s is below any such bound and therefore is the least upper bound of N (and as such uniquely defined). An analogous explanation applies to the infimum.

As easy exercises, the reader may wish to use indirect (in)equality to infer

$$a \leq b \Leftrightarrow b = a \sqcup b \qquad \text{and} \qquad a \leq b \Leftrightarrow a = a \sqcap b\ . \tag{1.2}$$

1.2.2 (Semi)Lattices

Definition 1.2.4

1. When $a \sqcup b$ exists for all elements $a, b \in M$ then $(M, \leq)$ is called an *upper semilattice*. When $a \sqcap b$ exists for all elements $a, b \in M$ then $(M, \leq)$ is called a *lower semilattice*. If $(M, \leq)$ is both an upper and a lower semilattice, it is called a *lattice*. This entails the absorption laws

$$a \sqcup (a \sqcap b) = a = a \sqcap (a \sqcup b)\ .$$

A lattice is called *distributive* if it satisfies the distributivity axioms

$$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)\ , \qquad a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)\ .$$

It is well known that it suffices to stipulate one of them; the other follows.

2. When *every* subset $N \subseteq M$ has a supremum $\bigsqcup N$ (and hence, by standard lattice theory also an infimum $\bigsqcap N$), $(M, \leq)$ is called a *complete lattice*. In this case M has a least element $\bot$ and a greatest element $\top$.

A complete lattice is *completely distributive* if it satisfies the generalised distributivity axioms

$$a \sqcup (\bigsqcap N) = \bigsqcap \{a \sqcup b \,|\, b \in N\} \ , \qquad a \sqcap (\bigsqcup N) = \bigsqcup \{a \sqcap b \,|\, b \in N\} \ .$$

Again, it suffices to stipulate one of them; the other follows.

We prove the characteristic algebraic properties of semilattices to illustrate the use of the characterisation of $\sqcup$ and the principle of indirect equality.

Lemma 1.2.5 *In an upper semilattice, $\sqcup$ is an associative, commutative and idempotent binary operator on M, the latter property meaning $a \sqcup a = a$. Symmetrically, the infimum operator $\sqcap$ in a lower semilattice is associative, commutative and idempotent.*

Proof. The algebraic properties of $\sqcup$ are just played back to the corresponding ones of $\wedge$:
Associativity: $a \sqcup (b \sqcup c) \leq d \Leftrightarrow a \leq d \wedge b \sqcup c \leq d \Leftrightarrow a \leq d \wedge b \leq d \wedge c \leq d$
$\Leftrightarrow a \sqcup b \leq d \wedge c \leq d \Leftrightarrow (a \sqcup b) \sqcup c \leq d.$
Commutativity: immediate from the commutativity of $\wedge$.
Idempotence: $a \sqcup a \leq c \Leftrightarrow a \leq c \wedge a \leq c \Leftrightarrow a \leq c.$ □

Vice versa, one may step from an algebraic view to an order-theoretic one.

Lemma 1.2.6 *Let $\sqcup$ be an associative, commutative and idempotent binary operator on a set M. Then the relation $\leq$ given by*

$$a \leq b \Leftrightarrow_{df} a \sqcup b = b$$

is a partial order making M an upper semilattice with supremum operator $\sqcup$.

Proof.
Reflexivity: By the definition of $\leq$, its reflexivity is equivalent to idempotence of $\sqcup$.
Transitivity: Assume $a \leq b$ and $b \leq c$, i.e., $a \sqcup b = b$ and $b \sqcup c = c$. Then, by associativity of $\sqcup$, we have $a \sqcup c = a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c = b \sqcup c = c$, i.e., $a \leq c$.
Antisymmetry: Assume $a \leq b$ and $b \leq a$, i.e., $a \sqcup b = b$ and $b \sqcup a = a$. Then, by commutativity of $\sqcup$, we have $a = b \sqcup a = a \sqcup b = b$.

It remains to show that $\sqcup$ is a supremum operator, i.e., that

$$a \sqcup b \leq c \Leftrightarrow a \leq c \wedge b \leq c \ .$$

($\Rightarrow$) Assume $a \sqcup b \leq c$, i.e., $a \sqcup b \sqcup c = c$. Then, employing associativity and idempotence of $\sqcup$, we have $a \sqcup c = a \sqcup a \sqcup b \sqcup c = a \sqcup b \sqcup c = c$, i.e., $a \leq c$. Similarly, one shows $b \leq c$, using additionally commutativity of $\sqcup$.
($\Leftarrow$) We obtain, using the definition of $\leq$, associativity of $\sqcup$ and the definition of $\leq$ again,

$$a \leq c \wedge b \leq c \Leftrightarrow a \sqcup c = c \wedge b \sqcup c = c \Rightarrow$$
$$a \sqcup b \sqcup c = a \sqcup c = c \Leftrightarrow a \sqcup b \leq c \ .$$

□

Definition 1.2.7

1. A *Boolean algebra* is a lattice M with a complement operator $^- : M \to M$ that satisfies Huntington's axiom [36, 37]
$$a = \overline{\overline{a} \sqcup b} \sqcup \overline{\overline{a} \sqcup \overline{b}} \; .$$
This implies the distributive and De Morgan laws
$$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c) \; , \quad a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c) \; ,$$
$$\overline{a \sqcup b} = \overline{a} \sqcap \overline{b} \; , \qquad \overline{a \sqcap b} = \overline{a} \sqcup \overline{b} \; .$$
2. In a Boolean algebra we can define
$$\top =_{df} a \sqcup \overline{a} \quad \text{and} \quad \bot =_{df} a \sqcap \overline{a}$$
for an arbitrary a. The axioms entail $a \sqcup b = \top \Rightarrow \overline{a} \leq b$ and $a \sqcap b = \bot \Rightarrow b \leq \overline{a}$ and therefore $b = \overline{a}$. Hence the complement operator is unique if it exists. It is easy to show that $\bot$ and $\top$ are the least and greatest element of M, resp.
3. A Boolean algebra in which the underlying lattice is complete is called a *complete Boolean algebra*.

An important proof principle in Boolean algebras is the *shunting rule*
$$a \sqcap b \leq c \Leftrightarrow a \leq \overline{b} \sqcup c \; . \tag{1.3}$$
To enable application of the shunting rule, we state many assertions of the form $a = \bot$ in the equivalent form $a \leq \bot$ (the reverse inequation $\bot \leq a$ holds anyway, since $\bot$ is the least element of any Boolean algebra). An example is the special case $c = \bot$, namely $a \sqcap b \leq \bot \Leftrightarrow a \leq \overline{b}$.

Now we turn to functions between partial orders.

Definition 1.2.8 Consider a function $f : M \to N$ between partial orders $(M, \leq_M)$ and $(N, \leq_N)$.

1. We call f *isotone* or *monotonically increasing* when
$$a \leq_M b \Rightarrow f(a) \leq_N f(b) \; .$$
2. We call f *antitone* or *monotonically decreasing* when
$$a \leq_M b \Rightarrow f(b) \leq_N f(a) \; .$$
3. We call f *universally super-disjunctive* when for all $L \subseteq M$ such that $\bigsqcup L$ and $\bigsqcup f(L)$ exist (where $f(L) \subseteq N$ is the image of L under f) we have $\bigsqcup f(L) \leq f(\bigsqcup L)$.
4. Dually, f is *universally sub-conjunctive* when for all $L \subseteq M$ such that $\bigsqcap L$ and $\bigsqcap f(L)$ exist we have $f(\bigsqcap L) \leq \bigsqcap f(L)$.
5. We call f *super-disjunctive* when for all $a, b \in M$ for which $a \sqcup b$ and $f(a) \sqcup f(b)$ exist we have $f(a) \sqcup f(b) \leq f(a \sqcup b)$.
6. Dually, f is *sub-conjunctive* when for all $a, b \in M$ for which $a \sqcap b$ and $f(a) \sqcap f(b)$ exist we have $f(a \sqcap b) \leq f(a) \sqcap f(b)$.
7. We call f *(universally) disjunctive* when it is (universally) super-disjunctive and the inequations above strengthen to equations.
8. Dually, f is *(universally) conjunctive* when it is (universally) sub-conjunctive and the inequations above strengthen to equations.

9. A function is *continuous* if it preserves suprema of non-empty chains. Dually, it is *co-continuous* if it preserves infima of non-empty chains.

These notions generalise in a natural way to n-ary functions: $f : M_1 \times \ldots \times M_i \times \ldots \times M_n \to N$ is called *isotone in argument* i $(1 \leq i \leq n)$ if for all $(x_1, \ldots, x_i, \ldots, x_n) \in M_1 \times \ldots \times M_i \times \ldots \times M_n$ and every $y_i \in M_i$ with $x_i \leq y_i$ we have $f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \leq f(x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_n)$. The other notions generalise correspondingly.

We list some useful consequences.

Corollary 1.2.9 *Consider a function $f : M \to N$ between partial orders $(M, \leq_M)$ and $(N, \leq_N)$.*

1. *If f is isotone then it is universally super-disjunctive and universally sub-conjunctive.*
2. *If $(N, \leq_N)$ is an upper semilattice then f is isotone iff it is super-disjunctive.*
3. *In any upper semilattice, $\sqcup$ is isotone in both arguments.*

Proof.

1. Consider a subset $L \subseteq M$ such that $\bigsqcup L$ and $\bigsqcup f(L)$ exist. By straightforward generalisation of the characterisation of $\bigsqcup$ in (1.1) and isotony of f we have
$$\bigsqcup f(L) \leq_N f(\bigsqcup L) \Leftrightarrow (\forall\, a \in f(L) : a \leq_N f(\bigsqcup L))$$
$$\Leftrightarrow (\forall\, b \in L : f(b) \leq_N f(\bigsqcup L)) \Leftarrow (\forall\, b \in L : b \leq_M \bigsqcup L) \Leftrightarrow \mathsf{TRUE}\ .$$
2. By Part 1, every isotone function is super-disjunctive. For the converse implication, assume $a \leq_M b$, i.e., $a \sqcup_M b = b$. Since $(N, \leq_N)$ is an upper semilattice, $f(a) \sqcup_N f(b)$ exists, and super-disjunctivity of f implies $f(a) \sqcup_N f(b) \leq_N f(a \sqcup_M b) = f(b)$. By definition of $\sqcup$, this entails $f(a) \leq_N f(b)$.
3. Suppose $a \leq b$, i.e., $a \sqcup b = b$. Then, using associativity, commutativity and idempotence of $\sqcup$, we obtain $(a \sqcup c) \sqcup (b \sqcup c) = a \sqcup b \sqcup c = b \sqcup c$, i.e., $a \sqcup c \leq b \sqcup c$. The proof for the second argument is analogous. □

The following useful result seems not yet to be known in the literature.

Lemma 1.2.10 *Assume a Boolean algebra M and a lattice N. Consider, moreover, a function $f : M \to N$ that is conjunctive and disjunctive. Then the image set $f(M)$ again forms a Boolean algebra with $\overline{f(a)} = f(\overline{a})$.*

Proof. First, note that by the assumption and Cor. 1.2.9.2 f is isotone. In particular, $f(\bot)$ and $f(\top)$ are the least and greatest elements of $f(M)$, resp.

Second, by conjunctivity and disjunctivity $f(M)$ inherits distributivity from M.

Now we have to show that setting $\overline{f(a)} =_{df} f(\overline{a})$ is well defined. To this end we prove
$$f(a) = f(b) \Rightarrow f(\overline{a}) = f(\overline{b})\ .$$
By the definition of $\top$ and f disjunctivity we have $f(\top) = f(b) \sqcup f(\overline{b})$. Hence,

$$
\begin{array}{ll}
& f(\overline{a}) \\
= & f(\overline{a}) \sqcap (f(b) \sqcup f(\overline{b})) & \{\!\![\text{ greatestness of } f(\top) \text{ in } f(M)]\!\!\} \\
= & (f(\overline{a}) \sqcap f(b)) \sqcup (f(\overline{a}) \sqcap f(\overline{b})) & \{\!\![\text{ distributivity }]\!\!\} \\
= & (f(\overline{a}) \sqcap f(a)) \sqcup (f(\overline{a}) \sqcap f(\overline{b})) & \{\!\![\text{ assumption } f(a) = f(b)]\!\!\} \\
= & f(\overline{a} \sqcap a) \sqcup (f(\overline{a}) \sqcap f(\overline{b})) & \{\!\![f \text{ conjunctive }]\!\!\} \\
= & f(\bot) \sqcup (f(\overline{a}) \sqcap f(\overline{b})) & \{\!\![\text{ definition of } \bot]\!\!\} \\
= & f(\overline{a}) \sqcap f(\overline{b}) & \{\!\![\text{ leastness of } f(\bot) \text{ in } f(M)]\!\!\} \\
\leq & f(\overline{b}) \ . & \{\!\![\text{ characterisation of infima }]\!\!\}
\end{array}
$$

Symmetrically we obtain $f(\overline{b}) \leq f(\overline{a})$, which shows the claim.

Now we show that Huntington's axiom holds on the image set of f, which proves the claim:

$$
\begin{array}{ll}
& \overline{\overline{f(a)} \sqcup f(b)} \sqcup \overline{\overline{f(a)} \sqcup \overline{f(b)}} \\
= & \overline{f(\overline{a}) \sqcup f(b)} \sqcup f(\overline{a}) \sqcup f(\overline{b}) & \{\!\![\text{ above definition of complement }]\!\!\} \\
= & \overline{f(\overline{a} \sqcup b)} \sqcup f(\overline{a} \sqcup \overline{b}) & \{\!\![f \text{ disjunctive }]\!\!\} \\
= & f(\overline{\overline{a} \sqcup b}) \sqcup f(\overline{a} \sqcup \overline{b}) & \{\!\![\text{ above definition of complement }]\!\!\} \\
= & f(\overline{\overline{a} \sqcup b} \sqcup \overline{a} \sqcup \overline{b}) & \{\!\![f \text{ disjunctive }]\!\!\} \\
= & f(a) \ . & \{\!\![\text{ Huntington's axiom on } M]\!\!\}
\end{array}
$$

□

Finally, a concept that is useful in various circumstances is that of a dual function.

Definition 1.2.11 Let $f : M \to N$ be a function between Boolean algebras M, N. The *De Morgan dual* of f, denoted f°, is defined by $f^\circ(x) =_{df} \overline{f(\overline{x})}$.

1.2.3 Kernel Operators

Kernel operators arise in many contexts and satisfy quite useful properties.

Definition 1.2.12 A *kernel* operator is an isotone, contractive and idempotent function $f : M \to M$ from some partial order $(M, \leq)$ into itself. The latter two properties spell out to $f(x) \leq x$ and $f(f(x)) = f(x)$ for all $x \in M$.

Corollary 1.2.13 *The image $f(M)$ of a kernel operator f consists exactly of the fixed points of f, i.e., the elements $x \in M$ with $x = f(x)$.*

Proof. For $x \in f(M)$, say $x = f(y)$, idempotence of f shows $f(x) = f(f(y)) = f(y) = x$. Conversely, $x = f(x)$ trivially implies $x \in f(M)$. □

Lemma 1.2.14 *Let $f : M \to M$ be a kernel operator.*

1. *$f(a) = \bigsqcup \{b \in f(M) : b \leq a\}$.*
2. *If M has a least element $\bot$ then $f(\bot) = \bot$.*

3. *If M is an upper semilattice then $f(f(x) \sqcup f(y)) = f(x) \sqcup f(y)$, i.e., $f(M)$ is closed under $\sqcup$.*

Proof.
1. By Cor. 1.2.13 and isotony, $f(x)$ is an upper bound of $N =_{df} \{y \in f(M) : y \leq x\}$. But $f(x) \in N$, since $f(x) \leq x$ by contractivity of f, and so $f(x)$ is the supremum of N.
2. Immediate from contractivity of f.
3. ($\leq$) follows by contractivity of f.
   ($\geq$) By isotony and idempotence of f,
$$f(f(x) \sqcup f(y)) \geq f(f(x)) \sqcup f(f(y)) = f(x) \sqcup f(y) \ .$$

□

Lemma 1.2.15 *For a kernel operator $f : M \to M$ the following two statements are equivalent:*
1. *$f(M)$ is downward closed, i.e., $x \in f(M) \wedge y \leq x \Rightarrow y \in f(M)$.*
2. *For all $x, y \in M$ such that $x \sqcap y$ exists, also $f(x) \sqcap y$ and $f(x) \sqcap f(y)$ exist and $f(x \sqcap y) = f(x) \sqcap y = f(x) \sqcap f(y)$.*

Proof. First we show that the first equation in Part 2 implies the second one. Assume $f(x \sqcap y) = f(x) \sqcap y$ for all x, y such that $x \sqcap y$ exists. By idempotence of f we get, using this assumption twice and commutativity of $\sqcap$,
$$f(x \sqcap y) = f(f(x \sqcap y)) = f(f(x) \sqcap y) = f(x) \sqcap f(y) \ .$$
(Part 1 $\Rightarrow$ Part 2) Isotony and contractivity of f imply $f(x \sqcap y) \leq f(x)$ and $f(x \sqcap y) \leq f(y) \leq y$, so that $f(x \sqcap y)$ is a lower bound of $f(x)$ and y. Consider an arbitrary lower bound z of $f(x)$ and y. By the assumed downward closure of $f(M)$ also $z \in f(M)$, hence $z = f(z)$ y Cor. 1.2.13. Moreover, $z \leq f(x) \leq x$ by contractivity of f. Therefore $z \leq x \sqcap y$ and hence $z = f(z) \leq f(x \sqcap y)$ by isotony of f, so that $f(x \sqcap y)$ is indeed the greatest lower bound of $f(x)$ and y.

(Part 2 $\Rightarrow$ Part 1) Consider an $x \in f(M)$ and $y \leq x$, i.e., $y = x \sqcap y$. Then by assumption and Cor. 1.2.13, $f(y) = f(x \sqcap y) = f(x) \sqcap y = x \sqcap y = y$ and hence $y \in f(M)$ as well. □

Corollary 1.2.16 *Suppose that $f : M \to M$ is a kernel operator and $f(M)$ is downward closed.*
1. *If $x, y \in M$ with $y \leq x$ then $f(y) = y \sqcap f(x)$.*
2. *If $f(M)$ has a greatest element z then for all $x \in M$ we have $f(x) = x \sqcap z$.*
3. *If M has a greatest element $\top$ then $f(x) = x \sqcap f(\top)$ for all $x \in M$.*

Proof.
1. Immediate from Lm. 1.2.15.2.
2. By contractivity, $f(x) \leq x$. Moreover, $f(x) \leq z$ by $f(x) \in f(M)$. Consider now an arbitrary lower bound y of x and z. By downward closure of $f(M)$ also $y \in f(M)$ and hence $y = f(y)$ by Cor. 1.2.13. But $f(y) \leq f(x)$ by isotony, so that $f(x)$ is indeed the greatest lower bound of x and z.

3. Immediate from Part 2, since by isotony $f(\top)$ is the greatest element of $f(M)$. □

1.3 Basic Algebraic Structures

Definition 1.3.1

1. A *groupoid* is a structure $(M, \circ)$ where $\circ : M \times M \to M$ is a total binary operator on M. The groupoid is *commutative* when $\circ$ is, i.e., when $a \circ b = b \circ a$.
2. If $\circ$ is *associative*, i.e., satisfies $a \circ (b \circ c) = (a \circ b) \circ c$, then the groupoid is called a *semigroup*. It is customary to leave reasoning steps using only associativity or commutativity tacit.
3. In a semigroup, the *powers* a^i of an element a with a positive natural number $i \in \mathbb{N}\backslash\{0\}$ as exponent are defined inductively as follows:
$$\begin{aligned} a^1 &=_{df} a \ , \\ a^{i+1} &=_{df} a \circ a^i \ . \end{aligned}$$
Note the tacit use of associativity in this definition. It entails that $a^i = \underbrace{a \circ \cdots \circ a}_{i}$.
4. A *monoid* is a structure $(M, \circ, e)$ such that $(M, \circ)$ is a semigroup and e is *left* and *right neutral* (or the *left* and *right unit* of $\circ$), i.e., satisfies
$$e \circ a = a = a \circ e \ .$$
The unit of a monoid is unique. In a monoid one can also define the 0th power by
$$a^0 =_{df} e \ .$$

The powers satisfy the customary laws:
$$a^{m+n} = a^m \circ a^n \ , \qquad (a^m)^n = a^{m \cdot n} \ .$$

1.4 Idempotent Left Semirings

Now we introduce our first fundamental algebraic structure that captures the essential control constructs of choice and sequential composition which are typical of almost all systems.

Definition 1.4.1 A *left (or lazy) semiring*, briefly an *L-semiring*, is a quintuple $(S, +, \cdot, 0, 1)$ with the following properties:

1. $(S, +, 0)$ is a commutative monoid.
2. $(S, \cdot, 1)$ is a monoid.

3. The operator $\cdot$ of *multiplication* or *composition* is *right-distributive* over $+$ and *left-strict*:
$$(a+b)\cdot c = a\cdot c + b\cdot c\ , \qquad 0\cdot a = 0\ .$$
As customary, $\cdot$ binds tighter than $+$.

By these axioms, every ring as known from classical algebra becomes an L-semiring when disregarding the ring subtraction and the axioms of left-distributivity and right-strictness.

In many contexts the L-semiring operators can be interpreted as follows:

$+$ $\leftrightarrow$ choice,
$\cdot$ $\leftrightarrow$ sequential composition,
0 $\leftrightarrow$ empty choice/abortion/blocking,
1 $\leftrightarrow$ identity/skip/no-operation program.

We view succession from left to right, i.e., $a\cdot b$ means "first perform a and then b".

For abbreviation we often refer to an L-semiring $(S,+,\cdot,0,1)$ just by S.

Definition 1.4.2 An *idempotent* left semiring, briefly *IL-semiring*, is an L-semiring $(S,+,\cdot,0,1)$ with the following additional requirements.

1. Addition is idempotent. Hence by Lm. 1.2.6 it induces an upper semilattice with the *natural order* $\leq$ given by $a\leq b \Leftrightarrow_{df} a+b=b$, which means that b offers at least all the choices of a but possibly more.
2. Multiplication is right-isotone w.r.t. the natural order. With the help of Lm. 1.2.9.2 this can be axiomatised as super-disjunctivity:
$$a\cdot b + a\cdot c \leq a\cdot(b+c)\ .$$

Let us briefly discuss the role of 0 in connection with choice. Since 0 stands for the empty choice, i.e., "blocking", the neutrality equations $0+x=x=x+0$ can be interpreted as follows: if one branch of the choice is recognised as blocking, the other branch is chosen. Informally: "if things can go on, they will". This means an optimistic or angelic view of choice.

The left strictness equation $0\cdot a = 0$ means that, for composition, blocking of the first part means blocking of the whole system.

The name *natural* order is explained by the following lemma.

Lemma 1.4.3 *Consider an IL-semiring.*

1. *The element* 0 *is the least element w.r.t. the natural order. In particular,* $a\leq 0$ *iff* $a=0$.
2. *Addition is* $\leq$*-isotone in both arguments.*
3. *Multiplication is* $\leq$*-isotone also in its left argument.*
4. *The natural order is the only partial order on* S *for which* 0 *is the least element and for which addition and multiplication are isotone in both arguments.*

Proof.

1. We have $0+a=a$, i.e., $0\leq a$.

2. This was shown in Lm. 1.2.9.3.
3. This follows from Lm. 1.2.9.2, since right-distributivity of multiplication means disjunctivity and hence super-disjunctivity in its left argument.
4. Let $\preceq$ be an order on S with the stated properties. We want to show that $\preceq$ and $\leq$ coincide.
   ($\subseteq$) Assume $a \preceq b$. Then isotony of $+$ w.r.t. $\preceq$ and idempotence of addition imply $a+b \preceq b+b = b$. On the other hand we have $b = 0+b \preceq a+b$, since 0 is least w.r.t. $\preceq$ and $+$ is $\preceq$-isotone. Altogether, antisymmetry of $\preceq$ entails $a+b = b$, i.e., $a \leq b$.
   ($\supseteq$) Assume $a \leq b$, i.e., $a+b = b$. As before we infer $a = a+0 \preceq a+b = b$, i.e., $a \preceq b$. □

In an IL-semiring, by Cor. 1.2.9 and isotony, $\cdot$ is universally super-disjunctive and universally sub-conjunctive in both arguments; we state these properties for the right argument:

$$a \cdot (\bigsqcup L) \geq \bigsqcup \{a \cdot l : l \in L\} \ , \qquad a \cdot (\bigsqcap L) \leq \bigsqcap \{a \cdot l : l \in L\} \ .$$

Definition 1.4.4

1. An element a of an IL-semiring is called *left-distributive* if, for all b, c,
   $$a \cdot (b + c) \ = \ a \cdot b + a \cdot c \ .$$
   It is called *positively/universally left-distributive* if for all non-empty/for all subsets $L \subseteq S$ it satisfies $a \cdot (\bigsqcup L) = \bigsqcup \{a \cdot l \ : \ l \in L\}$. The IL-semiring is called *(positively/universally) left-distributive* if all elements are (positively/universally) left-distributive.
2. An element a of an IL-semiring is called *right-strict* if $a \cdot 0 = 0$. The IL-semiring is called *right-strict* if all elements are right-strict, i.e., if 0 is a right annihilator as well. Note that a universally left-distributive IL-semiring is right-strict.
3. A left-distributive and right-strict IL-semiring is called an *I-semiring*.

Numerous examples of IL-semirings will be provided in the next section.

Definition 1.4.5

1. An IL-semiring is *bounded* if it has a greatest element $\top$ w.r.t. the natural order.
2. An IL-semiring S is called a *left quantale* if the semilattice $(S, \leq)$ is a complete lattice and $\cdot$ is universally right-distributive.
3. Finally, S is *Boolean* if $(S, \leq)$ is a *Boolean algebra*. Every Boolean IL-semiring is bounded.

Lemma 1.4.6 *In a bounded IL-semiring we have* $\top \cdot \top = \top$.

Proof. By neutrality of 1, greatestness of $\top$ and isotony of $\cdot$ we have $\top = \top \cdot 1 \leq \top \cdot \top$. The reverse inequation is trivial by greatestness of $\top$. □

Now we introduce symmetric notions w.r.t. the right argument of composition.

Definition 1.4.7

1. For a binary operator $\cdot : S \times S \to S$ we define its *mirror operator* (or *opposite operator*) $\cdot^{\mathrm{op}} : S \times S \to S$ by $x \cdot^{\mathrm{op}} y = y \cdot x$.
2. We call $(S, +, \cdot, 0, 1)$ an *(idempotent) right semiring* (briefly *(I)R-semiring*) if $(S, +, \cdot^{\mathrm{op}}, 0, 1)$ is an (I)L-semiring. The notions of a *right quantale* and *Boolean* (I)R-semiring are defined analogously.
3. A *quantale* [59] is a semiring that is both a left and right quantale. A quantale is called a *standard Kleene algebra* in [13].
4. Finally, *Boolean (I-)semirings* and *Boolean quantales* are defined analogously as in Def. 1.4.5.

This definition implies that S is an I-semiring iff it is both an IL-semiring and an IR-semiring.

1.5 Examples of IL-Semirings

Since IL-semirings are a very important class, we look in more detail at them. Examples 1.5.1 to 1.5.5 present some finite ones with at most four elements from Conway's book (cf. [13], p. 101). They will later be used as counterexamples. For each of them we show the Hasse diagram of the natural order and the composition tables for $+$ and $\cdot$.

Example 1.5.1 The structure $S_2 = (\{0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

is an I-semiring, called the *two-element Boolean semiring*. The operators $+$ and $\cdot$ play the roles of disjunction and conjunction. □

Example 1.5.2 The structure $S_3^1 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	a	1
0	0	a	1
a	a	a	a
1	1	a	1

$\cdot$	0	a	1
0	0	0	0
a	0	a	a
1	0	a	1

is an I-semiring. □

Example 1.5.3 The structure $S_3^2 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	a	1
0	0	a	1
a	a	a	1
1	1	1	1

$\cdot$	0	a	1
0	0	0	0
a	0	0	a
1	0	a	1

is an I-semiring. □

Example 1.5.4 The structure $S_3^3 = (\{a, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	a	1
0	0	a	1
a	a	a	1
1	1	1	1

$\cdot$	0	a	1
0	0	0	0
a	0	a	a
1	0	a	1

is an I-semiring. It is like S_3^2 except for the value of $a \cdot a$. □

Example 1.5.5 The structure $S_4^1 = (\{a, b, 0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by

$+$	0	a	1	b
0	0	a	1	b
a	a	a	1	b
1	1	1	1	b
b	b	b	b	b

$\cdot$	0	a	1	b
0	0	0	0	0
a	0	0	a	a
1	0	a	1	b
b	0	a	b	b

is an I-semiring. □

Example 1.5.6 Consider the structure $\mathsf{REL}(M) = (2^{M \times M}, \cup, ;, \emptyset, \Delta_M)$ over a set M, where $2^{M \times M}$ denotes the set of binary relations over M, $\cup$ denotes set union, ; denotes relational composition, $\emptyset$ denotes the empty relation and Δ_M denotes the identity relation $\{(a, a) \mid a \in M\}$. Then $\mathsf{REL}(M)$ is a Boolean quantale with set inclusion as the natural ordering. We call it the *relational* I-semiring over M.

A binary relation R can be viewed as describing a directed graph with node set M. There is an edge form node x to node y iff $x\, R\, y$. For the powers R^n w.r.t. relational composition as the iterated operator we have $x\, R^n\, y$ iff there is a path from x to y with exactly n edges. □

Example 1.5.7 Let $(S, +, \cdot, 0, 1)$ be a *semiring*, i.e., a structure with the same properties as an I-semiring except for idempotence of addition, and M be a finite set. Then the set $S^{M \times M}$ can be viewed as the set of $|M| \times |M|$ matrices with indices in M and elements in S. Now consider the structure $\mathsf{MAT}(M, S) = (S^{M \times M}, +, \cdot, \mathbf{0}, \mathbf{1})$, where $+$ and $\cdot$ are matrix addition and multiplication, and $\mathbf{0}$ and $\mathbf{1}$ are the zero and unit matrices. Then $\mathsf{MAT}(M, S)$ again forms a semiring, the *matrix semiring* over M and S. $\mathsf{MAT}(M, S)$ is idempotent if S is. In this case, the natural order is the componentwise extension of the order from S to matrices. If S is a (Boolean) quantale, then so is $\mathsf{MAT}(M, S)$.

If S is the two-element Boolean semiring S_2, this yields another representation of $\mathsf{REL}(M)$ as $\mathsf{MAT}(M, S)$ in terms of adjacency matrices, where relation composition is represented by matrix multiplication. □

Example 1.5.8 For every Boolean algebra B the structure $\mathsf{BOOL}(B) = (B, \sqcup, \sqcap, \bot, \top)$ is an I-semiring, called the *Boolean semiring* over B. □

Example 1.5.9 Let Σ^* be the set of finite words over some alphabet Σ and consider the structure $\mathsf{LAN}(\Sigma) = (2^{\Sigma^*}, \cup, ., \emptyset, \{\varepsilon\})$, where 2^{Σ^*} denotes the set of languages over Σ, and $\cup$ denotes set union, $L_1.L_2 = \{v.w \mid v \in L_1, w \in L_2\}$, where $v\,.\,w$ denotes concatenation of v and w, $\emptyset$ denotes the empty language and ε denotes the empty word. Then $\mathsf{LAN}(\Sigma)$ is a Boolean quantale, called the *language* I-semiring over Σ, and language inclusion is its natural ordering. □

Example 1.5.10 Using matrices over the language algebra we can also model labelled transition systems. Assume a set Q of states and a set Σ of labels. The matrices in $\mathsf{MAT}(Q, \mathsf{LAN}(\Sigma))$ record possible sequences of labels (traces) that connect two states. When there is no possible transition between two states, the corresponding matrix element is the empty language. □

Example 1.5.11 Set $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$ and define the operators min and $+$ in the obvious way. Then the structure $(\min, +) = (\mathbb{N}_\infty, \min, +, \infty, 0)$ is an I-semiring, called the *tropical semiring* [47]. Its natural ordering is the converse of the standard ordering on $\mathbb{N}_\infty$. □

Example 1.5.12 Consider similarly $\mathbb{N}_{-\infty} = \mathbb{N} \cup \{-\infty\}$ and the structure $(\max, +) = (\mathbb{N}_{-\infty}, \max, +, -\infty, 0)$ with operators defined in the obvious way. Then $(\max, +)$ is an I-semiring, called the *max-plus semiring* [28]. Its natural ordering coincides with the standard ordering on $\mathbb{N}_{-\infty}$. □

Example 1.5.13 A left semiring structure is also at the core of process algebra frameworks (see e.g. [7, 8]). One model of an IL-semiring is the set of equivalence classes of processes under simulation equivalence. The associated natural order is the relation of simulability, i.e., the union of all simulation relations [57, 63]. The role of 0 is played by the deadlock or inaction element δ (also called nil or $\mathtt{STOP}$). The neutral element 1 for multiplication is the empty process or termination constant ε (also called $\mathtt{SKIP}$). A more thorough comparison of the analogies and differences is beyond the scope of this book. □

Example 1.5.14 Consider a set Σ of vertices (or states). Then subsets of $\Sigma^+ =_{df} \Sigma^* - \{\varepsilon\}$ can be viewed as sets of possible graph paths (or state sequences in a transition system). The partial operator of the *fusion product* glues paths in Σ^+ together at a common point. It is, for all $s, t \in \Sigma^+$ and $x, y \in \Sigma$, defined as

$$(s.x) \bowtie (y.t) = \begin{cases} s.x.t & \text{if } x = y\ , \\ \text{undefined} & \text{otherwise}\ . \end{cases}$$

It is extended to subsets of Σ^+ by

$$S \bowtie T = \{s \bowtie t \mid s \in S \wedge t \in T \wedge s \bowtie t \text{ defined}\}\ .$$

Then $\mathsf{PAT}(\Sigma) = (2^{\Sigma^+}, \cup, \bowtie, \emptyset, \Sigma)$ is a Boolean quantale, called the *path I-semiring* over Σ. Note that Σ is the neutral element of $\bowtie$.

In this algebra a directed graph with node set Σ can be represented by a set R of paths with exactly two nodes. A power R^n w.r.t. the fusion product $\bowtie$ as the iterated operator consists of all paths that use exactly n edges from R. □

Example 1.5.15 A *guarded string* over arbitrary sets Σ of *states* and T of *transitions* is a non-empty word ρ over $\Sigma \cup T$ such that the first element of ρ is in Σ and in which elements from Σ and T alternate. Moreover, if ρ is finite, its last element, too, has to be in Σ. Guarded strings are used in the context of labelled transition systems [2] and for the abstract interpretation of program schemes [39].

The set $(\Sigma \,.\, T)^* \,.\, \Sigma \cup (\Sigma \,.\, T)^\omega$ of all guarded strings over Σ and T is denoted by $\mathsf{GS}(\Sigma, T)$; the set $\mathsf{fin}\,\mathsf{GS}(\Sigma, T) = (\Sigma \,.\, T)^* \,.\, \Sigma$ denotes the set of all finite guarded strings.

The product of guarded strings ρ_0 and ρ_1 is simply $\rho_0 \bowtie \rho_1$ with $\bowtie$ as in Ex. 1.5.14. If defined it is a guarded string again.

The power set algebra $\mathsf{GRS}(\Sigma, T) =_{df} (\mathcal{P}(\mathsf{GS}(\Sigma, T)), \cup, \bowtie, \emptyset, \Sigma)$ with multiplication as in Ex. 1.5.18 is a left-distributive Boolean left quantale. The algebra $\mathsf{FGRS}(\Sigma, T) =_{df} \mathcal{P}(\mathsf{fin}\,\mathsf{GS}(\Sigma, T)), \cup, \bowtie, \emptyset, \Sigma)$ of sets of finite guarded strings forms a Boolean subquantale of it. □

To prepare the next examples, in addition to the set Σ^* of all finite words over Σ we consider the set Σ^ω of all infinite words over Σ. We set $\Sigma^\infty =_{df} \Sigma^* \cup \Sigma^\omega$ and extend concatenation by setting $s.t =_{df} s$ if $s \in \Sigma^\omega$.

Definition 1.5.16 A *(generalised) language* over Σ is a subset of Σ^∞. The *purely infinite* and *purely finite* parts of a language $U \subseteq \Sigma^\infty$ are defined by

$$\mathsf{inf}\, U =_{df} U \cap \Sigma^\omega, \qquad \mathsf{fin}\, U =_{df} U - \mathsf{inf}\, U \;.$$

By Boolean algebra the operators fin and inf distribute through arbitrary unions.

Our first algebra of finite and infinite words is based on concatenation as multiplication.

Example 1.5.17 A Boolean left quantale $\mathsf{WOR}(\Sigma) = (\mathcal{P}(\Sigma^\infty), \cup, \cdot, \emptyset, \{\varepsilon\})$ is obtained by extending concatenation to languages in the following way:

$$U \cdot V =_{df} \mathsf{inf}\, U \cup (\mathsf{fin}\, U) \,.\, V \;.$$

Note that in general $U \cdot V \neq U.V$; for $V = \emptyset$ one has $U.V = \emptyset$, whereas $U \cdot V = \mathsf{inf}\, U$. Using distributivity of fin and inf it is straightforward to show that $\mathsf{WOR}(\Sigma)$ is indeed a left quantale which is even positively left-distributive (the proof is analogous to the one given in Ex. 1.5.18 below). This algebra is well known from the classical theory of ω-languages (see e.g. [61] for a survey). □

Besides this algebra we use a second one with a more refined view of multiplication. It generalises the algebra $\mathsf{PAT}(\Sigma)$ from Ex. 1.5.14 analogously as $\mathsf{WOR}(\Sigma)$ generalises $\mathsf{LAN}(\Sigma)$.

Example 1.5.18 When the elements of an alphabet Σ are interpreted as states, finite and infinite paths over Σ are often called *computation streams*. Therefore we define the Boolean left quantale $\mathsf{STR}(\Sigma)$ of sets of finite and infinite computation streams by $\mathsf{STR}(\Sigma) =_{df} (\mathcal{P}(\Sigma^\infty - \{\varepsilon\}), \cup, \bowtie, \emptyset, \Sigma)$, where $\bowtie$ is extended to languages in the following way:

$$U \bowtie V =_{df} \mathsf{inf}\, U \cup \{s \bowtie t : s \in \mathsf{fin}\, U \wedge t \in V\} .$$

This operator has the language Σ as its neutral element. Moreover, as in Example 1.5.17, we have $U \bowtie \emptyset = \mathsf{inf}\, U$ and hence $U \bowtie \emptyset = \emptyset$ iff $\mathsf{inf}\, U = \emptyset$.

We show now that this left quantale is even positively left-distributive.

Consider $\mathcal{W} \subseteq \mathsf{STR}(\Sigma)$ with $V =_{df} \bigcup \mathcal{W} \neq \emptyset$ and $U \in \mathsf{STR}(\Sigma)$. When $U = \emptyset$ then $U \bowtie V = \emptyset = \bigcup\{U \bowtie W \mid W \in \mathcal{W}\}$. Otherwise,

$$\begin{array}{lll}
& u \in U \bowtie V & \\
\Leftrightarrow & \exists\, v \in U : \exists\, W \in \mathcal{W} : \exists\, w \in W : u = v \bowtie w & \{\!\![\,\text{definitions}\,]\!\!\} \\
\Leftrightarrow & \exists\, W \in \mathcal{W} : \exists\, v \in U : \exists\, w \in W : u = v \bowtie w & \{\!\![\,\text{commuting quantifiers}\,]\!\!\} \\
\Leftrightarrow & \exists\, W \in \mathcal{W} : u \in U \bowtie W & \{\!\![\,\text{definition}\,]\!\!\} \\
\Leftrightarrow & u \in \bigcup\{U \bowtie W \mid W \in \mathcal{W}\} . & \{\!\![\,\text{definition}\,]\!\!\}
\end{array}$$

□

Chapter 2
Tests, Domain and Modal Operators

I didn't fail the test, I just found 100 ways to do it wrong.
— Benjamin Franklin

2.1 Tests

Tests are the algebraic representation of assertions in programs. A statement `assert` p, as for instance known from certain macro libraries for the programming language `C`, acts as the identity on all program states that satisfy p and abortion-like on all others. Therefore it seems reasonable to model tests algebraically by certain elements below 1, the representation of "do nothing". Based on this idea one can then introduce a domain operator which for a transition element characterises all its starting states; in the case of transition relations it coincides with the classical notion of the domain of a relation.

The idea of tests as complemented sub-identities and the notion of domain date back at least to [49]. With the above definition of tests we deviate slightly from [44], in that we do not allow an arbitrary Boolean algebra of sub-identities as $\mathsf{test}(S)$ but only the maximal complemented one. The reason is that our axiomatisation of the domain operator forces this maximality anyway (see [18] and Th. 2.4.6.1 and 2.4.6.8).

Definition 2.1.1 A *test* in an IL-semiring is an element p that has a *complement* q relative to 1, i.e., $p + q = 1$ and $p \cdot q = 0 = q \cdot p$. In particular, 0 and 1 are tests. By the requirement $p + q = 1$ every test is a *sub-identity*, i.e., satisfies $p \leq 1$. The set of all tests of an IL-semiring S is denoted by $\mathsf{test}(S)$. An IL-semiring is *test-discrete* if $\mathsf{test}(S) = \{0, 1\}$. We will consistently write $a, b, c \ldots$ for arbitrary semiring elements and $p, q, r, \ldots$ for tests. In Th. 2.1.8.3 we show that a complement of p is unique if it exists; therefore we will denote it by $\neg p$. We will also use relative complement $p - q =_{df} p \cdot \neg q$ and implication $p \to q =_{df} \neg p + q$.

Before proving essential properties of tests we give some examples. Note that Conway's algebras from Sect. 1.5 (that is, Ex. 1.5.1 to Ex. 1.5.5) are all test-discrete and therefore not very interesting.

Example 2.1.2 In the relational semiring $\mathsf{REL}(M)$ from Ex. 1.5.6, all sub-relations $P, Q \subseteq \Delta_M$ satisfy $P\,;Q = P \cap Q$. Therefore every such P is a test with $\neg P = \Delta_M \backslash P$, where $\backslash$ denotes set-theoretic difference.

We note that the tests in the relational semiring are called *monotypes* in [5] and further work by these authors, but are not axiomatised algebraically there. □

Example 2.1.3 In the Boolean semiring semiring $\mathsf{BOOL}(B)$ from Ex. 1.5.8 we have $1 = \top$, and hence *every* element is a test, i.e., $\mathsf{test}(\mathsf{BOOL}(B)) = B$. □

Example 2.1.4 In the language semirings $\mathsf{LAN}(\Sigma)$ from Ex. 1.5.9 and $\mathsf{WOR}(\Sigma)$ from Ex. 1.5.17, the only sub-identities are $\emptyset$ and $\{\varepsilon\}$; hence $\mathsf{LAN}(\Sigma)$ and $\mathsf{WOR}(\Sigma)$ are always test-discrete. □

Example 2.1.5 In the path IL-semirings $\mathsf{PAT}(\Sigma)$ from Ex. 1.5.14 and $\mathsf{STR}(\Sigma)$ from Ex. 1.5.18, a sub-identity $P \subseteq \Sigma$ models a set of nodes or states. □

Example 2.1.6 In the tropical semiring from Ex. 1.5.11, all elements are sub-identities. However, except for 0 and ∞, they do not have complements, since the product $m+n$ of non-0 elements m, n always is non-0 again. Thus the only possible test algebra consists of the elements 0 and ∞ and the tropical semiring is test-discrete. □

Example 2.1.7 In the max-plus semiring from Ex. 1.5.12, the only multiplicatively idempotent sub-identities are $-\infty$ and 0. These two elements also are the only tests, so that the max-plus semiring is test-discrete. □

We show a number of important properties of tests, among others that the tests almost form a Boolean algebra.

Theorem 2.1.8 *Let $p, q, r \in \mathsf{test}(S)$ for an IL-semiring S.*

1. *For arbitrary $a \in S$ we have $p \cdot a \leq a$ and $a \cdot p \leq a$.*
2. *If $s \in S$ is a complement of $t \in S$, then t is a complement of s and s is a test.*
3. *The complement of p is unique; we denote it by $\neg p$.*
4. *$\neg p$ is a test with $\neg\neg p = p$.*
5. *0 and 1 are tests with $\neg 0 = 1$ and $\neg 1 = 0$.*
6. *Multiplication is idempotent on $\mathsf{test}(S)$, i.e., $p \cdot p = p$.*
7. *Multiplication is commutative on $\mathsf{test}(S)$. In particular, 0 is a right annihilator for tests.*
8. *We have the absorption laws*
$$p + p \cdot q = p\ , \quad p + q \cdot p = p\ , \quad p \cdot (p + q) = p\ , \quad (p + q) \cdot p = p\ .$$
9. *The following laws hold:*
$$p + \neg p \cdot q = p + q\ , \qquad p + q \cdot \neg p = p + q\ ,$$
$$(\neg p + q) \cdot p = q \cdot p\ , \qquad (\neg p + q) \cdot p = p \cdot q\ .$$
However, $p \cdot (\neg p + q) = p \cdot q$ does not.

10. *We have* $r \leq p \cdot q \;\Leftrightarrow\; r \leq p \wedge r \leq q$. *Hence if* $p \cdot q$ *is a test it is the infimum of* p *and* q *in* $\mathsf{test}(S)$.
11. *We have the* shunting rule *(a generalisation of contraposition):*
$$p \cdot q \leq a \;\Leftrightarrow\; p \leq \neg q + a \ .$$
In particular, setting $a = 0$ *and replacing* q *by* $\neg q$*, we get*
$$p \leq q \;\Leftrightarrow\; p \cdot \neg q \leq 0 \ .$$
Moreover, the operator $\neg$ *is antitone:* $p \leq q \;\Leftrightarrow\; \neg q \leq \neg p$.
12. *De Morgan's laws hold partially:*
$$(p + q) + (\neg p \cdot \neg q) = 1 \quad \textit{and} \quad (p + q) \cdot (\neg p \cdot \neg q) = 0 \ .$$
However, generally $(\neg p \cdot \neg q) \cdot (p + q) \neq 0$.
13. *If* $p \cdot q$ *is a test then* $\neg(p \cdot q) = \neg p + \neg q$.
If $p + q$ *is a test then* $\neg(p + q) = \neg p \cdot \neg q$.
14. *The following four assertions are equivalent:*
(*a*) $\mathsf{test}(S)$ *is closed under* $+$,
(*b*) $\mathsf{test}(S)$ *is closed under* $\cdot$,
(*c*) $\forall\, p, q \in \mathsf{test}(S) : p \cdot (\neg p + q) = p \cdot q$,
(*d*) $\forall\, p, q \in \mathsf{test}(S) : \neg p \cdot \neg q \cdot (p + q) = 0$.

Proof.

1. By isotony of multiplication and neutrality of 1,
$$p \cdot a \leq 1 \cdot a = a \ .$$
The second claim is shown symmetrically.
2. The conditions for the complement are symmetric in t and s. Therefore t is a complement of s and so s is a test.
3. Let q and r be complements of p, i.e., assume
$$\begin{aligned} p + q &= 1 \ , & p + r &= 1 \ , \\ p \cdot q &= 0 = q \cdot p \ , & p \cdot r &= 0 = r \cdot p \ . \end{aligned}$$
We have to show $q = r$. We calculate, using neutrality of 1, r being a complement of p, right-distributivity, q being a complement of p, neutrality of 0 and Part 1,
$$q = 1 \cdot q = (p + r) \cdot q = p \cdot q + r \cdot q = 0 + r \cdot q = r \cdot q \leq r \ .$$
Symmetrically we obtain $r \leq q$. Now antisymmetry of $\leq$ implies $q = r$.
4. By Part 2, p is a complement of $\neg p$ and so is $\neg\neg p$. Part 3 shows $\neg\neg p = p$.
5. We only need to check the complement conditions. By neutrality of 0 and 1 w.r.t. $+$ and $\cdot$ we have
$$0 + 1 = 1 \qquad 0 \cdot 1 = 0 = 1 \cdot 0$$
6. We use neutrality of 1, the first complement condition, right-distributivity, the second complement condition and neutrality of 0:
$$p = 1 \cdot p = (p + \neg p) \cdot p = p \cdot p + \neg p \cdot p = p \cdot p + 0 = p \cdot p \ .$$
7. By neutrality of 1, the first complement condition and right-distributivity,
$$p \cdot q = 1 \cdot p \cdot q = (q + \neg q) \cdot p \cdot q = q \cdot p \cdot q + \neg q \cdot p \cdot q \ .$$
By Part 1, isotony, the second complement condition and neutrality of 0,
$$q \cdot p \cdot q + \neg q \cdot p \cdot q \leq q \cdot p + \neg q \cdot q = q \cdot p + 0 = q \cdot p \ .$$
This shows $p \cdot q \leq q \cdot p$; the reverse inequation follows symmetrically.

8. The first two laws are, by definition of $\leq$, equivalent to $p \cdot q \leq p$ and $q \cdot p \leq p$, which hold by Part 1. For the third absorption law, using super-disjunctivity, Part 6 and the first absorption law, we obtain
$$p \cdot (p + q) \geq p \cdot p + p \cdot q = p + p \cdot q = p \ .$$
Conversely, by $p \leq 1$ (cf. Def. 2.1.1), isotony, idempotence of $+$ and neutrality of 1,
$$p \cdot (p + q) \leq p \cdot (1 + 1) = p \cdot 1 = p \ .$$
For the fourth absorption law, we calculate, using right-distributivity, Part 6 and the second absorption law,
$$(p + q) \cdot p = p \cdot p + q \cdot p = p + q \cdot p = p \ .$$
9. For the first law we calculate, using idempotence of $+$, neutrality of 1 and the definition of complement, right-distributivity, commutativity of $+$ and commutativity of $\cdot$ on tests (see Part 7), Part 8 and right distributivity and finally the definition of complement and neutrality of 1,
$$\begin{aligned} p + \neg p \cdot q &= p + p + \neg p \cdot q = p + (q + \neg q) \cdot p + \neg p \cdot q \\ &= p + q \cdot p + \neg q \cdot p + \neg p \cdot q = p + \neg q \cdot p + p \cdot q + \neg p \cdot q \\ &= p + (p + \neg p) \cdot q = p + q \ . \end{aligned}$$
The second law follows from the first by commutativity of $\cdot$ on tests (Part 7). The third law is proved by using right-distributivity, the definition of complementation and neutrality of 0:
$$(\neg p + q) \cdot p = \neg p \cdot p + q \cdot p = q \cdot p \ .$$
The fourth law follows from the third by commutativity of $\cdot$ on tests (Part 7).
A counterexample to $p \cdot (\neg p + q) = p \cdot q$ is given after the proof of this theorem.
10. ($\Rightarrow$) By Part 1, $p \cdot q \leq p \wedge p \cdot q \leq q$, and transitivity of $\leq$ shows the claim.
($\Leftarrow$) By Part 6 and isotony of $\cdot$ we obtain $r = r \cdot r \leq p \cdot q$.
11. ($\Rightarrow$) By Part 7 the assumption is equivalent to $q \cdot p \leq a$. Hence, using neutrality of 1, the first complement condition, right-distributivity, Part 1 and the assumption, we calculate
$$p = (\neg q + q) \cdot p = \neg q \cdot p + q \cdot p \leq \neg q + q \cdot p \leq \neg q + a \ .$$
($\Leftarrow$) Multiplying the assumption from the right by q we obtain, by isotony, right-distributivity, the second complement condition, neutrality of 0 and Part 1,
$$p \cdot q \leq (\neg q + a) \cdot q = \neg q \cdot q + a \cdot q = 0 + a \cdot q = a \cdot q \leq a \ .$$
Setting now $a = 0$ and replacing q by $\neg q$ we obtain the second claim using Part 4. From that, antitony of $\neg$ follows using Parts 7 and 4:
$$p \leq q \ \Leftrightarrow \ p \cdot \neg q \leq 0 \ \Leftrightarrow \ \neg q \cdot p \leq 0 \ \Leftrightarrow \ \neg q \leq \neg p \ .$$
12. For the first claim we calculate, using the definition of complement, neutrality of 1 and the definition of complement, right-distributivity, commutativity of $+$ and Part 9,

$$1 = q + \neg q = q + (p + \neg p) \cdot \neg q = q + p \cdot \neg q + \neg p \cdot \neg q$$
$$= p \cdot \neg q + q + \neg p \cdot \neg q = p + q + \neg p \cdot \neg q \ .$$

The second claim follows by the third law of Part 9 with p replaced by $\neg p$, double negation (Part 4), commutativity of $\cdot$ on tests (Part 7), the definition of complementation and left strictness of $\cdot$:

$$(p + q) \cdot \neg p \cdot \neg q = q \cdot \neg p \cdot \neg q = q \cdot \neg q \cdot \neg p = 0 \cdot \neg p = 0 \ .$$

A counterexample to $(\neg p \cdot \neg q) \cdot (p + q) = 0$ is given after the proof of this theorem.

13. First, by Part 1 and antitony of $\neg$ (Part 11) we have $\neg p \leq \neg(p \cdot q)$ and $\neg q \leq \neg(p \cdot q)$, hence $\neg p + \neg q \leq \neg(p \cdot q)$. For the reverse inequation, we obtain By Part 11, Part 7, Part 11 with Part 4, commutativity of $+$ and Part 11, and reflexivity of $\leq$:

$$\neg(p \cdot q) \leq \neg p + \neg q \Leftrightarrow \neg(p \cdot q) \cdot p \leq \neg q \Leftrightarrow p \cdot \neg(p \cdot q) \leq \neg q$$
$$\Leftrightarrow p \leq p \cdot q + \neg q \Leftrightarrow p \cdot q \leq p \cdot q \Leftrightarrow \mathsf{TRUE} \ .$$

The proof of the second property is similar. From $p \leq p+q$, $q \leq p+q$ and antitony of $\neg$ (Part 11) we have $\neg(p + q) \leq \neg p$ and $\neg(p + q) \leq \neg q$. Since $p+q$ is a test by assumption, Parts 4 and 6 with isotony of $\cdot$ and antitony of $\neg$ yield $\neg(p+q) = \neg(p+q) \cdot \neg(p+q) \leq \neg p \cdot \neg q$. The reverse inequation follows be applying the identity of 1 and both shunting (Part 11) and double negation (Part 4) twice:

$$\neg p \cdot \neg q \leq \neg(p + q) \ \Leftrightarrow \ 1 \cdot \neg p \leq q + \neg(p + q) \ \Leftrightarrow \ 1 \leq p + q + \neg(p + q) \ ,$$

which holds by the definition of complements.

14. (a) $\Rightarrow$ (c) holds by Parts 7 and 9.
(c) $\Rightarrow$ (b): By Part 7, assumption (c), isotony and the definition of complement we obtain

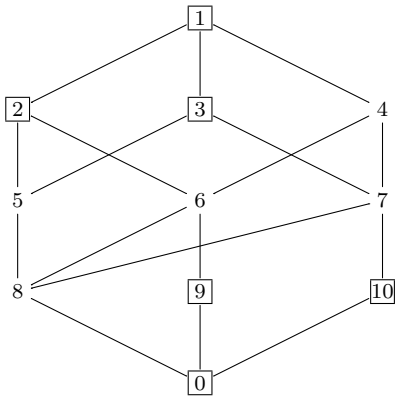
$$p \cdot q \cdot (\neg p + \neg q) = q \cdot p \cdot (\neg p + \neg q) = q \cdot p \cdot \neg q \leq q \cdot \neg q = 0 \ .$$

Together with Parts 4 and 12 this shows that $\neg p + \neg q$ is a complement of $p \cdot q$, so that $p \cdot q \in \mathsf{test}(S)$.
(b) $\Rightarrow$ (d): By Part 4, assumption (b) and Part 13 $\neg p \cdot \neg q$ is a test with complement $p+q$, so that the definition of complements shows the claim.
(d) $\Rightarrow$ (a): The assumption (d) with Part 12 shows that $p + q$ has a complement and so is a test. □

Example 2.1.9 We now present the announced counterexample. Fig. 2.1 contains the definition of an IL-semiring that is not an I-semiring.

The IL-semiring contains 11 elements, numbered 0 to 10. The operators are given by the tables, while the graph displays the natural ordering on the elements. The set of tests is $\{0, 1, 2, 3, 9, 10\}$ (the square nodes in the graph). This IL-semiring provides counterexamples to the four equivalent properties of Th. 2.1.8.14:

- $9 + 10 = 4$ shows that $p + q$ need not be a test,
- $2 \cdot 3 = 5$ shows that $p \cdot q$ need not be a test,



$\leq$	0	1	2	3	4	5	6	7	8	9	10
0	1	1	1	1	1	1	1	1	1	1	1
1	0	1	0	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0	0
3	0	1	0	1	0	0	0	0	0	0	0
4	0	1	0	0	1	0	0	0	0	0	0
5	0	1	1	1	0	1	0	0	0	0	0
6	0	1	1	0	1	0	1	0	0	0	0
7	0	1	0	1	1	0	0	1	0	0	0
8	0	1	1	1	1	1	1	1	1	0	0
9	0	1	1	0	1	0	1	0	0	1	0
10	0	1	0	1	1	0	0	1	0	0	1

$\neg$	
0	1
1	0
2	10
3	9
4	0
5	0
6	0
7	0
8	0
9	3
10	2

$+$	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	2	1	2	1	1	2	2	1	2	2	1
3	3	1	1	3	1	3	1	3	3	1	3
4	4	1	1	1	4	1	4	4	4	4	4
5	5	1	2	3	1	5	2	3	5	2	3
6	6	1	2	1	4	2	6	4	6	6	4
7	7	1	1	3	4	3	4	7	7	4	7
8	8	1	2	3	4	5	6	7	8	6	7
9	9	1	2	1	4	2	6	4	6	9	4
10	10	1	1	3	4	3	4	7	7	4	10

$\cdot$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	2	5	6	5	6	8	8	9	0
3	0	3	5	3	7	5	8	7	8	0	10
4	0	4	9	10	4	0	9	10	0	9	10
5	0	5	5	5	8	5	8	8	8	0	0
6	0	6	9	0	6	0	9	0	0	9	0
7	0	7	0	10	7	0	0	10	0	0	10
8	0	8	0	0	8	0	0	0	0	0	0
9	0	9	9	0	9	0	9	0	0	9	0
10	0	10	0	10	10	0	0	10	0	0	10

Fig. 2.1 An IL-semiring with 11 elements that is not an I-semiring.

- $3{\cdot}(\neg 3{+}10) = 3{\cdot}(9{+}10) = 3{\cdot}4 = 7 \neq 10 = 3{\cdot}10$ shows that $p{\cdot}(\neg p{+}q) = p{\cdot}q$ does not hold,
- $\neg 9 \cdot \neg 10 \cdot (9 + 10) = 3 \cdot 2 \cdot 4 = 5 \cdot 4 = 8 \neq 0$ show that $\neg p \cdot \neg q \cdot (p + q) = 0$ does not hold.

This counterexample was the smallest one generated by Mace4. Assuming completeness of Mace4 this means that there is no smaller counterexample. □

2.2 Restriction

Let now semiring element a describe an action or abstract program and test p a proposition or assertion on states. Remember that we view computations as proceeding from left to right. Therefore $p \cdot a$ describes a *restricted* program that acts like a when the initial state satisfies p and aborts otherwise. Symmetrically, $a \cdot p$ describes a *restriction* of a in its possible final states. We show some helpful properties about restriction originating from [52].

Lemma 2.2.1 *Assume an IL-semiring S. Then for all $a, b, c \in S$ and all $p, q \in \mathsf{test}(S)$ the following properties hold.*

1. *If S is left-distributive and $p \cdot q = 0$ then*
$$p \cdot a \leq q \cdot b + c \Leftrightarrow p \cdot a \leq c \ .$$
2. *If $a \sqcap b$ exists then $p \cdot (a \sqcap b) = p \cdot a \sqcap b = p \cdot a \sqcap p \cdot b$.*
3. *$p \cdot q \cdot a = p \cdot a \sqcap q \cdot a$.*
4. *$p \cdot q = 0 \Rightarrow p \cdot a \sqcap q \cdot a = 0$.*
5. *If $b \leq a$ then $p \cdot b = p \cdot a \sqcap b$.*

Assume now that S is bounded.

6. *$p \cdot b = b \sqcap p \cdot \top$. In particular, $p = 1 \sqcap p \cdot \top$.*
7. *$\neg p \cdot \top$ is a complement of $p \cdot \top$ w.r.t. $\top$ in S, i.e.,*
$$p \cdot \top + \neg p \cdot \top = \top \qquad \text{and} \qquad p \cdot \top \sqcap \neg p \cdot \top = 0 \ .$$
8. *$p \leq q \Leftrightarrow p \cdot \top \leq q \cdot \top$.*

Proof.

1. ($\Rightarrow$) $p \cdot a = p \cdot p \cdot a \leq p \cdot (q \cdot b + c) = p \cdot q \cdot b + p \cdot c = 0 + p \cdot c \leq c$.
($\Leftarrow$) $p \cdot a \leq c \leq q \cdot b + c$.
2. The function $f_p(a) =_{df} p \cdot a$ is, by $p \leq 1$ and $p \cdot p = p$ a kernel operator. Moreover, $f_p(S)$ is downward closed:
$$b \leq p \cdot a \ \Rightarrow \ \neg p \cdot b \leq \neg p \cdot p \cdot a = 0 \cdot a = 0 \ .$$
Hence
$$b = (p + \neg p) \cdot b = p \cdot b + \neg p \cdot b = p \cdot b + 0 = p \cdot b \in f(S) \ .$$
Therefore Lm. 1.2.15.2 shows the claim.
3. Employ that $a \sqcap a = a$ and use Part 2 with $b = a$:
$$p \cdot q \cdot a = p \cdot q \cdot (a \sqcap a) = p \cdot (q \cdot a \sqcap a) = p \cdot (a \sqcap q \cdot a) = p \cdot a \sqcap q \cdot a \ .$$
4. Immediate from Part 3.
5. Since $b \leq a$ the meet $a \sqcap b$ exists and equals b. Now Part 2 shows the claim.
6. For the first claim substitute $\top$ for a in Part 5. For the second claim substitute 1 for b in the first claim.
7. By right distributivity, definition of $\neg$ and neutrality of 1 we have
$$p \cdot \top + \neg p \cdot \top = (p + \neg p) \cdot \top = 1 \cdot \top = \top \ .$$
By Part 3, definition of $\neg$ and since 0 is a left annihilator, we have
$$p \cdot \top \sqcap \neg p \cdot \top = p \cdot \neg p \cdot \top = 0 \cdot \top = 0 \ .$$
8. ($\Rightarrow$) Immediate from isotony of $\cdot$.
($\Leftarrow$) Assume $p \cdot \top \leq q \cdot \top$. Then by Part 6 and isotony we have
$$p = 1 \sqcap p \cdot \top \leq 1 \sqcap q \cdot \top = q \ .$$

□

The properties listed in this lemma can be shown to hold more generally for certain kernel operators, i.e., isotone, contractive and idempotent operators (see Sect. 1.2.3). The operator $a \mapsto p \cdot a$ for a fixed test p is such an operator.

Corollary 2.2.2 *Assume an I-semiring S such that $\mathsf{test}(S)$ is a Boolean algebra and consider an arbitrary element $a \in S$. Then the set $R =_{df} \{p \cdot a \mid p \in \mathsf{test}(S)\}$ again forms a Boolean algebra, where the infimum of $p \cdot a$ and $q \cdot a$ is $p \cdot q \cdot a$, the supremum of $p \cdot a$ and $q \cdot a$ is $(p+q) \cdot a$ and the complement of $p \cdot a$ is $\neg p \cdot a$.*

Proof. This follows from Lm. 1.2.10 by choosing $f : \mathsf{test}(S) \to S$ as $f(p) =_{df} p \cdot a$. Then $f(\mathsf{test}(S)) = R$, and Lm. 2.2.1.3 shows that f preserves binary infima. Moreover, by I-semiring distributivity f also preserves binary suprema and we are done. □

The following lemma collects some properties of tests that will be helpful for deriving the laws of the modal operators introduced in Sect. 2.8.

Lemma 2.2.3 *In an IL-semiring S with $a \in S$ and $p, q \in \mathsf{test}(S)$, consider the properties*

(1) $p \cdot a \leq a \cdot q$, (2) $a \cdot \neg q \leq \neg p \cdot a$, (3) $p \cdot a \cdot \neg q \leq 0$, (4) $p \cdot a = p \cdot a \cdot q$.

Then we have the following table of implications, where $\Rightarrow$ and $\Leftrightarrow$ mean implication for arbitrary IL-semiring element a and test p, $\underset{\text{LD}}{\Rightarrow}$ means implication provided $p \cdot a$ is left-distributive and $\underset{\text{RS}}{\Rightarrow}$ means implication provided a is right-strict.

	(1)	(2)	(3)	(4)
(1)	$\Leftrightarrow$	$\underset{\text{RS}}{\Rightarrow}$	$\underset{\text{RS}}{\Rightarrow}$	$\Leftrightarrow$
(2)	$\underset{\text{LD}}{\Rightarrow}$	$\Leftrightarrow$	$\Leftrightarrow$	$\underset{\text{LD}}{\Rightarrow}$
(3)	$\underset{\text{LD}}{\Rightarrow}$	$\Leftrightarrow$	$\Leftrightarrow$	$\underset{\text{LD}}{\Rightarrow}$
(4)	$\Leftrightarrow$	$\underset{\text{RS}}{\Rightarrow}$	$\underset{\text{RS}}{\Rightarrow}$	$\Leftrightarrow$

In particular, if $p \cdot a$ is left-distributive and a is right-strict, which holds in all I-semirings, all four properties are equivalent.

Proof. We first show some of the implications of the table.
(1)$\underset{\text{RS}}{\Rightarrow}$(3): By isotony, definition of complement and right-strictness,

$$p \cdot a \leq a \cdot q \;\Rightarrow\; p \cdot a \cdot \neg q \leq a \cdot q \cdot \neg q = a \cdot 0 = 0 \ .$$

(2)$\underset{\text{LD}}{\Rightarrow}$(1): By neutrality of 1, definition of complement, left distributivity of $p \cdot a$, assumption (2), isotony, definition of complement again, left-strictness and neutrality of 0,

$$\begin{aligned} p \cdot a = p \cdot a \cdot 1 = p \cdot a \cdot (q + \neg q) = p \cdot a \cdot q + p \cdot a \cdot \neg q \\ \leq a \cdot q + p \cdot \neg p \cdot a = a \cdot q + 0 \cdot a = a \cdot q + 0 = a \cdot q \ . \end{aligned}$$

(1) $\Rightarrow$ (4): The inequality $p \cdot a \cdot q \leq p \cdot a$ is direct by isotony. The other inequality follows by isotony and idempotence of $\cdot$ for tests:

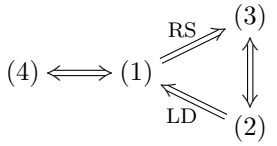
$$p \cdot a \leq a \cdot q \;\Rightarrow\; p \cdot p \cdot a \leq p \cdot a \cdot q \;\Leftrightarrow\; p \cdot a \leq p \cdot a \cdot q \ .$$

(4) $\Rightarrow$ (1): $p \cdot a = p \cdot a \cdot q \leq a \cdot q$.

(2) ⇒ (3): $p \cdot a \cdot \neg q \leq p \cdot \neg p \cdot a = 0 \cdot a = 0$.
(3) ⇒ (2): By definition of complement, right distributivity, assumption (3), neutrality of 0 and isotony,

$$a \cdot \neg q = (p + \neg p) \cdot a \cdot \neg q = p \cdot a \cdot \neg q + \neg p \cdot a \cdot \neg q = 0 + \neg p \cdot a \cdot \neg q \leq \neg p \cdot a \ .$$

The implications shown so far are displayed in the following diagram.



The other implications in the table follow simply by transitivity of implication. □

Counterexamples to the missing reverse implications can be found in Figures 2.2 and 2.3.

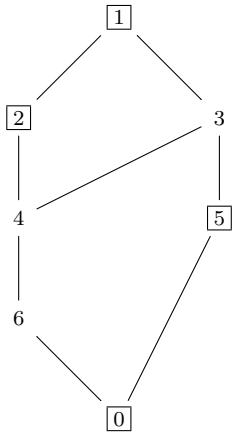
≤	0	1	2
0	1	1	1
1	0	1	1
2	0	0	1

¬	
0	1
1	0
2	0

+	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

·	0	1	2
0	0	0	0
1	0	1	2
2	2	2	2

Fig. 2.2 Counter-example to (1) ⇒ (2) in Lm. 2.2.3, with $p, q, a := 1, 0, 2$, where := means substitution or instantiation.



≤	0	1	2	3	4	5	6
0	1	1	1	1	1	1	1
1	0	1	0	0	0	0	0
2	0	1	1	0	0	0	0
3	0	1	0	1	0	0	0
4	0	1	1	1	1	0	0
5	0	1	0	1	0	1	0
6	0	1	1	1	1	0	1

¬	
0	1
1	0
2	5
3	0
4	0
5	2
6	0

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1
2	2	1	2	1	2	1	2
3	3	1	1	3	3	3	3
4	4	1	2	3	4	3	4
5	5	1	1	3	3	5	3
6	6	1	2	3	4	3	6

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	2	4	4	0	6
3	0	3	6	3	6	5	6
4	0	4	6	4	6	0	6
5	0	5	0	5	0	5	0
6	0	6	6	6	6	0	6

Fig. 2.3 Counter-example to (2) ⇒ (1) in Lm. 2.2.3, with $p, q, a := 2, 2, 3$, assuming that a is left-distributive (cf. Def. 1.4.4).

Now Property (3) in Lm. 2.2.3 can be used to encode assertion logic (e.g. [44]). Remember that the Hoare triple $\{p\}\ a\ \{q\}$ expresses that for

every state satisfying the precondition p all successor states under a, considered as a program, satisfy the postcondition q. Equivalently, if we pre-restrict a to p, we obtain a program that, when post-restricted to $\neg q$, becomes the empty program 0. This motivates the following general definition of Hoare triples in an IL-semiring.

Definition 2.2.4 For left-distributive IL-semiring S and $a \in S, p, q \in \mathsf{test}(S)$, the *Hoare triple* $\{p\}\ a\ \{q\}$ is defined by

$$\{p\}\ a\ \{q\} \Leftrightarrow_{df} p \cdot a \cdot \neg q \leq 0 \ .$$

In particular, p is called an *invariant* of a if $\{p\}\ a\ \{p\}$ holds.

In an I-semiring, as a consequence of Lm. 2.2.3 and by using the mirror operator $\cdot^{\mathrm{op}}$ (see Def. 1.4.7), the following properties are equivalent:

$$a \cdot q \leq p \cdot a \ , \qquad \neg p \cdot a \leq a \cdot \neg q \ , \qquad \neg p \cdot a \cdot q \leq 0 \ , \qquad a \cdot q = p \cdot a \cdot q \ .$$

We close with a variation of Lm. 2.2.3 for bounded I-semirings.

Lemma 2.2.5 *Assume an IL-semiring S with $a \in S$ and $p \in \mathsf{test}(S)$.*

1. *$p \cdot a \leq 0 \Leftrightarrow a \leq \neg p \cdot a$. If S is bounded, these are further equivalent to $a \leq \neg p \cdot \top$.*
2. *If S is even an I-semiring then $a \cdot p \leq 0 \Leftrightarrow a \leq a \cdot \neg p$. If S is bounded, these are further equivalent to $a \leq \top \cdot \neg p$.*

Proof.

1. The implication ($\Leftarrow$) follows by multiplying both sides of the right inequality by p and using Boolean algebra and left strictness. The converse implication follows by neutrality of 0, right distributivity, Boolean algebra again and neutrality of 1:

$$\begin{aligned} p \cdot a \leq 0 \ &\Rightarrow\ p \cdot a + \neg p \cdot a = \neg p \cdot a \ \Leftrightarrow\ (p + \neg p) \cdot a = \neg p \cdot a \\ &\Leftrightarrow\ 1 \cdot a = \neg p \cdot a \ \Leftrightarrow\ a = \neg p \cdot a \ . \end{aligned}$$

   For the second claim, the direction ($\Rightarrow$) follows by $a \leq \top$ and isotony. Finally, by isotony, the definition of complement and left-strictness of 0,

$$a \leq \neg p \cdot \top \ \Rightarrow\ p \cdot a \leq p \cdot \neg p \cdot \top = 0 \ .$$

2. Since in an I-semiring $\cdot$ is left-distributive and right-strict, the proof of Part 1 dualises. □

2.3 Tests as a Boolean Algebra

We can now give sufficient conditions when the set of tests forms a Boolean algebra.

Theorem 2.3.1 *Assume an IL-semiring S.*

1. *If multiplication is left-distributive on* $\mathsf{test}(S)$*, i.e.,* $p \cdot (q + r) = p \cdot q + p \cdot r$ *for all* $\forall\, p, q, r \in \mathsf{test}(S)$*, then* $\mathsf{test}(S)$ *is closed under addition and multiplication; the complements are determined according to De Morgan's laws, i.e.,*
$$\neg(p + q) = \neg p \cdot \neg q \ , \qquad \neg(p \cdot q) = \neg p + \neg q \ .$$
Hence $(\mathsf{test}(S), +, \cdot, \neg, 0, 1)$ *is a Boolean algebra. This holds, in particular, when* S *is a left-distributive IL-semiring.*
2. *Consider a subset* $T \subseteq \mathsf{test}(S)$ *that is closed under addition, multiplication and complement. Then multiplication is left-distributive on* T *and* $(T, +, \cdot, \neg, 0, 1)$ *is a Boolean algebra.*
3. *If* $\mathsf{test}(S)$ *is closed under addition or multiplication then it is a Boolean algebra.*
4. *If* S *is Boolean then* $\mathsf{test}(S)$ *coincides with the set of all elements below* 1*, with* $\neg p = \overline{p} \sqcap 1$*. It is closed under complementation, addition and multiplication, and hence forms a Boolean algebra. If* S *is a complete lattice, then so is* $\mathsf{test}(S)$*.*

Proof.

1. We show that Property (d) of Th. 2.1.8.14 holds. By left distributivity, commutativity of $\cdot$ for tests, definition of complement and left-strictness,
$$\begin{aligned}(\neg p \cdot \neg q) \cdot (p + q) &= \neg p \cdot \neg q \cdot p + \neg p \cdot \neg q \cdot q \\ &= \neg p \cdot p \cdot \neg q + \neg q \cdot q \cdot \neg p = 0 \cdot \neg q + 0 \cdot \neg p = 0 \ ,\end{aligned}$$
so that $p + q$ and $\neg p \cdot \neg q$ are complements of each other by Th. 2.1.8.12. Hence $p + q$ and $\neg p \cdot \neg q$ are tests again and the first De Morgan law holds by Lm. 2.1.8.13. Since p, q are arbitrary, we may replace them by $\neg p, \neg q$ and obtain from Th. 2.1.8.4 that also $\neg\neg p \cdot \neg\neg q = p \cdot q$ is a test and that the second De Morgan law holds. Moreover, by Th. 2.1.8.8 we have the absorption laws. By the definition of IL-semirings and the assumption that multiplication distributes over addition, the set of tests is a distributive lattice. From this, one can infer by a standard proof that also addition distributes over multiplication. Hence we have a Boolean algebra.
2. By closure under addition, $q + r$ is a test. Hence, using Th. 2.1.8.7, right-distributivity and Th. 2.1.8.7 again, we have
$$p \cdot (q + r) = (q + r) \cdot p = q \cdot p + r \cdot p = p \cdot q + p \cdot r \ ,$$
and $(T, +, \cdot, \neg, 0, 1)$ is a Boolean algebra by an argument similar to that for Part 1.
3. By Th. 2.1.8.14 $\mathsf{test}(S)$ is also closed under addition and multiplication, and by the definition of complements it is closed under complements, so that Part 2 applies.
4. Let $T = \{p \,|\, p \leq 1\}$ and suppose $p \in T$. Then by Boolean distributivity and the definitions of Boolean complement and infimum we have
$$p + (\overline{p} \sqcap 1) = (p + \overline{p}) \sqcap (p + 1) = \top \sqcap 1 = 1 \ .$$

Since multiplication is isotone and hence sub-conjunctive in both arguments, we obtain, together with neutrality of 1, Th. 2.1.8.1 and again the definition of Boolean complement,

$$p \cdot (\overline{p} \sqcap 1) \leq p \cdot \overline{p} \sqcap p \cdot 1 = p \cdot \overline{p} \sqcap p \leq \overline{p} \sqcap p = 0 \ .$$

A symmetric derivation shows that also $(\overline{p} \sqcap 1) \cdot p = 0$. Hence indeed $\neg p = \overline{p} \sqcap 1$ and p is a test[1].

By construction $\neg p \leq 1$, which shows closure of T under complements.

By the characterisation of the supremum, $p \leq 1 \wedge q \leq 1 \Rightarrow p + q \leq 1$, which shows closure of T under addition.

Finally, by isotony and neutrality, $p \leq 1 \wedge q \leq 1 \Rightarrow p \cdot q \leq 1 \cdot 1 = 1$, which shows closure of T under multiplication.

Now Part 2 applies.

For the final claim consider an arbitrary subset $P \subseteq \mathsf{test}(S)$. Since S is complete, there is a supremum $p = \bigsqcup P \in S$. By definition, 1 is an upper bound of P. Since p is the least upper bound, we obtain $p \leq 1$ and hence $p \in \mathsf{test}(S)$, too.

□

2.4 Predomain and Domain

We now introduce an abstract domain operator $\ulcorner$ that assigns to an element the test that describes precisely its possible starting states. We present one particular axiomatisation that is easy to understand informally. There are are others with certain algebraic advantages, for instance the *dynamic negation* of [35] or the *antidomain* of [21, 22, 23]; these are discussed elsewhere.

As a motivation, consider again the relational IL-semiring of Ex 1.5.6. Let R be a binary relation on some set M. Then the domain $\ulcorner R$ of R is given by the set

$$\{a \in M \mid \exists\, b \in M : (a, b) \in R\}.$$

For a treatment in the semiring setting it should be represented as a test in the IL-semiring of binary relations, that is, as the sub-identity

$$\ulcorner R = \{(a, a) \in M \times M \mid \exists\, b \in M : (a, b) \in R\}.$$

Abstracting from the relational IL-semiring to a general one, we arrive at the following definition. The notation was first introduced in [11]; the predecessor paper [10] used the notation of [5]. Both papers were based on an axiomatisation via a Galois connection in quantales; the inequational axioms presented below for general IL-semirings are from [17].

[1] The first result follows more directly from Lm. 2.2.1.2. We have chosen the longer derivation, since that can be reused for the symmetric result, which is not the case for Lm. 2.2.1.2.

Definition 2.4.1 A *prepredomain IL-semiring* is a structure $(S, \ulcorner)$, where S is an IL-semiring and the *prepredomain operator* $\ulcorner : S \to \mathsf{test}(S)$ satisfies, for all $a \in S$,

$$a \leq \ulcorner a \cdot a \ . \tag{d1}$$

We call $\ulcorner$ a *predomain operator* if additionally it satisfies, for all $a \in S$ and $p \in \mathsf{test}(S)$,

$$\ulcorner(p \cdot a) \leq p \ . \tag{d2}$$

Finally, a predomain operator $\ulcorner$ is called a *domain operator* if additionally it satisfies, for all $a, b \in S$, the *locality* axiom

$$\ulcorner(a \cdot \ulcorner b) \leq \ulcorner(a \cdot b) \ . \tag{d3}$$

In the latter cases, $(S, \ulcorner)$ is called a *predomain IL-semiring* and a *domain IL-semiring*, resp. Finally, an I-semiring with a ((pre)pre)domain operator is called a *((pre)pre)domain I-semiring*.

This definition deviates from the one given in [18] and subsequent papers in that the elements p quantified in the axioms are not restricted to a distinguished subset of $\mathsf{test}(S)$ but may be arbitrary tests. This has the somewhat surprising consequence (see Th. 2.4.6) that the image set of the predomain operator coincides with $\mathsf{test}(S)$ which, moreover, necessarily is a Boolean algebra.

Since by definition $\ulcorner a$ is a test, we have $\ulcorner a \leq 1$ and hence by isotony the reverse inequation to (d1) holds as well, so that (d1) is equivalent to

$$a = \ulcorner a \cdot a \ . \tag{2.1}$$

The axioms can be understood as follows. Axiom (d1), which, as mentioned in (2.1), strengthens to an equality, means that restriction to all starting states is no actual restriction, whereas (d2) means that after restriction the remaining starting states should satisfy the restricting test. Axiom (d3), which, as will be shown in Lm. 2.4.8, again strengthens to an equality, states that the domain of $a \cdot b$ is not determined by the inner structure or the final states of b; information about $\ulcorner b$ in interaction with a suffices.

Mace4 proves that Axioms (d1)–(d3) are independent. We show below that still there is some interrelation between them.

We now discuss consequences of the axioms.

Lemma 2.4.2 *Assume a prepredomain IL-semiring $(S, \ulcorner)$ and let $\ulcorner S$ be the image of S under $\ulcorner$.*

1. *If $a \leq 1$ then $a \leq \ulcorner a$.*
2. *$\ulcorner 1 = 1$ and hence $1 \in \ulcorner S$.*
3. *If $\ulcorner a = 0$ then $a = 0$. The reverse implication does not hold.*

Proof.

1. By (d1), the assumption, isotony of $\cdot$ and neutrality of 1 we have $a \leq \ulcorner a \cdot a \leq \ulcorner a \cdot 1 = \ulcorner a$.
2. By Part 1 we have $1 \leq \ulcorner 1$. Since $\ulcorner 1$ is a test, we also have $\ulcorner 1 \leq 1$.

3. By (d1), the assumption and left strictness,
$$a \leq \lceil a \cdot a = 0 \cdot a = 0 \ .$$
The reverse implication does not hold: taking $\lceil a = 1$ for all a satisfies (d1). □

Now we are ready for the announced interrelation between the axioms.

Lemma 2.4.3 *Axioms* (d1) *and* (d3) *together with the additional assumption* $\lceil 0 = 0$ *imply* (d2)*.*

Proof. We calculate:

$$\begin{array}{lll} & \lceil(p \cdot a) \leq p & \\ \Leftrightarrow & \neg p \cdot \lceil(p \cdot a) = 0 & \{\![\text{ shunting }]\!\} \\ \Leftarrow & \lceil(\neg p \cdot \lceil(p \cdot a)) = 0 & \{\![\text{ Lm. 2.4.2.3 }]\!\} \\ \Leftarrow & \lceil(\neg p \cdot p \cdot a) = 0 & \{\![\text{ (d3) }]\!\} \\ \Leftarrow & \lceil 0 = 0 & \{\![\text{ definition of tests and left strictness }]\!\} \\ \Leftrightarrow & \mathsf{TRUE} \ . & \{\![\text{ assumption } \lceil 0 = 0]\!\} \end{array}$$

□

For a further explanation of (d1) and (d2) we show equivalent characterisations of their conjunction. For this we investigate the formulas

$$\lceil a \leq p \ \Leftrightarrow \ a \leq p \cdot a \ , \tag{llp}$$
$$p \leq \neg\lceil a \ \Leftrightarrow \ p \cdot a \leq 0 \ , \tag{gla}$$
$$p \cdot \lceil a \leq 0 \ \Leftrightarrow \ p \cdot a \leq 0 \tag{2.2}$$

Formula (llp) says that $\lceil a$ is the least left preserver of a, while (gla) says that $\neg\lceil a$ is the greatest left annihilator of a.

Lemma 2.4.4 (d1) $\wedge$ (d2) $\Leftrightarrow$ (llp) $\Leftrightarrow$ (gla) $\Leftrightarrow$ (2.2)*, where the fully universally quantified versions of* (d1)*,* (d2)*,* (llp)*,* (gla) *and* (2.2) *are meant.*

Proof.
- (d1) $\wedge$ (d2) $\Rightarrow$ (llp): Assume (d1) and suppose $\lceil a \leq p$. Then by (2.1) and isotony of $\cdot$ we get $a = \lceil a \cdot a \leq p \cdot a$. Assume (d2) and suppose $a \leq p \cdot a$. By $p \leq 1$ and isotony we obtain $a = p \cdot a$. Hence $\lceil a = \lceil(p \cdot a) \leq p$ by (d2).
- (llp) $\Rightarrow$ (d1): Substitute $p := \lceil a$ in (llp).
- (llp) $\Rightarrow$ (d2): Substitute $a := p \cdot a$ in (llp) and use $p \cdot p = p$.
- Before showing (llp) $\Leftrightarrow$ (gla), we note that (llp) can be rewritten as
$$p \leq \neg\lceil a \ \Leftrightarrow \ a \leq \neg p \cdot a \tag{2.3}$$
by substituting $p := \neg p$ in (llp) and using shunting.
- (2.3) $\Rightarrow$ (gla): By (2.3) and Lm. 2.2.5.1, $p \leq \neg\lceil a \ \Leftrightarrow \ a \leq \neg p{\cdot}a \ \Leftrightarrow \ p{\cdot}a \leq 0$.
- (gla) $\Rightarrow$ (2.3): By (gla) and Lm. 2.2.5.1, $p \leq \neg\lceil a \ \Leftrightarrow \ p{\cdot}a \leq 0 \ \Leftrightarrow \ a \leq \neg p{\cdot}a$.
- Finally, by shunting, the left hand side of (gla) is equivalent to $p \cdot \lceil a \leq 0$, which shows the last claimed equivalence.

□

In [49] the predomain $\overleftarrow{a}$ of a is *defined* as the least element of the set of left preservers of a in a set-theoretic way, but not *axiomatised* by (llp). No consequences except additivity of $^{\leftarrow}$ are proved there and nothing corresponding to Axiom (d3) is given.

Lemma 2.4.5 *A predomain operator is uniquely characterised by the axioms if it exists.*

Proof. (llp) characterises $\lceil a$ as the least element in the set of all tests that are left preservers of a. Now the claim follows, since least elements are unique in partial orders (see Def. 1.2.3). □

Theorem 2.4.6 *Assume a predomain IL-semiring $(S, \lceil)$ and let a, b range over S and p, q over $\mathsf{test}(S)$. Moreover, set $\lceil S =_{df} \{\lceil a \mid a \in S\}$.*

1. $\lceil p = p$ (Stability).
   In particular, $\lceil\lceil a = \lceil a$ and $\neg p = \lceil(\neg p)$ and hence $\lceil S$ is closed under complement. Moreover, $\lceil$ is surjective, i.e., $\lceil S = \mathsf{test}(S)$.
2. *The predomain operator is fully strict, i.e., $\lceil a = 0 \Leftrightarrow a = 0$.*
3. $\neg\lceil a \cdot a = 0$.
4. *The predomain operator is isotone.*
5. *Predomain preserves arbitrary existing suprema. More precisely, if a subset $A \subseteq S$ has a supremum b in S then the image set of A under $\lceil$ has a supremum in $\mathsf{test}(S)$, namely $\lceil b$. Note that neither completeness of S nor that of $\mathsf{test}(S)$ is required. This means that predomain is universally disjunctive and hence continuous (cf. Def. 1.2.8) and strict.*
6. $\lceil(a \cdot b) \leq \lceil(a \cdot \lceil b)$.
7. $p \cdot q = \lceil(p \cdot q)$. *Hence $\lceil S = \mathsf{test}(S)$ is closed under $\cdot$.*
8. *$\mathsf{test}(S)$ is a Boolean algebra and hence also closed under $+$.*
9. *Predomain satisfies the import/export law $\lceil(p \cdot a) = p \cdot \lceil a$.*
10. $\lceil(a + b) = \lceil a + \lceil b$.
11. *If $a \sqcap b$ exists then $\lceil b \cdot a \sqcap \lceil a \cdot b = a \sqcap b$.*

Assuming that S is bounded, the following additional properties hold.

12. *We have the Galois connection (see Sect. 2.7) $\lceil a \leq p \Leftrightarrow a \leq p \cdot \top$.*
13. $\lceil(a \cdot \top) = \lceil a$. *Hence also $\lceil(p \cdot \top) = p$; in particular $\lceil\top = 1$.*

Proof.

1. By Lm. 2.4.2.1 it remains to show ($\leq$). By neutrality of 1 and (d2) we obtain $\lceil p = \lceil(p \cdot 1) \leq p$.
2. The direction ($\Leftarrow$) is a special case of Part 1, since $0 \in \mathsf{test}(S)$. ($\Rightarrow$) is immediate from (d1) and left strictness of 0.
3. Substitute $\neg\lceil a$ for p in (gla).
4. Assume $a \leq b$. We have, by shunting, (gla), the assumption and isotony of $\cdot$, and finally (gla) again,
$$\lceil a \leq \lceil b \Leftrightarrow \neg\lceil b \leq \neg\lceil a \Leftrightarrow \neg\lceil b \cdot a \leq 0 \Leftarrow \neg\lceil b \cdot b \leq 0 \Leftrightarrow \mathsf{TRUE}\ .$$
5. Let $b = \bigsqcup A$ exist for some set $A \subseteq S$. We must show that $\lceil b$ is a supremum of $\lceil A =_{df} \{\lceil a \mid a \in A\}$ in $\mathsf{test}(S)$. First, by isotony of predomain, $\lceil b$

is an upper bound of the set $\lceil A$, since b is an upper bound of A. To show that $\lceil b$ is the least upper bound of $\lceil A$ in $\mathsf{test}(S)$, let p be an arbitrary upper bound of $\lceil A$ in $\mathsf{test}(S)$. Then for all $a \in A$ we have $\lceil a \leq p$, equivalently $a \leq p \cdot a$ by (llp), and therefore $a \leq p \cdot b$ by definition of b and isotony of $\cdot$. Hence $p \cdot b$ is an upper bound of A and therefore $b \leq p \cdot b$. By (llp) this is equivalent to $\lceil b \leq p$, so that $\lceil b$ is indeed the least upper bound of $\lceil A$ in $\mathsf{test}(S)$.

6. By (llp) and (2.1) thrice we obtain
$$\lceil(a \cdot b) \leq \lceil(a \cdot \lceil b) \Leftrightarrow a \cdot b \leq \lceil(a \cdot \lceil b) \cdot a \cdot b \Leftrightarrow a \cdot b \leq \lceil(a \cdot \lceil b) \cdot a \cdot \lceil b \cdot b$$
$$\Leftrightarrow a \cdot b \leq a \cdot \lceil b \cdot b \Leftrightarrow a \cdot b \leq a \cdot b \Leftrightarrow \mathsf{TRUE}\ .$$
7. ($\leq$) follows from Lm. 2.4.2.1, since $p, q \leq 1$ implies $p \cdot q \leq 1$. For ($\geq$) we have by Lm. 2.1.8.6, (d1), $p \leq 1$ with Part 4, and Part 1,
$$\lceil(p \cdot q) = \lceil(p \cdot q) \cdot \lceil(p \cdot q) \leq p \cdot \lceil q = p \cdot q\ .$$
8. This follows from Part 7 and Th. 2.3.1.3.
9. By (d2) we know $\lceil(p \cdot a) \leq p$. By $p \leq 1$, isotony of $\cdot$ and $\lceil$ and neutrality of 1 we obtain $\lceil(p \cdot a) \leq \lceil(1 \cdot a) = \lceil a$. Now the inequation $\lceil(p \cdot a) \leq p \cdot \lceil a$ follows by isotony of $\cdot$ and idempotence of $\cdot$ on tests.
For the reverse inequation we argue as follows.

$p \cdot \lceil a \leq \lceil(p \cdot a)$	
$\Leftrightarrow \lceil a \leq \neg p + \lceil(p \cdot a)$	{[shunting]}
$\Leftrightarrow a \leq (\neg p + \lceil(p \cdot a)) \cdot a$	{[(llp), since $\neg p + \lceil(p \cdot a)$ is a test by Part 8]}
$\Leftrightarrow a \leq \neg p \cdot a + \lceil(p \cdot a) \cdot a$	{[right distributivity]}
$\Leftrightarrow a \leq \neg p \cdot a + \lceil(p \cdot a) \cdot p \cdot a$	{[$\lceil(p \cdot a) \leq p$ by (d2), hence $\lceil(p \cdot a) \cdot p = \lceil(p \cdot a)$]}
$\Leftrightarrow a \leq \neg p \cdot a + p \cdot a$	{[(2.1)]}
$\Leftrightarrow a \leq a$	{[right distributivity, complement, neutrality of 1]}
$\Leftrightarrow \mathsf{TRUE}\ .$	{[reflexivity]}

10. By isotony of $\lceil$ and Cor. 1.2.9.1 we have $\lceil(a+b) \geq \lceil a + \lceil b$. For the reverse inequation we employ that by Part 8 $\lceil a + \lceil b \in \mathsf{test}(S)$ and obtain by (llp), the characterisation of suprema, isotony of $\cdot$ and (d1):
$$\lceil(a+b) \leq \lceil a + \lceil b \Leftrightarrow a + b \leq (\lceil a + \lceil b) \cdot (a+b)$$
$$\Leftrightarrow a \leq (\lceil a + \lceil b) \cdot (a+b) \wedge b \leq (\lceil a + \lceil b) \cdot (a+b)$$
$$\Leftarrow a \leq \lceil a \cdot a \wedge b \leq \lceil b \cdot b \Leftrightarrow\Leftrightarrow \mathsf{TRUE}\ .$$
11. Using Lm. 2.2.1.2 four times and (2.1) twice, we obtain $\lceil b \cdot a \sqcap \lceil a \cdot b = \lceil a \cdot \lceil b \cdot (a \sqcap b) = \lceil a \cdot a \sqcap \lceil b \cdot b = a \sqcap b$.
12. We calculate, employing (llp), greatestness of $\top$ and isotony of $\cdot$, isotony of $\lceil$, and finally (d2),
$$\lceil a \leq p \Leftrightarrow a \leq p \cdot a \Rightarrow a \leq p \cdot \top \Rightarrow \lceil a \leq \lceil(p \cdot \top) \Rightarrow \lceil a \leq p\ .$$
13. First, by isotony of $\cdot$, Lm. 1.4.6 and $a = a \cdot 1 \leq a \cdot \top$ we get
$$a \leq p \cdot \top \Rightarrow a \cdot \top \leq p \cdot \top \cdot \top \Leftrightarrow a \cdot \top \leq p \cdot \top \Rightarrow a \leq p \cdot \top\ ,$$

so that $a \cdot \top \leq p \cdot \top \Leftrightarrow a \leq p \cdot \top$. Now, by Part 12, this observation and Part 12 again,

$$\lceil(a \cdot \top) \leq p \Leftrightarrow a \cdot \top \leq p \cdot \top \Leftrightarrow a \leq p \cdot \top \Leftrightarrow \lceil a \leq p \ ,$$

and the principle of indirect equality II (Lm. 1.2.2) shows the claim. □

Next we show an auxiliary property for predomain operators on Boolean IL-semirings.

Lemma 2.4.7 *If a predomain IL-semiring $(S, \lceil)$ is Boolean then*

$$\neg\lceil a \leq \lceil\overline{a}, \text{ hence } \neg\lceil\overline{a} \leq \lceil a \ , \quad \text{and} \quad \overline{p \cdot \top} = \neg p \cdot \top \ .$$

Proof. By Th. 2.4.6.13, Boolean algebra and Th. 2.4.6.10, $1 = \lceil\top = \lceil(a + \overline{a}) = \lceil a + \lceil\overline{a}$. Now the first two claims follow by shunting and neutrality of 1.

By Boolean algebra we only have to show that $\neg p \cdot \top + p \cdot \top = \top$ and $\neg p \cdot \top \sqcap p \cdot \top = 0$. The first equation follows by right-distributivity and the definition of complement, the second one by Lm. 2.2.1.3 and the definition of complement. □

The reverse inequality $\lceil\overline{a} \leq \neg\lceil a$ does not hold. A simple counterexample is obtained by setting $a := 1$ in the relational IL-semiring.

We conclude this section by turning to the case of a domain IL-semiring.

Lemma 2.4.8 *Over a domain IL-semiring $(S, \lceil)$ property* (d3) *strengthens to the equality $\lceil(a \cdot b) = \lceil(a \cdot \lceil b)$, which we term again* locality.

Proof. This is immediate from Th. 2.4.6.6. □

Definition 2.4.9 We call a bounded predomain IL-semiring S $\top$*-determined* if $a \cdot \top = \lceil a \cdot \top$ for all $a \in S$.

Example 2.4.10 The IL-semiring $\mathsf{REL}(M)$ over a set M is $\top$-determined. □

Lemma 2.4.11 *A bounded predomain IL-semiring is $\top$-determined iff predomain has the explicit representation*

$$\lceil a = a \cdot \top \sqcap 1 \ .$$

Proof. ($\Rightarrow$) By the assumption and Lm. 2.2.1.6

$$a \cdot \top \sqcap 1 = \lceil a \cdot \top \sqcap 1 = \lceil a \ .$$

($\Leftarrow$) Isotony of $\cdot$ (due to $a \cdot \top \sqcap 1 \leq a \cdot \top$) and the fact that $\top$ is the greatest element yield

$$\lceil a \cdot \top = (a \cdot \top \sqcap 1) \cdot \top \leq a \cdot \top \cdot \top \leq a \cdot \top.$$

The converse inequation holds in all predomain IL-semirings (set $p = \lceil a$ in Thm. 2.4.6.12). □

Hence the predomain representation holds in every full relation algebra $\mathsf{REL}(M)$.

2.5 Examples of Predomain and Domain Semirings

First we show that there is always a meaningful — albeit not very interesting — predomain definition for a test-discrete IL-semiring.

Lemma 2.5.1 *A test-discrete IL-semiring S admits precisely one predomain operator, namely $\lceil 0 = 0$ and $\lceil a = 1$ for all $0 \neq a \in S$.*

Proof. We show that $\lceil$ satisfies (d1) and (d2).

For (d1), if $a = 0$ then trivially $a \leq \lceil a \cdot a$. Otherwise, $a \neq 0$ and $\lceil a = 1$ by Th. 2.4.6.2. Hence $a = 1 \cdot a = \lceil a \cdot a$.

For (d2), if $\lceil(p \cdot a) = 0$ then (d2) holds trivially. Otherwise, if $\lceil(p \cdot a) = 1$ then $p \cdot a \neq 0$ by Th. 2.4.6.2 and therefore also $p \neq 0$. Thus $p = 1$ by discreteness and (d2) also holds.

Thus $\lceil$ is a well-defined predomain operator for S.

Finally, uniqueness follows from Th. 2.4.6.2. as well as from Lm. 2.4.5. □

We now specify a necessary and sufficient condition on a discrete predomain IL-semiring to be a domain IL-semiring.

Definition 2.5.2 In analogy to the definition of an integral domain in ring theory, an IL-semiring S is *integral* if it has no zero divisors, that is, for all $a, b \in S$,

$$a \cdot b \leq 0 \;\Rightarrow\; a \leq 0 \vee b \leq 0. \tag{2.4}$$

Example 2.5.3 The language IL-semirings $\mathsf{LAN}(\Sigma)$ and $\mathsf{WOR}(\Sigma)$ over an alphabet Σ are integral. □

Lemma 2.5.4 *Let S be an integral IL-semiring. If S is a predomain IL-semiring then it is also a domain IL-semiring.*

Proof. Let S be integral. To prove (d3), by the principle of indirect inequality II (Lm. 1.2.2) it suffices to show that $\lceil(a \cdot b) \leq p \;\Rightarrow\; \lceil(a \cdot \lceil b) \leq p$ for all $p \in \mathsf{test}(S)$. Using shunting, (gla), integrality, (gla) and shunting again, we calculate

$$\begin{aligned}\lceil(a \cdot b) \leq p &\Leftrightarrow \neg p \leq \neg\lceil(a \cdot b) \Leftrightarrow \neg p \cdot a \cdot b \leq 0 \Rightarrow \neg p \cdot a \leq 0 \vee b \leq 0\\ &\Leftrightarrow \neg p \leq \neg\lceil a \vee b \leq 0 \Leftrightarrow \lceil a \leq p \vee b \leq 0.\end{aligned}$$

If $\lceil a \leq p$, by isotony and neutrality of 1, $\lceil(a \cdot \lceil b) \leq \lceil(a \cdot 1) = \lceil a \leq p$. Otherwise $b = 0$ and hence by Th. 2.4.6.2, $\lceil(a \cdot \lceil b) = \lceil(a \cdot b) \leq p$. □

For test-discrete IL-semirings the condition of integrality is also necessary.

Lemma 2.5.5 *A test-discrete IL-semiring is a domain IL-semiring iff it is integral.*

Proof. Let S be a test-discrete IL-semiring. From Lm. 2.5.1 we know that S is a predomain IL-semiring with $\lceil 0 = 0$ and $\lceil a = 1$ for all $0 \neq a \in S$.

($\Rightarrow$) Now let $\ulcorner$ satisfy (d3), that is, $\ulcorner(a \cdot \ulcorner b) \leq \ulcorner(a \cdot b)$, and let $a \cdot b \leq 0$. Then by full strictness (Th. 2.4.6.2) twice, $\ulcorner(a \cdot \ulcorner b) \leq \ulcorner(a \cdot b) \leq \ulcorner 0 = 0$ and hence $a \cdot \ulcorner b \leq 0$. There are two cases.
- If $\ulcorner b = 1$ then $a \cdot \ulcorner b = a \cdot 1 = a$. Hence $a \cdot \ulcorner b \leq 0$ implies $a \leq 0$.
- If $\ulcorner b = 0$ then $b = 0$ by full strictness (Th. 2.4.6.2).

Thus $a \cdot b \leq 0$ implies $a \leq 0$ or $b \leq 0$, whence S is integral.
($\Leftarrow$) follows from Lm. 2.5.4. □

With this we can now analyse some of our earlier examples concerning (pre)domain operators.

Example 2.5.6 In the Boolean I-semiring S_2 (Ex. 1.5.1), the test algebra coincides with S_2. Setting $\ulcorner x = 0 \Leftrightarrow x = 0$ is compatible with the definition of $\ulcorner$ in Lm. 2.5.1. Thus (d1) and (d2) are valid. Since S_2 is integral, (d3) holds, too. Moreover, the (pre)domain definition is unique. □

Example 2.5.7 In S_3^2 (Ex. 1.5.3), the test algebra is $\{0, 1\}$. Setting $\ulcorner 0 = 0$, $\ulcorner a = 1$ and $\ulcorner 1 = 1$ is compatible with Lm. 2.5.1. Thus (d1) and (d2) are satisfied. Since S_3^2 is integral, (d3) holds, too. Moreover, the (pre)domain definition is unique. □

Example 2.5.8 A prominent example of a domain I-semiring is $\mathsf{REL}(M)$ over a set M with the full set of tests (see Ex. 2.1.2). There, the domain operator is given by

$$\ulcorner R = \{(x, x) \mid \exists\, y : (x, y) \in R\} \ .$$

□

Example 2.5.9 Generalising Ex. 2.5.6 we get from Ex. 2.1.3 that $\mathsf{BOOL}(B)$ can be made into a domain I-semiring by setting $\ulcorner x = x$ for all $x \in B$. □

Example 2.5.10 In $\mathsf{LAN}(\Sigma)$ and $\mathsf{WOR}(\Sigma)$ (Exs. 1.5.9 and 1.5.17) the test set is $\{\emptyset, \{\varepsilon\}\}$, so that both IL-semirings are test-discrete. Hence setting $\ulcorner\emptyset = \emptyset$ and $\ulcorner L = \{\varepsilon\}$ for all $\emptyset \neq L \subseteq \Sigma^*$ is compatible with Lm. 2.5.1 and (d1) and (d2) are satisfied. Since both IL-semirings are integral, (d3) holds, too. Moreover, the (pre)domain definition is unique. □

Example 2.5.11 In $\mathsf{PAT}(\Sigma)$ and $\mathsf{STR}(\Sigma)$ (Exs. 1.5.14) and 1.5.18), the test algebra is 2^Σ. For $U \subseteq \Sigma^+$, the set $\ulcorner U$ consists of all starting nodes of paths in U. Although neither IL-semiring is integral, (d3) holds. □

Example 2.5.12 In the tropical I-semiring (Ex. 1.5.11), the test algebra consists solely of 0 and ∞. Taking $\ulcorner\infty = \infty$ and $\ulcorner n = 0$ for $n \in \mathbb{N}$ is compatible with Lm. 2.5.1 and (d1) and (d2) hold. Since the tropical I-semiring is integral, (d3) holds, too. Moreover, the domain definition is unique. □

These examples show that our domain axioms are meaningful in all the usual models, although non-trivial only in the relational, the path and the stream IL-semirings.

2.6 Precodomain and Codomain

We now turn to the dual case of the (pre)codomain operator.

In the case where we also have left distributivity of multiplication, a (pre)codomain operator $^\urcorner$ can easily be defined as a (pre)domain operator in the mirror IL-semiring (see Def. 1.4.7). But by lack of left distributivity this does not work in the general IL-semiring setting; we additionally have to postulate isotony of (pre)codomain (again in the form of super-disjunctivity to have a purely equational axiom). Mace4 finds a counterexample to isotony if only (cd1) and (cd2) are stipulated.

Definition 2.6.1 A *preprecodomain IL-semiring* is a structure $(S, ^\urcorner)$, where S is an IL-semiring and the *preprecodomain operator* $^\urcorner : S \to \mathsf{test}(S)$ satisfies, for all $a \in S$,

$$a \leq a \cdot a^\urcorner \ . \tag{cd1}$$

We call $^\urcorner$ a *precodomain operator* if additionally it satisfies, for all $a \in S$ and $p \in \mathsf{test}(S)$,

$$(a \cdot p)^\urcorner \leq p \ , \tag{cd2}$$

$$a^\urcorner + b^\urcorner \leq (a + b)^\urcorner \ . \tag{cd4}$$

A precodomain operator $^\urcorner$ is called a *codomain operator* if additionally it satisfies, for all $a, b \in S$, the *locality axiom*

$$(a^\urcorner \cdot b)^\urcorner \leq (a \cdot b)^\urcorner \ , \tag{cd3}$$

In the latter cases, $(S, ^\urcorner)$ is called a *precodomain IL-semiring* and a *left codomain IL-semiring*, resp. Finally, an IL- semiring with a (pre)codomain operator is called a *(pre)codomain IL-semiring*.

We use the convention that $^\urcorner$ has higher precedence than $\neg$. Hence $\neg a^\urcorner$ means $\neg(a^\urcorner)$ and not $(\neg a)^\urcorner$, even when a is a test (for non-test elements the latter reading would be meaningless anyway, since $\neg$ is only defined for tests).

As for prepredomain, (cd1) is equivalent to

$$a = a \cdot a^\urcorner \tag{2.5}$$

and the conjunction of (cd1) and (cd2) is equivalent to

$$a^\urcorner \leq p \ \Leftrightarrow \ a \leq a \cdot p \ , \tag{lrp}$$

i.e., $a^\urcorner$ is the least right preserver of a.

However, by lack of right-strictness, $\neg(a^\urcorner)$ need not be the greatest right annihilator of a.

Finally, as for domain, Axiom (cd3) strengthens to the equality

$$(a^\urcorner \cdot b)^\urcorner = (a \cdot b)^\urcorner \ . \tag{2.6}$$

Precodomain satisfies a weaker version of the dual of Th. 2.4.6:

Theorem 2.6.2 *Let $(S, ^\urcorner)$ be a precodomain IL-semiring.*

1. *The precodomain operator is isotone.*

2. *Precodomain preserves arbitrary existing suprema. More precisely, if a subset $A \subseteq S$ has a supremum b in S then the image set of A under $\lceil$ has a supremum in $\mathsf{test}(S)$, namely $\lceil b \rceil$. Note that neither completeness of S nor that of $\mathsf{test}(S)$ is required.*
3. $\lceil a \rceil \leq 0 \Leftrightarrow a \leq a \cdot 0$. *In particular,* $\lceil 0 \rceil = 0$. *Moreover, in a right-strict IL-semiring the law simplifies to* $\lceil a \rceil \leq 0 \Leftrightarrow a \leq 0$.
4. $\lceil p \rceil = p$. *In particular,* $\lceil \lceil a \rceil \rceil = \lceil a \rceil$. (Stability)
5. $\lceil a \cdot p \rceil \leq \lceil a \rceil \cdot p$. (Partial Import/Export)
6. $\lceil a \cdot b \rceil \leq \lceil a \cdot \lceil b \rceil \rceil$.
7. $\lceil a \cdot b \rceil \leq \lceil b \rceil$.
8. *If S is bounded then* $\lceil \top \cdot p \rceil = p$. *In particular,* $\lceil \top \rceil = 1$.

Proof.

1. This is immediate from (cd4) and Cor. 1.2.9.2.
2. Since for predomain the proof of preservation of suprema (Th. 2.4.6.5) only involves isotony and (llp), we can carry it over to precodomain by Part 1 and (lrp)).
3. This is the special case $p = 0$ of (lrp).
4. Again, the proof of stability of predomain (Th. 2.4.6.1) only uses (d1) via Lm. 2.4.2.1 and (d2) and hence carries over to precodomain.
5. By isotony and $p \leq 1$ we obtain $\lceil a \cdot p \rceil \leq \lceil a \rceil$. Moreover, $\lceil a \cdot p \rceil \leq p$ by (cd2). Now the claim follows from the fact that $\lceil a \rceil \cdot p$ is the infimum of $\lceil a \rceil$ and p in the subalgebra of tests.
6. Using (lrp) and (2.5) thrice we obtain
$$\lceil a \cdot b \rceil \leq \lceil a \cdot \lceil b \rceil \rceil \Leftrightarrow a \cdot b \leq a \cdot b \cdot \lceil a \cdot \lceil b \rceil \rceil \Leftrightarrow a \cdot b \leq a \cdot \lceil a \rceil \cdot b \cdot \lceil a \cdot \lceil b \rceil \rceil$$
$$\Leftrightarrow a \cdot b \leq a \cdot \lceil a \rceil \cdot b \Leftrightarrow a \cdot b \leq a \cdot b \Leftrightarrow \mathsf{TRUE} \ .$$
7. Immediate from Part 6, $\lceil a \rceil \leq 1$, isotony and neutrality of 1.
8. ($\leq$) is immediate from (cd2). For ($\geq$) we calculate, using isotony, neutrality of 1 and Part 4,
$$\lceil \top \cdot p \rceil \geq \lceil 1 \cdot p \rceil = \lceil p \rceil = p \ .$$
The second claim follows by setting $p = 1$. □

The properties $\lceil a = 0 \Leftrightarrow a = 0$ of Th. 2.4.6.2 and $\lceil a \rceil \leq 0 \Leftrightarrow a \leq a \cdot 0$ of Th. 2.6.2.3 show once more the asymmetry between domain and codomain.

The following results combine predomain and precodomain.

Lemma 2.6.3 *In a predomain and precodomain IL-semiring,* $\lceil a \rceil \cdot \lceil b = 0 \Rightarrow a \cdot b = a \cdot 0$. *If additionally the IL-semiring is right-strict and has both domain and codomain then* $\lceil a \rceil \cdot \lceil b = 0 \Leftrightarrow a \cdot b = 0$.

Proof. By (2.5) and (2.1), the assumption and left strictness,
$$a \cdot b = a \cdot \lceil a \rceil \cdot \lceil b \cdot b = a \cdot 0 \cdot b = a \cdot 0 \ .$$
Under the additional premises, using Th. 2.4.6.2, Lm. 2.4.8, Th. 2.4.6.2, Th. 2.6.2.3 with the assumed right-strictness, (cd3) and Th. 2.6.2.3 again,

$$a \cdot b = 0 \Leftrightarrow \lceil(a \cdot b) = 0 \Leftrightarrow \lceil(a \cdot \lceil b) = 0 \Leftrightarrow a \cdot \lceil b = 0$$
$$\Leftrightarrow (a \cdot \lceil b)\rceil = 0 \Leftrightarrow (a\rceil \cdot \lceil b)\rceil = 0 \Leftrightarrow a\rceil \cdot \lceil b = 0 \ .$$

□

The following lemma illustrates again the asymmetry between predomain and precodomain in left semirings; it is a counterpart to Lm. 2.2.5.

Lemma 2.6.4 *Consider an IL-semiring S.*

1. *If S is a predomain IL-semiring then $\lceil a \leq p \Leftrightarrow a \leq p \cdot a \Leftrightarrow \neg p \cdot a \leq 0$. If S is bounded then additionally $a \leq p \cdot a \Leftrightarrow a \leq p \cdot \top$.*
2. *If S is a precodomain IL-semiring then $a\rceil \leq p \Leftrightarrow a \leq a \cdot p \Rightarrow a \cdot \neg p \leq a \cdot 0$. If S is bounded then additionally $a \leq a \cdot p \Leftrightarrow a \leq \top \cdot p$.*

Proof.

1. The first equivalence is (llp), while the second holds by Lm. 2.2.5.1 with $\neg p$ substituted for p. For the second claim, $(\Rightarrow)$ follows by isotony of $\cdot$. For $(\Leftarrow)$ we reason, using isotony of domain, (d2) and (llp),
$$a \leq p \cdot \top \Rightarrow \lceil a \leq \lceil(p \cdot \top) \Rightarrow \lceil a \leq p \Leftrightarrow a \leq p \cdot a \ .$$
2. The equivalence is (lrp), while the implication follows by isotony of $\cdot$ and the definition of complements. The second claim is proved symmetrically to the one in Part 1. □

Finally, we show that for a codomain operator the implication in Part 2 of this lemma strengthens to an equivalence.

Lemma 2.6.5 *In a codomain IL-semiring we have the* equivalence
$$p \leq \neg a\rceil \Leftrightarrow a \cdot p \leq a \cdot 0 \ . \qquad \text{(wgra)}$$

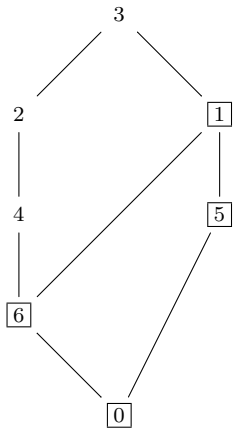
Proof. Replacing p by $\neg p$ in Lm. 2.6.4.2 and using shunting we see that it suffices to show $(\Leftarrow)$. Suppose $a \cdot p \leq a \cdot 0$. By (cd2) we have $(a \cdot 0)\rceil \leq 0$ and hence by isotony of $\rceil$ also $(a \cdot p)\rceil \leq 0$. By Th. 2.6.2.6 and (cd3) this is equivalent to $(a\rceil \cdot p)\rceil \leq 0$ and hence, by stability (Th. 2.6.2.4), equivalent to $a\rceil \cdot p \leq 0$, so that shunting shows the claim. □

We conclude this section with a counterexample that refutes four properties; see Figure 2.6.

2.7 Galois Connections

In this section we briefly review an algebraic concept that will capture fundamental symmetries of modal operators: Galois connections.

Galois connections have been advocated in computer science by Cousot [14] and Backhouse [5]. A description of certain modal algebras in terms of Galois connections has been given before by von Karger [64]. By using this concept, many properties of modal operators can be derived in a generic way. This is



$\leq$	0	1	2	3	4	5	6
0	1	1	1	1	1	1	1
1	0	1	0	1	0	0	0
2	0	0	1	1	0	0	0
3	0	0	0	1	0	0	0
4	0	0	1	1	1	0	0
5	0	1	0	1	0	1	0
6	0	1	1	1	1	0	1

$\neg$	
0	1
1	0
2	0
3	0
4	0
5	6
6	5

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	1	3	3	3	1	1
2	2	3	2	3	2	3	2
3	3	3	3	3	3	3	3
4	4	3	2	3	4	3	4
5	5	1	3	3	3	5	1
6	6	1	2	3	4	1	6

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	2	2	4	0	4
3	0	3	2	3	4	5	4
4	0	4	2	2	4	0	4
5	0	5	0	5	0	5	0
6	0	6	2	2	4	0	6

$\lceil$	
0	0
1	1
2	6
3	1
4	6
5	5
6	6

$\rceil$	
0	0
1	1
2	1
3	1
4	6
5	5
6	6

Fig. 2.4 Counter-example to the following properties in presence of the domain and precodomain axioms (without the locality axiom (cd3) of codomain):

1. (2) $\Rightarrow$ (1) in Lm. 2.2.3, with $p, q, a := 6, 6, 3$, assuming that a is left-distributive (cf. Def. 1.4.4).
2. Locality of codomain: use $a, b := 2, 5$.
3. Equality in Lm. 2.6.2.5 (partial import/export): use $a, p := 2, 5$.
4. Left implication in (wgra): use $a, p := 2, 5$.

in contrast to the logical approach where complex individual axiom systems must be used for formalizing different modal logics.

Definition 2.7.1 A *Galois connection* (see [3, 50]) is a pair of mappings $f^\flat : B \to A$ and $f^\sharp : A \to B$ between partial orders $(A, \leq_A)$ and $(B, \leq_B)$ such that, for all $a \in A$ and $b \in B$,

$$f^\flat(b) \leq_A a \Leftrightarrow b \leq_B f^\sharp(a) \ .$$

The mappings $f^\flat$ and $f^\sharp$ are called the *lower* and *upper adjoints* of the Galois connection.

In the remainder we omit the indices of the partial order relations involved.

We quote a number of standard properties of lower and upper adjoints which are immediate from the definition.

Lemma 2.7.2

1. *$f^\flat(x) = \bigsqcap \{y \,|\, x \leq f^\sharp(y)\}$ and $f^\sharp(y) = \bigsqcup \{x \,|\, f^\flat(x) \leq y\}$, whence lower and upper adjoints uniquely determine each other.*
2. *Lower adjoints preserve all existing suprema; more precisely, if $L \subseteq M$ has a supremum $z \in M$ then $f^\flat(z)$ is the supremum of the image set $f^\flat(L)$. Dually, upper adjoints preserve all existing infima.*
3. *A mapping f on a lattice L has an upper adjoint iff the following conditions are satisfied.*
   - *f is universally disjunctive,*

– $\bigsqcup\{x \mid f(x) \leq y\}$ *exists for all* $y \in L$.

4. *A mapping* g *on a lattice* L *has a lower adjoint iff the following conditions are satisfied.*
   – g *is universally conjunctive and*
   – $\bigsqcap\{y \mid x \leq g(y)\}$ *exists for all* $x \in L$.

Example 2.7.3 Over tests, the shunting rule from Th. 2.1.8.11, specialised by setting $a = r$ and using the $\rightarrow$ notation (see Def. 2.1.1),

$$p \cdot q \leq r \;\Leftrightarrow\; q \leq p \rightarrow r$$

establishes, for every fixed test p, a Galois connection between the functions $(p\,\cdot) =_{df} \lambda x\,.\,p \cdot x$ and the analogous $(p \rightarrow)$.

Similarly, the function $(p\,+)$ on tests is the upper adjoint in the Galois connection

$$p - q \leq r \;\Leftrightarrow\; p \leq q + r\ ,$$

where $p - q = p \cdot \neg q$ (see Def. 2.1.1). From these observations we obtain that

$$(p\,\cdot) \text{ is universally disjunctive} \quad \text{and} \quad (p+) \text{ is universally conjunctive.} \tag{2.7}$$

□

Example 2.7.4 Generalising Ex. 2.7.3, every complete Boolean algebra is completely distributive because of the Galois connection induced by the shunting rule

$$a \sqcap b \leq c \;\Leftrightarrow\; a \leq \overline{b} \sqcup c$$

mentioned already as (1.3). □

We now present further properties of adjoints of Galois connections that are interesting for our considerations. To state them concisely, we use the standard pointwise lifting of partial orders to endofunctions $f, g : L \rightarrow L$ on some partially ordered set L:

$$f \leq g \;\Leftrightarrow_{df}\; \forall\, x : f(x) \leq g(x)\ . \tag{2.8}$$

1. For Galois-connected endofunctions $f^\flat$ and $f^\sharp$ on L we have the *cancellation properties*

$$f^\flat \circ f^\sharp \leq id \quad \text{and} \quad id \leq f^\sharp \circ f^\flat\ , \tag{2.9}$$

   where id is the identity function.
2. $f^\sharp \circ f^\flat \circ f^\sharp = f^\sharp$ and $f^\flat \circ f^\sharp \circ f^\flat = f^\flat$.
3. If f is an isotone endofunction, g an endofunction, and $h^\flat$ and $h^\sharp$ the lower and upper adjoints of some Galois connection on L, then

$$f \circ h^\sharp \leq g \Rightarrow f \leq g \circ h^\flat. \tag{2.10}$$

4. If f is a mapping and g is antitone, then

$$g \circ h^\flat \leq f \Rightarrow g \leq f \circ h^\sharp. \tag{2.11}$$

The domain and predomain operators are neither lower or upper adjoints of Galois connections. This may be surprising, since many properties of domain and codomain also arise from Galois connections. We will see in the next section that Galois connections arise for the modal operators introduced there.

2.8 Modal Operators

We now introduce forward and backward diamond and box operators. As usual, diamonds and boxes are De Morgan duals (Def. 1.2.11).

In a state transition view, the value $|a]q$ of the forward box is a test that contains exactly those states for which all immediate successors (if any) under a lie in q. Hence, while the diamond $|a\rangle q$ expresses the *possibility* of reaching a successor in q, the box expresses a guarantee.

Remark In the I-semiring $\mathsf{REL}(M)$, the forward box operator coincides with the *monotype factor* as defined by Backhouse and van der Woude in [5].

Definition 2.8.1 For a predomain IL-semiring $(S, {}^{\ulcorner})$ we set, for all $a \in S$ and $p \in \mathsf{test}(S)$,

$$|a\rangle p \;=_{df}\; {}^{\ulcorner}(a \cdot p) \;. \tag{2.12}$$

Symmetrically, for a precodomain IL-semiring $(S, {}^{\urcorner})$ we set, for all $a \in S$ and $p \in \mathsf{test}(S)$,

$$\langle a|p \;=_{df}\; (p \cdot a)^{\urcorner} \;. \tag{2.13}$$

Moreover, we define

$$|a]p \;=_{df}\; \neg|a\rangle\neg p \;, \qquad [a|p \;=_{df}\; \neg\langle a|\neg p \;. \tag{2.14}$$

Finally, a *modal IL-semiring* $(S, {}^{\ulcorner}, {}^{\urcorner})$ is a domain and codomain IL-semiring which hence has both forward and backward modal operators. If S is even an I-semiring we call $(S, {}^{\ulcorner}, {}^{\urcorner})$ a *modal I-semiring*.

Let us explain these definitions for the forward case. For $|a\rangle p = {}^{\ulcorner}(a \cdot p)$, by forming $a \cdot p$ we first restrict a to that part where the end states lie in p. Then the starting states of that part, as computed by ${}^{\ulcorner}(a \cdot p)$, are precisely those states that have some a-successor in p. One may therefore also view $|a\rangle p$ as the inverse image of p under a. The box $|a]p = \neg|a\rangle\neg p$ consists of all those states that do not have an a-successor in $\neg p$, i.e., of those states from which all a-transitions are guaranteed to lead to p-states.

The modal operators and pre(co)domain are interdefinable:

$${}^{\ulcorner}a = |a\rangle 1 = \neg|a]0 \;, \qquad a^{\urcorner} = \langle a|1 = \neg[a|0 \;. \tag{2.15}$$

In a predomain or precodomain IL-semiring, De Morgan duality gives, respectively, the *swapping rules*

$$|a\rangle p \leq |b]q \;\Leftrightarrow\; |b\rangle\neg q \leq |a]\neg p \;, \qquad \langle a|p \leq [b|q \;\Leftrightarrow\; \langle b|\neg q \leq [a|\neg p \;. \tag{2.16}$$

Forward and backward operators are also linked by the following properties that are related to the Schröder laws of relational calculus:

$$|a\rangle p \leq q \;\Leftrightarrow\; \langle a|\neg q \leq \neg p \;, \qquad q \leq |a]p \;\Leftrightarrow\; \neg p \leq [a|\neg q \;. \tag{2.17}$$

From domain import/export (Th. 2.4.6.9) as well as from the definition of diamond we immediately obtain two import/export properties for the diamond:

$$|p \cdot a\rangle q = p \cdot |a\rangle q \;, \qquad |a \cdot p\rangle q = |a\rangle(p \cdot q) \;. \tag{2.18}$$

By right-distributivity, the forward modalities are homomorphic w.r.t. $+$:

$$|a+b]p \;=\; (|a]p)\cdot(|b]p)\;, \qquad |a+b\rangle p \;=\; |a\rangle p + |b\rangle p\;. \tag{2.19}$$

Hence box is antitone and diamond is isotone in the first argument:

$$a \le b \;\;\Rightarrow\;\; |a]p \ge |b]p \;\;\wedge\;\; |a\rangle p \le |b\rangle p\;. \tag{2.20}$$

To understand the antitony, recall that the implication order $a \le b$ expresses that b offers at least as many transition possibilities as a. Now, if more choices are offered, one can guarantee less, which is expressed by $|b]p \le |a]p$.

Moreover, both box and diamond are isotone in their second argument:

$$p \le q \;\;\Rightarrow\;\; |a]p \le |a]q \;\;\wedge\;\; |a\rangle p \le |a\rangle q\;. \tag{2.21}$$

Definition 2.8.2 An IL-semiring with a forward or backward diamond operator is called *extensional* if it also satisfies the reverses of the implications (2.20):

$$(\forall\, p : |a]p \ge |b]p) \;\Rightarrow\; a \le b\;, \qquad (\forall\, p : |a\rangle p \le |b\rangle p) \;\Rightarrow\; a \le b\;,$$
$$(\forall\, p : [a|p \ge [b|p) \;\Rightarrow\; a \le b\;, \qquad (\forall\, p : \langle a|p \le \langle b|p) \;\Rightarrow\; a \le b\;.$$

By the swapping rules (2.16) and the Schröder-like rules (2.17) with indirect equality all four conditions are equivalent; hence it is sufficient to stipulate only one of them.

A prominent example is provided by the relational I-semiring $\mathsf{REL}(M)$ over some set M.

Definition 2.8.3 For some of the properties to come it is useful to call a test p *valid*, in signs $\models p$, if $p = 1$.

Then isotony entails

$$\models |a]p \;\;\wedge\;\; p \le q \;\;\Rightarrow\; \models |a]q\;. \tag{2.22}$$

For tests p the forward and backward modalities $|p\rangle$ and $\langle p|$ as well as $|p]$ and $[p|$ coincide. Therefore, we will use the notation $\langle p\rangle$ and $[p]$ for these. Then by Th. 2.4.6.7,

$$\langle p\rangle q = p\cdot q\;, \qquad [p]q = p \to q\;. \tag{2.23}$$

In particular,

$$\langle 1\rangle q = q = [1]q\;, \tag{2.24}$$

i.e., $\langle 1\rangle = [1]$ is the identity function on tests. Moreover,

$$\langle 0\rangle p = 0\;, \qquad [0]p = 1\;. \tag{2.25}$$

Example 2.8.4 From Ex. 2.5.9 and (2.23) we derive for $\mathsf{BOOL}(B)$ that $\langle p\rangle q = p \sqcap q$ and $[p]q = \overline{p} \sqcup q$. □

By Th. 2.4.6.6 and shunting we obtain

$$|a\cdot b\rangle p \le |a\rangle|b\rangle p\;, \qquad |a\cdot b]p \ge |a]|b]p\;. \tag{2.26}$$

Likewise Th.2.6.2.6 implies

$$\langle a\cdot b|p \le \langle b|\langle a|p\;, \qquad [a\cdot b|p \ge [b|[a|p\;. \tag{2.27}$$

If the underlying IL-semiring is even a domain IL-semiring, by the locality property (d3) of domain and Lm. 2.4.8 we obtain multiplicativity of the forward modal operators:

$$|a \cdot b\rangle p \;=\; |a\rangle|b\rangle p \;, \qquad\qquad |a \cdot b]p \;=\; |a]|b]p \;. \tag{2.28}$$

Via the connection (2.15) these properties are even equivalent to (d3). Likewise (cd3) is equivalent to

$$\langle a \cdot b|p \;=\; \langle b|\langle a|p \;, \qquad\qquad [a \cdot b|p \;=\; [b|[a|p \;. \tag{2.29}$$

We now give a characterisation of the forward box operator.

Lemma 2.8.5 *Let S be an IL-semiring and assume a family $(f_a)_{a \in S}$ of endofunctions $f_a : \mathsf{test}(S) \to \mathsf{test}(S)$ that each satisfy*

$$\forall\, p, q \in \mathsf{test}(S) : p \leq f_a(q) \;\Leftrightarrow\; p \cdot a \cdot \neg q \leq 0 \;. \tag{2.30}$$

1. *Setting $\ulcorner a \;=_{df}\; \neg f_a(0)$ for all $a \in S$ makes $(S, \ulcorner)$ a predomain IL-semiring.*
2. *If $(S, \ulcorner)$ is a predomain IL-semiring then for all $a \in S, q \in \mathsf{test}(S)$ we have $f_a(q) = |a]q$.*
3. *If, additionally, for all $a, b \in S$ we have $f_{a \cdot b} = f_a \circ f_b$ then the predomain operator defined in Part 1 is even a domain operator and consequently satisfies the multiplicativity properties* (2.28)*.*

Proof.

1. We calculate, using the definition of $\ulcorner$, double negation, the assumption about the f_a, $\neg 0 = 1$ and neutrality of 1,
$$p \leq \neg\ulcorner a \;\Leftrightarrow\; p \leq \neg\neg f_a(0) \;\Leftrightarrow\; p \leq f_a(0) \;\Leftrightarrow\; p \cdot a \cdot \neg 0 \leq 0 \;\Leftrightarrow\; p \cdot a \leq 0 \;.$$
Now (gla) and the uniqueness of predomain (Lm. 2.4.5) show the claim.
2. Using the assumption about the f_a, (gla) and the definition of box, we obtain
$$p \leq f_a(q) \;\Leftrightarrow\; p \cdot a \cdot \neg q \leq 0 \;\Leftrightarrow\; p \leq \neg\ulcorner(a \cdot \neg q) \;\Leftrightarrow\; p \leq |a]q \;,$$
so that indirect equality shows the claim.
3. We calculate, using Part 1, the additional assumption, Boolean algebra, Part 1, Parts 1 and 2, (2.14) and (2.12),
$$\begin{aligned} \ulcorner(a \cdot b) \;&=\; \neg f_{a \cdot b}(0) \;=\; \neg f_a(f_b(0)) \;=\; \neg f_a(\neg\neg f_b(0)) \\ &=\; \neg f_a(\neg\ulcorner b) \;=\; \neg|a]\neg\ulcorner b \;=\; |a\rangle\ulcorner b \;=\; \ulcorner(a \cdot \ulcorner b) \;. \end{aligned}$$

□

By this lemma and Lm. 2.2.3 we obtain the following equivalent characterisations of the forward box operator:

$$p \leq |a]q \;\Leftrightarrow\; p \cdot a \cdot \neg q \leq 0 \;\Leftrightarrow\; a \cdot \neg q \leq \neg p \cdot a \;\Leftrightarrow\; \{p\}\; a\; \{q\} \;. \tag{2.31}$$

The relation with the Hoare triple $\{p\}\; a\; \{q\}$ (see Def. 2.2.4) again exhibits the guarantee character of the box operator. It also shows that the forward box operator $|a]q$ is an algebraic abstraction of the *weakest liberal precondition* $\mathsf{wlp}(a, q)$ introduced in [24]: in a concrete setting, that predicate characterises the largest set of states from which a-transitions are guaranteed to lead to states in q (if to any at all).

The modal operators satisfy a rich set of further properties which will be used extensively throughout the remainder of the book. Many of them are well known from the field of modal logic, see e.g. [58], or early work on Boolean algebras with operators [38].

Lemma 2.8.6 *In a left-distributive predomain IL-semiring S we have the following additional properties:*

1. *Box is conjunctive and diamond is disjunctive in the second argument:*
$$|a](p \cdot q) = |a]p \cdot |a]q \ , \qquad |a\rangle(p + q) = |a\rangle p + |a\rangle q \ . \tag{2.32}$$
2. *Box satisfies Axiom* K *of modal logic (*modal modus ponens*) and diamond its dual:*
$$|a](p \to q) \leq |a]p \to |a]q \ , \qquad |a\rangle p - |a\rangle q \leq |a\rangle(p - q) \ . \tag{2.33}$$
*By shunting, the above laws are equivalent to the following forms (*modal modus tollens*, given only for box):*
$$|a](p \to q) \cdot \neg|a]q \leq \neg|a]p \ , \qquad |a](p + q) \cdot \neg|a]q \leq \neg|a]\neg p \ . \tag{2.34}$$
3. *Box satisfies the following propagation law:*
$$(|a]q) \cdot a \ = \ (|a]q) \cdot a \cdot q \ , \tag{2.35}$$
which means that starting in a state for which all a-successors guarantee q allows indeed asserting q as a postcondition of a. This law entails
$$\models |a]q \ \Rightarrow \ a \ = \ a \cdot q \ . \tag{2.36}$$
In a full I-semiring also the reverse implication holds, which further entails $\models |a \cdot q]q$, since $a \cdot q \ = \ a \cdot q \cdot q$.

Proof.

1. We show the property for diamond; the one for box follows from that by straightforward De Morgan dualisation. By the definition of diamond, left distributivity, distributivity of domain (Th. 2.4.6.10) and the definition of diamond again,
$|a\rangle(p+q) = \lceil(a \cdot (p+q)) = \lceil(a \cdot p + a \cdot q) = \lceil(a \cdot p) + \lceil(a \cdot q) = |a\rangle p + |a\rangle q$.
2. We use that every disjunctive endofunction f and every conjunctive endofunction g on a Boolean algebra satisfy, for all elements p and q,
$$f(p) - f(q) \leq f(p - q) \quad \text{and} \quad g(p \to q) \leq g(p) \to g(q) \tag{2.37}$$
(see e.g [38]). By conjunctivity of box and disjunctivity of diamond, the claimed properties are instances of (2.37) with $f = |a\rangle$ and $g = |a]$. Nevertheless, for the readers' benefit, we show the properties for box; the ones for diamond follow from that by straightforward De Morgan dualisation. By shunting, conjunctivity of box, Boolean algebra and $p \leq 1$ with isotony of box,
$$\begin{aligned} &|a](p \to q) \leq |a]p \to |a]q \ \Leftrightarrow \ |a](p \to q) \cdot |a]p \leq |a]q \\ &\Leftrightarrow \ |a]((p \to q) \cdot p) \leq |a]q \ \Leftrightarrow \ |a](q \cdot p) \leq |a]q \ \Leftrightarrow \ \mathsf{TRUE} \ . \end{aligned}$$
Now, by definition of $\to$, contraposition and shunting,
$$\begin{aligned} |a](p \to q) \leq |a]p \to |a]q \ &\Leftrightarrow \ |a](p \to q) \leq \neg|a]q \to \neg|a]p \\ &\Leftrightarrow \ |a](p \to q) \cdot \neg|a]q \leq \neg|a]p \ . \end{aligned}$$

3. For (2.35) we have, by neutrality of 1, the definition of complement and left distributivity,

$$(\lfloor a]q)\cdot a = (\lfloor a]q)\cdot a\cdot(q+\neg q) = (\lfloor a]q)\cdot a\cdot q + (\lfloor a]q)\cdot a\cdot\neg q\ .$$

Now, by definition of box and Th. 2.4.6.3

$$(\lfloor a]q)\cdot a\cdot\neg q = \neg\ulcorner(a\cdot\neg q)\cdot a\cdot\neg q = 0$$

and we are done.

From this (2.36) is immediate, since $\models \lfloor a]q \Leftrightarrow \lfloor a]q = 1$ by Def. 2.8.3.

For the last claim assume $a = a\cdot q$. Then by right-strictness

$$a\cdot\neg q = a\cdot q\cdot\neg q = a\cdot 0 = 0\ .$$

Now, by neutrality of 1, reflexivity of $\leq$, (2.31) and greatestness of 1,

$$a\cdot\neg q = 0 \Leftrightarrow 1\cdot a\cdot\neg q\leq 0 \Leftrightarrow 1\leq\lfloor a]q \Leftrightarrow\models\lfloor a]q\ .$$

□

Next we note the following fact.

Lemma 2.8.7 *A left-distributive predomain IL-semiring S is an I-semiring iff box satisfies Axiom* M *of modal logic and diamond its dual; algebraically they read*

$$\lfloor a]1 = 1\ , \qquad \lfloor a\rangle 0 = 0\ . \tag{2.38}$$

Hence, if (2.38) holds then $\models p \Rightarrow\models\lfloor a]p$. A consequence of (2.38) and (2.33) is

$$\models p\to q \Rightarrow\models\lfloor a]p\to\lfloor a]q\ . \tag{2.39}$$

Now we state a few properties concerning the interaction between forward and backward modal operators.

Lemma 2.8.8 *In a modal IL-semiring box and diamond satisfy*

$$p\leq\lfloor a]q \Rightarrow \langle a\rfloor p\leq q\ .$$

In a modal I-semiring this strengthens to the exchange law

$$p\leq\lfloor a]q \Leftrightarrow \langle a\rfloor p\leq q\ , \tag{2.40}$$

which establishes a Galois connection between $\lfloor a]$ and $\langle a\rfloor$. In this case, De Morgan duality entails a symmetric Galois connection between $[a\rfloor$ and $\lfloor a\rangle$:

$$p\leq[a\rfloor q \Leftrightarrow \lfloor a\rangle p\leq q\ . \tag{2.41}$$

Proof. Let us work out, using the definitions, the meaning of the two formulas involved in that law in a modal IL-semiring. By Boolean algebra and (gla)/(wgra), we obtain

$$p\leq\lfloor a]q \Leftrightarrow p\leq\neg\ulcorner(a\cdot\neg q) \Leftrightarrow p\cdot a\cdot\neg q\leq 0$$

and

$$\langle a\rfloor p\leq q \Leftrightarrow (p\cdot a)^{\urcorner}\leq q \Leftrightarrow \neg q\leq\neg(p\cdot a)^{\urcorner} \Leftrightarrow p\cdot a\cdot\neg q\leq p\cdot a\cdot 0\ . \tag{dia1}$$

This shows the first claim, since $p\cdot a\cdot\neg q\leq 0$ implies $p\cdot a\cdot\neg q\leq p\cdot a\cdot 0$.

For the second claim we use that in a modal I-semiring 0 is also a right annihilator; hence always $p\cdot a\cdot 0 = 0$.

The third claim follows by straightforward Boolean algebra. □

The Galois connections have interesting consequences. In particular, diamonds (boxes) of strict elements commute with all existing suprema (infima) of the test algebra.

2.9 Modal Operators as Semiring Elements

Many properties of a modal IL-semiring $(S, {}^{\ulcorner}, {}^{\urcorner})$ can be expressed more succinctly in the endofunction space $\mathsf{test}(S) \to \mathsf{test}(S)$. The IL-semiring operators are lifted pointwise as

$$(f \pm g)(p) = f(p) \pm g(p)\ ,\ \ (f \sqcap g)(p) = f(p) \cdot g(p)\ ,\ \ (f \circ g)(p) = f(g(p)) \tag{2.42}$$

and likewise for the other Boolean operators. In particular, $\langle 1]$ and $\langle 0]$ are the identity and the constant 0-valued function on tests, respectively. Some immediate consequences of the pointwise lifting are the properties

$$(f \pm g) \circ h = f \circ h \pm g \circ h\ , \qquad (f \sqcap g) \circ h = f \circ h \sqcap g \circ h\ . \tag{2.43}$$

For the special case of modal operators we obtain the additive distribution properties

$$|a + b\rangle = |a\rangle + |b\rangle, \qquad |a + b] = |a] \sqcap |b] \tag{2.44}$$

and the covariant and contravariant multiplicative distribution properties

$$\left.\begin{array}{ll} |a \cdot b\rangle = |a\rangle \circ |b\rangle\ , & \langle a \cdot b| = \langle b| \circ \langle a|\ , \\ |a \cdot b] = |a] \circ |b]\ , & [a \cdot b| = [b| \circ [a|\ . \end{array}\right\} \tag{2.45}$$

We will apply them tacitly most of the time. In Def. 1.2.8 Property 2.44 has been called "disjunctivity" (in the left argument of diamond), but in the setting of IL-semirings "additivity" seems more natural. Moreover, it corresponds to "multiplicativity" 2.45.

This lifting yields further interesting operator-level laws. The Galois connections (2.41) and (2.40) extend to endofunctions f and g on $\mathsf{test}(S)$:

$$|a\rangle \circ f \leq g \Leftrightarrow f \leq [a| \circ g, \qquad \langle a| \circ f \leq g \Leftrightarrow f \leq |a] \circ g. \tag{2.46}$$

This implies the following cancellation properties, instantiated from (2.9):

$$|a\rangle \circ [a| \leq \langle 1] \leq [a| \circ |a\rangle, \qquad \langle a| \circ |a] \leq \langle 1\rangle \leq |a] \circ \langle a|. \tag{2.47}$$

These allow the following calculation for isotone operators f and g:

$$\begin{aligned} f \circ |a] \leq g \Rightarrow f \circ |a] \circ \langle a| \leq g \circ \langle a| \Rightarrow f \leq g \circ \langle a| \\ \Rightarrow f \circ |a] \leq g \circ \langle a| \circ |a] \Rightarrow f \circ |a] \leq g\ . \end{aligned}$$

A similar derivation works for antitone operators. Hence we have the additional Galois connections

$$\begin{array}{ll} f \circ |a] \leq g \Leftrightarrow f \leq g \circ \langle a| & \text{if } f \text{ and } g \text{ are isotone,} \\ f \circ |a\rangle \leq g \Leftrightarrow f \leq g \circ [a| & \text{if } f \text{ and } g \text{ are antitone.} \end{array}$$

Moreover, diamonds are isotone and boxes are antitone, that is,

$$a \leq b \Rightarrow |a\rangle \leq |b\rangle, \quad a \leq b \Rightarrow |b] \leq |a]. \tag{2.48}$$

Diamonds and boxes in a left-distributive IL-semiring satisfy variants of (2.33), that is,

$$|a] \circ (f \to g) \leq |a] \circ f \to |a] \circ g \ , \qquad |a\rangle \circ f - |a\rangle \circ g \leq |a\rangle \circ (f - g) \ . \tag{2.49}$$

The proof proceeds as the one for Lm. 2.8.6.2.

Finally, the above laws entail the following lifting property.

Theorem 2.9.1 *The set of forward diamonds of a predomain IL-semiring and the set of backward diamonds of a precodomain IL-semiring each form an IL-semiring.*

The point-free style and the properties of the operator algebra yield more concise specifications and proofs in the following sections.

Chapter 3
Iteration: Kleene and Omega Algebras

Iteration, like friction, is likely to generate heat instead of progress.
— George Eliot

3.1 Elements of Fixed Point Theory

As is well known, there is a close connection between iteration and recursion. The basis of mathematical semantics is fixed point theory, of which we recapitulate some basic facts here.

Definition 3.1.1 Let f be an endofunction on a poset $(A, \leq)$.

1. An element $a \in A$ is a *pre-fixed point* of f if $f(a) \leq a$. The notion of *post-fixed point* is order-dual, and a is a *fixed point* of f if it is both a pre- and a post-fixed point. The set of all fixed points of f is denoted by $\mathsf{fix}\, f$.
2. An element is called the *least (pre-)fixed point* of f if it is the least element of the set of (pre-)fixed points of f. The notion of *greatest (post-)fixed point* is order-dual. Note that neither of these elements need exist.
3. The least and greatest fixed points of f are denoted by μf and νf, resp., when they exist. If $f(x) = E$, where E is an expression containing the variable x, we write $\mu x \,.\, E$ and $\nu x \,.\, E$ instead of μf and νf.

The following fundamental theorem, in particular Part 4, is due to Knaster and Tarski [62].

Theorem 3.1.2 (Knaster/Tarski) *Consider a partial order $(M, \leq)$ and an isotone endofunction $f : M \to M$.*

1. *If f has a least pre-fixed point $u \in M$ then $u = \mu f$, i.e., u is also the least fixed point of f. In formulas,*
$$f(u) \leq u \;\wedge\; (\forall\, y : f(y) \leq y \;\Rightarrow\; u \leq y)) \;\Rightarrow\; u = \mu f \;. \tag{3.1}$$
Moreover, again under the hypothesis that f has a least pre-fixed point, we have the principle of least fixed point induction*:*
$$f(x) \leq x \;\Rightarrow\; \mu f \leq x \;. \tag{3.2}$$
2. *Analogously, if f has a greatest post-fixed point $u \in M$ then it is also the greatest fixed point νf of f. In formulas,*

$$u \leq f(u) \wedge (\forall\, y : y \leq f(y) \;\Rightarrow\; y \leq u)) \;\Rightarrow\; u = \nu f \;. \tag{3.3}$$

Moreover, again under the hypothesis that f has a greatest post-fixed point, we have the principle of greatest fixed point co-induction*:*

$$x \leq f(x) \;\Rightarrow\; x \leq \nu f \;. \tag{3.4}$$

3. *Let also $g : M \to M$ be isotone and satisfy $f \leq g$, i.e., $\forall\, x : f(x) \leq g(x)$. If the set of pre-fixed points of f has a least element μf then $\mu f \leq u$ for every pre-fixed point u of g. In particular, if μg exists then $\mu f \leq \mu g$. Analogously, if g has a greatest post-fixed point νg, then also $u \leq \nu g$ for every post-fixed point u of f. In particular, if νf exists then $\nu f \leq \nu g$.*
4. *If $(M, \leq)$ is even a complete lattice then μf and νf exist and satisfy*

$$\begin{array}{rcl} \mu f & = & \bigsqcap \{x \,|\, f(x) = x\} \;=\; \bigsqcap \{x \,|\, f(x) \leq x\} \;, \\ \nu f & = & \bigsqcup \{x \,|\, f(x) = x\} \;=\; \bigsqcup \{x \,|\, x \leq f(x)\} \;. \end{array}$$

In Th. 3.1.2.3 the assumptions about existence of a least pre-fixed or greatest post-fixed point cannot be dropped as the following example shows.

Example 3.1.3 Let $M =_{df}]0, 3] \subseteq \mathbb{R}$ with the canonical order and consider the isotone functions $f, g : M \to M$ defined by

$$f(x) =_{df} \begin{cases} x/2 & \text{if } x < 2, \\ x & \text{otherwise,} \end{cases} \qquad g(x) =_{df} \begin{cases} x/2 & \text{if } x < 1, \\ x & \text{otherwise.} \end{cases}$$

Then $f \leq g$, but $\mu g = 1 < \mu f = 2$. Note that neither f nor g has a least pre-fixed point. □

Moreover, existence of a least/greatest fixed point need not imply existence of a least pre-fixed/greatest post-fixed point, and hence the induction principles (3.2) and (3.4) need not hold in arbitrary partial orders.

Example 3.1.4 Let $M = \mathbb{N}$ with the standard partial order and define $f : M \to M$ by $f(0) = 0$ and $f(n) = n + 1$ for $n > 0$. Then f is isotone and all elements x are *expanded* by f, i.e., satisfy $x \leq f(x)$. It has the unique fixed point 0, hence $\mu f = 0 = \nu f$. But $x \leq f(x) \;\Rightarrow\; x \leq \nu f$ holds only for $x = 0$. □

In the case of a Boolean lattice, least and greatest fixed points can be related via the dual functions introduced in Def. 1.2.11.

Lemma 3.1.5 *Let f be a function on a Boolean lattice and f° its dual. If μf exists then also νf° exists and $\nu f^\circ = \overline{\mu f}$. Likewise, if νf exists then also μf° exists and $\mu f^\circ = \overline{\nu f}$.*

We now mention two very useful groups of fixed point fusion laws (see e.g. [4] for further fixed point properties). They allow fusing the application of some function g with the recursion described by a function h, yielding a recursion described by a function f. Let $f, g, h : L \to L$ be isotone functions on a complete lattice $(L, \leq)$ with least element $\bot$ and greatest element $\top$. Then we have the *μ-super-fusion* law

$$g \circ h \geq f \circ g \;\Rightarrow\; g(\mu h) \geq \mu f \;. \tag{3.5}$$

If g is continuous (cf. Def. 1.2.8) and satisfies $g(\bot) \leq \mu f$ then we have the *μ-sub-fusion and μ-fusion* laws

$$g \circ h \leq f \circ g \;\Rightarrow\; g(\mu h) \leq \mu f \;, \qquad g \circ h = f \circ g \;\Rightarrow\; g(\mu h) = \mu f \;. \tag{3.6}$$

Dually we have the *ν-sub-fusion* law

$$g \circ h \leq f \circ g \;\Rightarrow\; g(\nu h) \leq \nu f \;. \tag{3.7}$$

If g is co-continuous (cf. Def. 1.2.8) and satisfies $g(\top) \geq \nu f$ then we have the *ν-super-fusion and ν-fusion* laws

$$g \circ h \geq f \circ g \;\Rightarrow\; g(\nu h) \geq \nu f \;, \qquad g \circ h = f \circ g \;\Rightarrow\; g(\nu h) = \nu f \;. \tag{3.8}$$

The notion of (co-)continuity has another important application which is due to Kleene in [40].

Theorem 3.1.6 (Kleene) *Assume again a complete lattice L and an endo-function $f : L \to L$. For $x \in L$ set $f^0(x) =_{df} x$ and $f^{i+1}(x) =_{df} f(f^i(x))$. If f is continuous then*

$$\mu f \;=\; \bigsqcup \{ f^i(\bot) \,|\, i \in \mathbb{N} \} \;.$$

Dually, if f is co-continuous then

$$\nu f \;=\; \bigsqcap \{ f^i(\top) \,|\, i \in \mathbb{N} \} \;.$$

This allows iterative computation of μf and νf.

3.2 Finite Iteration: Left Kleene Algebras

The central operator that moves an I-semiring to a Kleene algebra [13] is the star that models arbitrary but finite iteration. Fortunately, we can reuse the conventional definition [43] for our setting of IL-semirings.

In axiomatising iteration we deal with iteration "on the left" and "on the right" separately, since in presence of infinite computations the "right side" is never reached. This is reflected in the following definition.

Definition 3.2.1 A *left-inductive left Kleene algebra* is a structure $(S, {}^*)$ such that S is an IL-semiring and the star operator ${}^* : S \to S$ satisfies, for all $a, b, c \in S$, the *left star unfold* and *left star induction* axioms

$$1 + a \cdot a^* \;\leq\; a^* \;, \tag{3.9}$$

$$b + a \cdot c \leq c \;\Rightarrow\; a^* \cdot b \leq c \;. \tag{3.10}$$

If S is even an I-semiring the we call it a *left-inductive Kleene algebra*.

These axioms are close in spirit to the characterisation of a least pre-fixed point in the premiss of (3.1). Before we derive further properties from them we show an important result about the existence of the star operator in left quantales.

Theorem 3.2.2 ([52])

1. *Every left quantale can uniquely be extended to a left-inductive left Kleene algebra by defining* $a^* =_{df} \mu h$ *with* $h(x) =_{df} 1 + a \cdot x$.
2. *If the left quantale is left-distributive one has*
$$a^* = \bigsqcup \{a^i \mid i \in \mathbb{N}\} .$$

Proof.

1. The left unfold axiom holds by the definition of a^*. We show that $a^* \cdot b = \mu f$ with $f(x) =_{df} b + a \cdot x$, which entails the left star induction axiom by Th. 3.1.2.1.
   First, by definition of f, neutrality of 1, right distributivity, star unfold and isotony,
   $$f(a^* \cdot b) = b + a \cdot a^* \cdot b = (1 + a \cdot a^*) \cdot b \leq a^* \cdot b .$$
   Hence $a^* \cdot b$ is a pre-fixed point of f and least fixed point induction (3.2) shows $\mu f \leq a^* \cdot b$.
   Second, since we assume a left quantale, the function $g(x) =_{df} x \cdot b$ is universally disjunctive, hence continuous, and satisfies $g(0) = 0 \leq \mu h$. Moreover, by definition of g and f, right distributivity, neutrality of 1 and the definitions of f and g,
   $$g(h(x)) = (1 + a \cdot x) \cdot b = b + a \cdot x \cdot b = f(g(x)) .$$
   Therefore sub-fusion (3.6) implies $a^* \cdot b = g(\mu h) \leq \mu f$ and the left star induction axiom is shown.
   Finally, uniqueness of the extension is proved as follows. If $a^\star =_{df} \mu g$ for some other function g and if $a^\star$ satisfies the unfold and induction axioms, then $a^* \leq a^\star$, since $a^* \leq a^\star \Leftarrow 1 + a \cdot a^\star \leq a^\star$. Similarly, $a^\star \leq a^*$, so that $a^\star = a^*$.
2. By Kleene's Theorem 3.1.6 we have $a^* = \mu h = \bigsqcup H$ where
   $$H =_{df} \{h^i(0) \mid i \in \mathbb{N}\} .$$
   A straightforward induction on i using left distributivity shows $h^i(0) = \sum_{j<i} a^j + a^i \cdot 0$. Now let
   $$K =_{df} \{a^i \mid i \in \mathbb{N}\} .$$
   Every upper bound of H is also an upper bound of K, since for each $a^i \in K$ we have $a^i \leq h^{i+1}(0)$. Conversely, every upper bound b of K is also an upper bound of H, since for each $h^i(0) \in H$ we have $h^i(0) \leq \sum_{j \leq i} a^j \leq b$ by the supremum property of $+$. Since H and K have the same upper bounds, also their suprema coincide, which shows the claim. □

By this theorem, the left quantales $\mathsf{WOR}(\Sigma)$ and $\mathsf{STR}(\Sigma)$ can be extended to left-inductive left Kleene algebras. We will discuss this in more detail below.

The left star axioms already imply many laws of standard Kleene algebra.

Lemma 3.2.3 *The following properties hold in a left-inductive left Kleene algebra.*

1. *The element $a^* \cdot b$ is the least pre-fixed point and the least fixed point of the function $\lambda x \,.\, b + a \cdot x$.*
2. $a^* = 1 + a \cdot a^*$.
3. *The star operator is characterised uniquely by the axioms.*
4. *The star operator is isotone with respect to the natural ordering.*
5. $a \leq 1 \Rightarrow a^* = 1$.
6. $a \leq a^*$.
7. $a^* \cdot a^* = a^*$. (Idempotence I)
8. $(a^*)^* = a^*$. (Idempotence II)
9. $(a + b)^* = a^* \cdot (b \cdot a^*)^*$. (Star of Sum)
10. $a \cdot c \leq c \cdot b \Rightarrow a^* \cdot c \leq c \cdot b^*$. (Semicommutation I)
11. $a^* \cdot a \leq a \cdot a^*$. (Semi-Selfcommutation I)
12. $1 + a^* \cdot a \leq a^*$. (Right Star Unfold)
13. $(a \cdot b)^* \cdot a \leq a \cdot (b \cdot a)^*$. (Semi-Sliding I)
14. $\forall\, n \in \mathbb{N} : a^n \leq a^*$.
15. *If a is right-strict, i.e., $a \cdot 0 = 0$, then so is a^*.*

Proof.

1. From Axiom (3.9) we infer by neutrality of 1 and right distributivity that $b + a \cdot a^* \cdot b \leq a^* \cdot b$, so $a^* \cdot b$ is a pre-fixed point of the function. Now the claim follows by Axiom (3.10) and Th. 3.1.2.1.
2. This results from Part 1 by setting $b = 1$ and using neutrality of 1.
3. This holds by the uniqueness of least fixed points.
4. This is immediate from Parts 1 and 2 together with Th. 3.1.2.3.
5. The inequation $1 \leq a^*$ holds by (3.9). The reverse inclusion reduces by (3.10) to $1 + a \cdot 1 \leq 1$, which holds by neutrality of 1 and the assumption $a \leq 1$.
6. Using neutrality of 1 and (3.9) we have $a = a \cdot 1 \leq a \cdot a^* \leq a^*$.
7. $(\geq)$ follows by neutrality of 1, by $1 \leq a^*$ and isotony. $(\leq)$ reduces by (3.10) to $a^* + a \cdot a^* \leq a^*$, which holds by lattice algebra and (3.9).
8. $(\geq)$ follows by Part 6 and isotony, while $(\leq)$ by (3.10) reduces to $1 + a^* \cdot a^* \leq a^*$, which holds by (3.9) and Part 7.
9. By Parts 7 and 8, (3.9) and isotony we get
   $$(a + b)^* = (a + b)^* \cdot ((a + b)^*)^* \geq a^* \cdot ((a + b) \cdot (a + b)^*)^* \geq a^* \cdot (b \cdot a^*)^* \,.$$
   The reverse inequality reduces by (3.10) to $1 + (a + b) \cdot a^* \cdot (b \cdot a^*)^* \leq a^* \cdot (b \cdot a^*)^*$. This follows by commutativity with right distributivity, Part 2, right distributivity with neutrality of 1, and Part 2 again:
   $$\begin{aligned} 1 + (a + b) \cdot a^* \cdot (b \cdot a^*)^* &= 1 + b \cdot a^* \cdot (b \cdot a^*)^* + a \cdot a^* \cdot (b \cdot a^*)^* \\ &= (b \cdot a^*)^* + a \cdot a^* \cdot (b \cdot a^*)^* \\ &= (1 + a \cdot a^*) \cdot (b \cdot a^*)^* = a^* \cdot (b \cdot a^*)^* \,. \end{aligned}$$
10. Assume $a \cdot c \leq c \cdot b$. The result follows from (3.9) with isotony, the assumption with isotony, $1 \leq b^*$ with isotony and neutrality of 1, and (3.10): $\mathsf{TRUE} \Leftrightarrow c \cdot b \cdot b^* \leq c \cdot b^* \Rightarrow a \cdot c \cdot b^* \leq c \cdot b^* \Leftrightarrow c + a \cdot c \cdot b^* \leq c \cdot b^* \Rightarrow a^* \cdot c \leq c \cdot b^*$.
11. Immediate from Part 10 by setting $b = c = a$.

12. Immediate from Part 11 and (3.9).
13. By (3.10) the claim reduces to $a + a \cdot b \cdot a \cdot (b \cdot a)^* \leq a \cdot (b \cdot a)^*$. But $a \leq a \cdot (b \cdot a)^*$ follows from $1 \leq (b \cdot a)^*$, identity of 1 and isotony, while $a \cdot b \cdot a \cdot (b \cdot a)^* \leq a \cdot (b \cdot a)^*$ follows from (3.9) and isotony.
14. We show this by induction on n. For $n = 0$ we have $a^0 = 1 \leq a^*$ by (3.9). Assuming $a^n \leq a^*$, by isotony and (3.9) again, $a^{n+1} = a \cdot a^n \leq a \cdot a^* \leq a^*$.
15. This is immediate from left star induction (3.10) with $b = c = 0$. □

Definition 3.2.4 In a left-inductive left Kleene algebra, the *transitive closure* of a is

$$a^+ =_{df} a \cdot a^*.$$

The above results entail the following properties of transitive closure.

Lemma 3.2.5

1. $a^+ \leq a^*$.
2. $a \leq a^+$.
3. $a^* \cdot a^+ = a^+ = a^+ \cdot a^*$.
4. $a \cdot a^+ \leq a^+$ *and* $a^+ \cdot a \leq a^+$.
5. $a^+ \cdot a^+ \leq a^+$.
6. $(a^+)^+ = a^+$.

Proof.

1. This is immediate from the definition of transitive closure and star unfold (3.9).
2. By neutrality of 1 with $1 \leq a^*$ by star unfold and the definition of transitive closure we have
$$a = a \cdot 1 \leq a \cdot a^* = a^+ .$$
3. For the first equation we calculate, using Lm. 3.2.3.2, right distributivity and neutrality of 1,
$$a^* \cdot a^+ = (1 + a \cdot a^*) \cdot a^+ = a^+ + a \cdot a^* \cdot a^+ .$$
For the second summand we obtain, by Part 1 with isotony, Lm. 3.2.3.7 and the definition of transitive closure,
$$a \cdot a^* \cdot a^+ \leq a \cdot a^* \cdot a^* = a \cdot a^* = a^+ ,$$
and lattice algebra shows the claim.
For the second equation we have, by the definition of transitive closure, Lm. 3.2.3.7 and the definition of transitive closure again,
$$a^+ \cdot a^* = a \cdot a^* \cdot a^* = a \cdot a^* = a^+ .$$
4. By Lm. 3.2.3.6 and Part 3,
$$a \cdot a^+ \leq a^* \cdot a^+ = a^+ \quad \text{and} \quad a^+ \cdot a \leq a^+ \cdot a^* = a^+ .$$
5. By Part 1 with isotony, Part 3 and the definition of transitive closure,
$$a^+ \cdot a^+ \leq a^+ \cdot a^* = a^+ .$$
6. ($\geq$) follows from Part 2.
($\leq$) We have

$$
\begin{array}{ll}
& (a^+)^+ \leq a^+ \\
\Leftrightarrow & a \cdot a^* \cdot (a^+)^* \leq a \cdot a^* \quad \{\!\![\text{ definition of transitive closure thrice }]\!\!\} \\
\Leftarrow & a^* \cdot (a^+)^* \leq a^* \quad \{\!\![\text{ isotony }]\!\!\} \\
\Leftarrow & (a^+)^* + a \cdot a^* \leq a^* \quad \{\!\![\text{ left star induction (3.10) }]\!\!\} \\
\Leftrightarrow & (a^+)^* \leq a^* \quad \{\!\![\text{ left star unfold (3.9), lattice algebra }]\!\!\} \\
\Leftarrow & (a^*)^* \leq a^* \quad \{\!\![\text{ Part 1, isotony of star }]\!\!\} \\
\Leftrightarrow & \mathsf{TRUE}\ . \quad \{\!\![\text{ Lm. 3.2.3.8 }]\!\!\}
\end{array}
$$

The following definition enforces a more symmetric behaviour of iteration.

Definition 3.2.6 A left-inductive left Kleene algebra is *right-inductive* if it also satisfies the *right star induction* axiom

$$b + c \cdot a \leq c \Rightarrow b \cdot a^* \leq c\ . \tag{3.11}$$

In a right-inductive and left-inductive left Kleene algebra, the properties of Semicommutation I, Semi-Selfcommutation I and Semi-Sliding I of Lm. 3.2.3 can be mirrored or strengthened.

Lemma 3.2.7 *The following additional laws hold in a right-inductive and left-inductive left Kleene algebra.*

1. $c \cdot a \leq b \cdot c \Rightarrow c \cdot a^* \leq b^* \cdot c$. (Semicommutation II)
2. $a \cdot a^* \leq a^* \cdot a$ *and hence* $a \cdot a^* = a^* \cdot a$. (Semi-Selfcommutation II)
3. $a \cdot (b \cdot a)^* \leq (a \cdot b)^* \cdot a$ *and hence* $a \cdot (b \cdot a)^* = (a \cdot b)^* \cdot a$. (Semi-Sliding II)
4. $b \cdot a^*$ *is the least pre-fixed point and least fixed point of the function* $\lambda x\,.\,x \cdot a + b$.

Proof.

1. Assume $c \cdot a \leq b \cdot c$. The result follows from Lm. 3.2.3.12 with isotony, the assumption with isotony, $1 \leq b^*$ with isotony and neutrality of 1, and (3.11): $\mathsf{TRUE} \Leftrightarrow b^* \cdot b \cdot c \leq b^* \cdot c \Rightarrow b^* \cdot c \cdot a \leq b^* \cdot c \Leftrightarrow c + b^* \cdot c \cdot a \leq b^* \cdot c \Rightarrow c \cdot a^* \leq b^* \cdot c$.
2. Immediate from $a \cdot a \leq a \cdot a$ and Part 1.
3. We only need to show that $b \cdot a^*$ is a pre-fixed point of the function, since (3.11) then asserts that it is a least pre-fixed point and thus also a least fixed point. By isotony, hence super-disjunctivity, and Lm. 3.2.3.12 we have $b + b \cdot a^* \cdot a \leq b \cdot (1 + a^* \cdot a) \leq b \cdot a^*$.
4. By (3.11) the proof is completely symmetric to that of Lm. 3.2.3.13. □

Definition 3.2.8 *Right-inductive right Kleene algebras* are the duals of left-inductive left Kleene algebras with respect to opposition, that is, they are IR-semirings that satisfy the *right star unfold* and *right star induction* axioms $1 + a^* \cdot a \leq a^*$ and $b + c \cdot a \leq c \Rightarrow b \cdot a^* \leq c$ mentioned in Lm. 3.2.3.12 and (3.11). A left-distributive IL-semiring that is both a left-inductive left and a right-inductive right Kleene algebra is called a *left-distributive Kleene algebra*. Finally, a *full Kleene algebra*, for short *Kleene algebra*, is a left-distributive Kleene algebra that is an I-semiring.

In a Kleene algebra Def. 3.2.4 implies

$$a^+ = a \cdot a^* = a^* \cdot a \ . \tag{3.12}$$

3.3 Examples of Kleene Algebras

Example 3.3.1 We reconsider the finite I-semirings from Sect. 1.5.

- S_2 from Ex. 1.5.1 can uniquely be extended to a Kleene algebra by setting $0^* = 1^* = 1$.
- S_3^1 from Ex. 1.5.2 can uniquely be extended to a Kleene algebra by setting $0^* = 1^* = 1$ and $a^* = a$.
- S_3^2 from Ex. 1.5.3 can uniquely be extended to a Kleene algebra by setting $a^* = 0^* = 1^* = 1$.
- S_3^3 from Ex. 1.5.4 can uniquely be extended to a Kleene algebra by setting $a^* = 0^* = 1^* = 1$.
- S_4^1 from Ex. 1.5.5 can uniquely be extended to a Kleene algebra by setting $0^* = a^* = 1^* = 1$ and $b^* = b$.

□

Conway [13] has shown that there are eighteen non-isomorphic four-element Kleene algebras.

Example 3.3.2 Since the relational I-semiring $\mathsf{REL}(M)$ from Ex. 1.5.6 is even a left-distributive left quantale, Th. 3.2.2 shows that it can be extended by a star operator in the usual way: for all $R \in \mathsf{REL}(M)$, the relation R^* is the reflexive transitive closure of R, that is, $R^* = \bigcup_{i \geq 0} R^i$, with $R^0 = I$ and $R^{i+1} = R \circ R^i$. We call $\mathsf{REL}(M)$ the *relational Kleene algebra* over M. For further discussion see e.g. [42]. □

Example 3.3.3 In the same way the full quantale $\mathsf{PAT}(\Sigma)$ from Ex. 1.5.14 can be extended into a full Kleene algebra of path sets. □

Example 3.3.4 Using again Th. 3.2.2 we see that the left-distributive left quantales $\mathsf{WOR}(\Sigma)$ and $\mathsf{STR}(\Sigma)$ over an alphabet Σ can uniquely be extended into left-distributive Kleene algebras.

In $\mathsf{WOR}(\Sigma)$, as in the classical theory of formal languages,

$$L^* = \{w_1.w_2.w_3.\cdots w_n \,|\, w_i \in L, n \in \mathbb{N}\} \ ,$$

where "factors" $w_i = \varepsilon$ vanish and an infinite w_i absorbs all subsequent w_j. For $n = 0$ we set $w_1.w_2.w_3.\cdots w_n =_{df} \varepsilon$.

The star operator in $\mathsf{STR}(\Sigma)$ works analogously with $\bowtie$ instead of the . operator. □

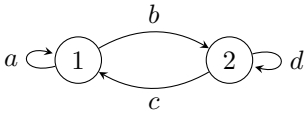
Example 3.3.5 Consider again the matrix I-semiring $\mathsf{MAT}(M, S)$ over an I-semiring S from Ex. 1.5.7. If S is a full Kleene algebra then $\mathsf{MAT}(M, S)$ can be extended to a full Kleene algebra (see [13]) by partitioning a non-singleton

matrix into non-empty submatrices a, b, c, d, of which a and d are square, and setting

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} f^* & a^* \cdot b \cdot g^* \\ d^* \cdot c \cdot f^* & g^* \end{pmatrix},$$

where $f = a + b \cdot d^* \cdot c$ and $g = d + c \cdot a^* \cdot b$.

Intuitively, the construction describes the finite execution paths in a two-state automaton with transitions labelled according to the matrix entries a, b, c and d:



The entry at row i and column j of the matrix contains a regular expression for the paths from node i to node j. □

Example 3.3.6 Another Kleene algebra is formed by extending the language I-semiring $\mathsf{LAN}(\Sigma)$ from Ex. 1.5.9 with the Kleene star. The definition is, as usual, $L^* = \{w_1 w_2 \dots w_n \mid n \geq 0, w_i \in L\}$. We call $\mathsf{LAN}(\Sigma)$ the *language* Kleene algebra over Σ.

The operators $\cup$, . and * are called *regular operators*, and the sets that can be obtained from finite subsets of Σ^* by a finite number of regular operators are called *regular subsets* or *regular events* of Σ^*. The equational theory of the regular subsets is called *algebra of regular events* [41].

There is a natural homomorphism L from the term algebra over the signature of the Kleene algebra generated by a set Σ onto the algebra $\mathsf{REG}(\Sigma)$ of regular events over Σ^*, given by $L(a) = \{a\}$ for each $a \in \Sigma$, $L(a + b) = L(a) \cup L(b)$ and $L(a \cdot b) = L(a) \,.\, L(b)$. In [43] it is shown that $\mathsf{REG}(\Sigma)$ is the free full Kleene algebra generated by Σ. In this sense, the equational theory of full Kleene algebras is the algebra of regular events and we can freely use all *regular identities*, that is, all valid identities of the algebra of regular events, in our calculations. □

Example 3.3.7 In the tropical I-semiring $(\min, +)$ from Ex. 1.5.11 the multiplicative unit 0 is the largest element, so that by Lm. 3.2.3.5 $(\min, +)$ can uniquely be extended to a Kleene algebra by setting $n^* = 0$ for all $n \in \mathbb{N}_\infty$. □

Example 3.3.8 Unlike the tropical I-semiring, the I-semiring $(\max, +)$ from Ex. 1.5.12 cannot be extended to a Kleene algebra. For $a > 0$ the set $\{a^n \mid n \in \mathbb{N}\} = \{na \mid n \in \mathbb{N}\}$ is unbounded, whereas, according to Lm. 3.2.3.14, it should have a^* as an upper bound. □

3.4 Infinite Iteration: Omega Algebras

In connection with laziness, the second essential operator is the infinite iteration of an element. While finite iteration suffices for safety analysis of infinite computations [46], infinite iteration is useful for describing liveness aspects (see e.g. [51]). It has been studied intensively in the theory of ω-languages [61]. Algebraic accounts are provided by Cohen's ω-algebra [12] and von Wright's demonic refinement algebra [65, 66]. However, both assume left distributivity, Cohen even right strictness of composition.

Definition 3.4.1 A *left-inductive left omega algebra* is a structure $(S, {}^\omega)$ consisting of a left-inductive left Kleene algebra S and a unary *omega* operator ${}^\omega : S \to S$ that satisfies, for $a, b, c \in S$, the *omega unfold* and *omega co-induction* laws

$$a^\omega \;=\; a \cdot a^\omega \;, \tag{3.13}$$

$$c \leq b + a \cdot c \;\Rightarrow\; c \leq a^\omega + a^* \cdot b \;. \tag{3.14}$$

If the underlying left-inductive left Kleene algebra is left-distributive or even a full Kleene algebra then the left omega algebra is called *left-distributive* or *full* as well.

The omega co-induction law is left-inductive, but since an omega algebra with a right-inductive omega co-induction law does not make sense, there is no need to introduce this distinction in the terminology.

These axioms are close in spirit to the characterisation of a greatest post-fixed point in the premiss of (3.3). One may wonder why we did not formulate omega unfold as $a^\omega \leq a \cdot a^\omega$. The reason is that in absence of right strictness the reverse inequation does not hold: by the omega co-induction law, the greatest (post-)fixed point of $\lambda x \,.\, a \cdot x$ is $a^\omega + a^* \cdot 0$ and $a^* \cdot 0$ need not vanish in a non-strict setting. Indeed, Mace4 finds the following 3-element counterexample:

$+$	0	1	a
0	0	1	a
1	1	1	a
a	a	a	a

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	a	a	a

	0	1	a
$*$	1	1	a
ω	0	a	0

This shows at the same time that isotony of omega would not hold with only the inequational form of omega unfold.

We can show the following properties.

Lemma 3.4.2

1. *$a^\omega + a^* \cdot b$ is the greatest (post-)fixed point of the function $f(x) = b + a \cdot x$ mentioned in Lm. 3.2.3.1.*
2. *$a^\omega = \nu x \,.\, a \cdot x$. In particular, we have the special omega co-induction law*
$$x \leq a \cdot x \;\Rightarrow\; x \leq a^\omega \;.$$
3. *The omega operator is unique if it exists.*

Proof.

1. By definition of f, isotony, (3.13), neutrality of 1, right distributivity, and finally omega unfold (3.13) and Lm. 3.2.3.2,
$$\begin{aligned} f(a^\omega + a^* \cdot b) &= b + a \cdot (a^\omega + a^* \cdot b) \geq b + a \cdot a^\omega + a \cdot a^* \cdot b \\ &= a \cdot a^\omega + b + a \cdot a^* \cdot b = a \cdot a^\omega + (1 + a \cdot a^*) \cdot b \\ &= a^\omega + a^* \cdot b \ , \end{aligned}$$
so that $a^\omega + a^* \cdot b$ is a post-fixed point of f. Now omega co-induction (3.14) and Th. 3.1.2.2 show the claim.
2. By left star induction (3.10) and omega unfold (3.13) we can easily show $a^* \cdot 0 \leq a^\omega$, so that by Part 1 a^ω coincides with the greatest (post-)fixed point of $\lambda x \,.\, a \cdot x + 0 = \lambda x \,.\, a \cdot x$. Therefore the specialised co-induction results by setting $b = 0$ in Axiom (3.14) and using again $a^* \cdot 0 \leq a^\omega$.
3. This is immediate from Part 2 and uniqueness of greatest elements in posets. □

The inequation $a^* \cdot 0 \leq a^\omega$ used in that proof seems natural, since by an easy induction on i and using (3.13) one can show $a^i \cdot 0 \leq a^\omega$ for all $i \in \mathbb{N}$ anyway.

For ease of comparison we note that von Wright's a^ω [65, 66] corresponds to $a^* + a^\omega$ in our setting (see [34] for a formal proof).

As in the case of star we show a sufficient criterion for existence of the omega operator.

Theorem 3.4.3 ([52]) *Let S be a left-distributive left quantale that is a completely distributive lattice. Then S can uniquely be extended to a left omega algebra by setting $a^\omega =_{df} \nu h$ with $h(x) =_{df} a \cdot x$. Moreover, with $f(x) =_{df} b + a \cdot x$ we have $\nu f = a^\omega + a^* \cdot b$.*

Proof. By its definition the omega operator satisfies omega unfold. So we only need to show that omega co-induction is valid as well. For this it suffices, by greatest fixed point induction (3.4), to show the last claim.

By Th. 3.2.2.1 we know that the star operator exists in S.

First, as in the proof of Lm. 3.4.2.1, we can show that $a^\omega + a^* \cdot b$ is a post-fixed point of f which implies $a^\omega + a^* \cdot b \leq \nu f$.

For the converse inequation we use ν-superfusion (3.8). Since we assume S to be completely distributive, the function $g(x) =_{df} x + a^* \cdot b$ is co-continuous. Moreover, trivially $g(\top) = \top \geq \nu h$. Finally,

$$\begin{aligned} & g(h(x)) \\ &= a \cdot x + a^* \cdot b && \{\![\text{ definition of } g, h \ ]\!\} \\ &= a \cdot x + (1 + a \cdot a^*) \cdot b && \{\![\text{ Lm. 3.2.3.2} \ ]\!\} \\ &= a \cdot x + b + a \cdot a^* \cdot b && \{\![\text{ right distributivity and neutrality of 1} \ ]\!\} \\ &= a \cdot (x + a^* \cdot b) + b && \{\![\text{ left distributivity} \ ]\!\} \\ &= f(g(x)) \ , && \{\![\text{ definition of } f, g \ ]\!\} \end{aligned}$$

and we are done. □

Example 3.4.4 By Th. 3.4.3 and the fact that every complete Boolean algebra forms a completely distributive lattice (see Ex. 2.7.4), the full relational Kleene algebra $\mathsf{REL}(M)$ of relations from Ex. 3.3.2 can uniquely be extended to a full omega algebra that is even Boolean. It turns out that there the complement of a^ω is also known as the *initial part* [60] of a, which coincides with the relation $N \times M$ where N is the set of points s_0 such that there is no infinite chain $s_0, s_1, s_2, \ldots$, with $(s_i, s_{i+1}) \in a$, for all $i \geq 0$. □

Definition 3.4.5 An element a is said to be *progressively finite* [60] iff $a^\omega = 0$.

In the relational I-semiring this is equivalent to saying that the initial part of a (see Ex. 3.4.4) is the universal relation.

Corollary 3.4.6 *Let a and b be elements of a left omega algebra.*

1. *If b is progressively finite and $a \leq b$ then also a is progressively finite.*
2. *Let $f(x) =_{df} a \cdot x + b$. If a is progressively finite then f has a unique fixed point, viz. $a^* \cdot b$ [4].*

Proof.

1. This is immediate from isotony of the omega operator.
2. This is immediate, since by Lm. 3.2.3.1 and Lm. 3.4.2.1 we have $\mu(f) = a^* \cdot b$ and $\nu(f) = \mu(f) + a^\omega$. □

Further details will be provided in Sect. 3.5 .

To state some additional consequences of the axioms we need the following notion.

Definition 3.4.7 An element a of an IL-semiring is *dense* if $a \leq a \cdot a$.

In relational I-semirings density of some a means that there is always an "intermediate point" between two a-related points, i.e., $x\,a\,y \Rightarrow \exists z : x\,a\,z \wedge z\,a\,y$. Every reflexive relation a is dense, because then one can choose z as either of x or y. Less trivial examples of dense relations in $\mathsf{REL}(\mathbb{Q})$ and $\mathsf{REL}(\mathbb{R})$ are provided by the standard strict orders $<$ on $\mathbb{Q}$ and $\mathbb{R}$.

Lemma 3.4.8 *Consider a left omega algebra S and an element $a \in S$.*

1. *S has a greatest element $\top =_{df} 1^\omega$.*
2. *Omega is isotone with respect to the natural ordering.*
3. *If $1 \leq a$ then $a^\omega = \top$.*
4. *If a is dense and right-strict, i.e., if $a \cdot a = a$ and $a \cdot 0 = 0$, then $a^\omega = a \cdot \top$. In particular, if p is a test then $p^\omega = p \cdot \top$.*

Proof.

1. This follows from neutrality of 1 and Lm. 3.4.2.2, since the premise of the specialised co-induction rule reduces to TRUE for $a = 1$.
2. This is immediate from isotony of the fixed point operators.
3. Immediate from Parts 1 and 2.

4. By (3.13), greatestness of $\top$ (Part 1) and isotony, $a^\omega = a \cdot a^\omega \leq a \cdot \top$. For the converse inequality we infer $a \cdot \top \leq a \cdot a \cdot \top$ from density of a and then use the specialised omega co-induction of Lm. 3.4.2.2.
   The second claim follows, since tests by Th. 2.1.8.7 are multiplicatively idempotent and hence dense. □

Example 3.4.9 Again by Th. 3.4.3 the left-distributive Boolean Kleene algebras $\mathsf{WOR}(\Sigma)$ and $\mathsf{STR}(\Sigma)$ over an alphabet Σ can uniquely be extended into left-distributive omega algebras.

In $\mathsf{WOR}(\Sigma)$ we have, as in the classical theory of formal languages and using Lm. 3.4.8.3,

$$L^\omega = \begin{cases} \mathsf{WOR}(\Sigma) & \text{if } \varepsilon \in L \ , \\ \{w_0.w_1.w_2.\cdots \mid w_i \in L\} & \text{otherwise} \ , \end{cases}$$

where in the latter case an infinite w_i absorbs all subsequent w_j.

The omega operator in $\mathsf{STR}(\Sigma)$ works analogously with $\bowtie$ instead of the . operator. □

We list a number of further useful laws.

Lemma 3.4.10 *Consider a left omega algebra S and elements $a, b \in S$ and $p \in \mathsf{test}(S)$.*

1. $a^\omega = a^* \cdot a^\omega = a^+ \cdot a^\omega$.
2. $(a^+)^\omega = a^\omega$.
3. $a^\omega \cdot b \leq a^\omega$.
4. $1 \leq b \Rightarrow a^\omega \cdot b = a^\omega$. *In particular,* $a^\omega \cdot \top = a^\omega$, *i.e.,* a^ω *is what is called a right ideal.*
5. $(a^\omega)^\omega \leq a^\omega$.
6. $a \cdot b \leq c \cdot a \Rightarrow a \cdot b^\omega \leq c^\omega$.
7. $(p^\omega)^\omega = p^\omega$.
8. $(a \cdot b)^\omega = a \cdot (b \cdot a)^\omega$.
9. $(p \cdot a)^\omega = (p \cdot a \cdot p)^\omega$.
10. $(a + b)^\omega = a^\omega + a^* \cdot b \cdot (a + b)^\omega$.
11. $(a + b)^\omega = (a^* \cdot b)^\omega + (a^* \cdot b)^* \cdot a^\omega$.

The last two properties can be informally explained as follows. Infinite iteration with a choice between a and b consists of infinite iteration of just a or some number (possibly 0) of as followed by b and then again an iteration with a choice between a and b. Another way of viewing such an iteration is that there may be infinitely many bs, interspersed with as, or only finitely many bs and then an infinite iteration just of as.

Proof.

1. For the first equation we argue as follows.
   ($\leq$) By neutrality of 1, $1 \leq a^*$ by left star unfold (3.9) and isotony we have
   $$a^\omega = 1 \cdot a^\omega \leq a^* \cdot a^\omega \ .$$

($\geq$) This reduces by left star induction (3.10) to $a^\omega + a \cdot a^\omega \leq a^\omega$, which holds by lattice algebra and omega unfold (3.13).
The second equation follows by the definition of plus, the first equation and omega unfold:

$$a^+ \cdot a^\omega = a \cdot a^* \cdot a^\omega = a \cdot a^\omega = a^\omega \ .$$

2. ($\geq$) follows from Lm. 3.2.5.2 and isotony of $^\omega$. For ($\leq$) it suffices by Lm. 3.4.2.2 to show that $(a^+)^\omega \leq a \cdot (a^+)^\omega$. Indeed, by omega unfold (3.13), definition of a^+, Lm. 3.2.5.2 with isotony of star and Part 1,
$$(a^+)^\omega = a^+ \cdot (a^+)^\omega = a \cdot a^* \cdot (a^+)^\omega \leq a \cdot (a^+)^* \cdot (a^+)^\omega = a \cdot (a^+)^\omega \ .$$
3. By omega unfold (3.13) $a^\omega \cdot b = a \cdot a^\omega \cdot b$, and the claim follows from Lm. 3.4.2.2.
4. By neutrality of 1 and isotony $a^\omega = a^\omega \cdot 1 \leq a^\omega \cdot b$. The reverse inequation was shown in Part 3. The second claim results by setting $b = \top$.
5. By omega unfold (3.13) and Part 3 we have $(a^\omega)^\omega = a^\omega \cdot (a^\omega)^\omega \leq a^\omega$.
6. By Lm. 3.4.2.2 it suffices to show that $a \cdot b^\omega$ is a post-fixed point of $h(x) =_{df} c \cdot x$. By omega unfold (3.13), the assumption and isotony,
$$a \cdot b^\omega = a \cdot b \cdot b^\omega \leq c \cdot a \cdot b^\omega \ .$$
7. By neutrality of 1, isotony of $^\omega$, Lm. 3.4.8.4 and Part 5, $p^\omega \leq (p \cdot \top)^\omega = (p^\omega)^\omega \leq p^\omega$, which entails the claimed equation.
8. By omega unfold (3.13) we have $a \cdot (b \cdot a)^\omega = a \cdot b \cdot a \cdot (b \cdot a)^\omega$ and hence $a \cdot (b \cdot a)^\omega \leq (a \cdot b)^\omega$ by Lm. 3.4.2.2.
Since a, b are arbitrary, also $b \cdot (a \cdot b)^\omega \leq (b \cdot a)^\omega$, and hence, using again omega unfold and isotony,
$$(a \cdot b)^\omega = a \cdot b \cdot (a \cdot b)^\omega \leq a \cdot (b \cdot a)^\omega \ .$$
9. By multiplicative idempotence of tests, Part 8, multiplicative idempotence of tests, Part 8 and multiplicative idempotence of tests,
$(p{\cdot}a)^\omega = (p{\cdot}p{\cdot}a)^\omega = p{\cdot}(p{\cdot}a{\cdot}p)^\omega = p{\cdot}(p{\cdot}a{\cdot}p{\cdot}p)^\omega = (p{\cdot}p{\cdot}a{\cdot}p)^\omega = (p{\cdot}a{\cdot}p)^\omega$.
10. ($\geq$) We show that both summands of the right hand side are less than or equal to the left hand side. For a^ω this follows by isotony of $^\omega$. Moreover, using isotony of *, $b \leq a + b$, omega unfold (3.13) and Part 1, we obtain again
$$a^* \cdot b \cdot (a + b)^\omega \leq (a + b)^* \cdot (a + b) \cdot (a + b)^\omega = (a + b)^\omega \ .$$
($\leq$) Set $h(x) =_{df} a{\cdot}x{+}b{\cdot}(a{+}b)^\omega$. By Lm. 3.4.2.1 then $a^\omega{+}a^*{\cdot}b{\cdot}(a{+}b)^\omega = \nu h$ and it suffices to show that $(a + b)^\omega$ is a fixed point of h. Indeed, by definition of h, right distributivity and omega unfold,
$$\begin{aligned} h((a + b)^\omega) &= a \cdot (a + b)^\omega + b \cdot (a + b)^\omega \\ &= (a + b) \cdot (a + b)^\omega = (a + b)^\omega \ . \end{aligned}$$
11. ($\geq$) Again we show that both summands of the right hand side are less than or equal to the left hand side. First, by Part 2, Def. 3.2.4, Lm. 3.2.3.11, isotony of star and isotony of $^\omega$,
$(a{+}b)^\omega = ((a{+}b)^+)^\omega = ((a{+}b){\cdot}(a{+}b)^*)^\omega \geq ((a{+}b)^*{\cdot}(a{+}b))^\omega \geq (a^*{\cdot}b)^\omega$.
Moreover, by isotony of star and $^\omega$, Lm. 3.2.3.8 and Part 1,

$$(a^* \cdot b)^* \cdot a^\omega \leq ((a+b)^*)^* \cdot (a+b)^\omega = (a+b)^* \cdot (a+b)^\omega \;=\; (a+b)^\omega \;.$$

($\leq$) By omega co-induction (3.14) it suffices to show that

$$(a+b)^\omega \leq (a^* \cdot b) \cdot (a+b)^\omega + a^\omega \;,$$

which is implied by Part 10. □

3.5 Iteration, Tests and Modal Operators

Definition 3.5.1 A left Kleene/omega algebra over a (pre)domain IL-semiring $(S, ^\ulcorner)$ is called a *left (pre)domain Kleene/omega algebra*, and a Kleene/omega algebra over a (pre)domain I-semiring $(S, ^\ulcorner)$ is called a *(pre)domain Kleene/omega algebra*.

In such an algebra we have for all $p \in \mathsf{test}(S)$ that $p^* = 1.$ by Lm. 3.2.3.5 and $p^\omega = p \cdot \top$ by Lm. 3.4.8.4.

It turns out that no extra axioms for the interaction between star and the modal operators are needed, since the following properties can be shown.

Lemma 3.5.2 *Assume a left predomain Kleene algebra $(S, ^\ulcorner)$.*

1. *We have the induction laws*

$$q \leq p \cdot |a]q \;\Rightarrow\; q \leq |a^*]p \;, \qquad p + |a\rangle q \leq q \;\Rightarrow\; |a^*\rangle p \leq q \;, \tag{3.15}$$

$$q \leq |a]p \cdot |a]q \;\Rightarrow\; q \leq |a^+]p \;, \quad |a\rangle p + |a\rangle q \leq q \;\Rightarrow\; |a^+\rangle p \leq q \;. \tag{3.16}$$

2. *If S is even a left domain Kleene algebra we have the unfold laws*

$$|a^*]p \leq p \cdot |a]|a^*]p \;, \qquad p + |a\rangle|a^*\rangle p \leq |a^*\rangle p \;, \tag{3.17}$$

$$|a^+]p \leq |a]p \cdot |a]|a^+]p \;, \qquad |a\rangle p + |a\rangle|a^+\rangle q \leq |a^+\rangle p \;. \tag{3.18}$$

Consequently, the tests $|a^*\rangle p$ and $|a^+\rangle p$ are the least (pre-)fixed points of the functions $\lambda x \,.\, p + |a\rangle x$ and $\lambda x \,.\, |a\rangle p + |a\rangle x$, resp. Analogously, the tests $|a^*]p$ and $|a^+]p$ are the greatest (post-)fixed points of the functions $\lambda x \,.\, p \cdot |a]x$ and $\lambda x \,.\, |a]p \cdot |a]x$, resp. Hence the above inequations strengthen to equations.

Proof.

1. As a sample we show the proof of forward box induction in (3.15). Assume $q \leq p \cdot |a]q$, i.e., $q \leq p \wedge q \leq |a]q$. By isotony of $|a]$ the claim follows from $q \leq p \wedge q \leq |a^*]q$. The first conjunct is an assumption. For the second one we calculate $q \leq |a]q \;\Leftrightarrow\; a \cdot \neg q \leq \neg q \cdot a \;\Rightarrow\; a^* \cdot \neg q \leq \neg q \cdot a^* \;\Leftrightarrow\; q \leq |a^*]q$. The first step uses (2.31). The second one follows from Lm. 3.2.3.10. The last step reverses the first one, but for a^* instead of a.
2. As a sample we show the proof of forward box unfold in (3.17):

$$|a^*]p = |1 + a \cdot a^*]p = |1]p \cdot |a \cdot a^*]p = p \cdot |a]|a^*]p \;.$$

The first step uses Lm. 3.2.3.2, the second one (2.19) and the third one (2.24) and (2.28).

The claims about least (pre-)fixed points and greatest (post-)fixed points follow from Th. 3.1.2.1 and Th. 3.1.2.2. □

Using Hoare triples (Def. 2.2.4 and Pr. (2.31), the box part of (3.15) reads $(q \leq p \wedge \{q\}\, a\, \{q\}) \Rightarrow \{q\}\, a^*\, \{p\}$, which is related to the familiar Hoare rule for the while loop. For the case $p = q$ (3.15) and (3.16) yield the laws

$$q \leq |a]q \Rightarrow q \leq |a^*]q\ , \qquad |a\rangle q \leq q \Rightarrow |a^*\rangle q \leq q\ , \tag{3.19}$$

$$q \leq |a]q \Rightarrow q \leq |a^+]q\ , \qquad |a\rangle q \leq q \Rightarrow |a^+\rangle q \leq q\ . \tag{3.20}$$

The third of these reads in terms of Hoare triples $\{q\}\, a\, \{q\} \Rightarrow \{q\}\, a^+\, \{q\}$, i.e., an invariant of a is also one of a^+.

We conclude our treatment of the cooperation between modal operators and finite iteration by exhibiting a relationship with PDL (see e.g. [32]).

Lemma 3.5.3 ([27]) *In a left-distributive domain IL-semiring we have the* PDL *induction rules*

$$|a^*](p \to |a]p) \leq p \to |a^*]p\ , \qquad |a^*\rangle p - p \leq |a^*\rangle(|a\rangle p - p)\ . \tag{3.21}$$

Conversely, already in a left-distributive predomain IL-semiring these rules imply the induction laws (3.15)*.*

Proof. We only deal with the diamond case; the box case follows from that by De Morgan dualisation.

$$\begin{array}{ll} & |a^*\rangle p - p \leq |a^*\rangle(|a\rangle p - p) \\ \Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\ & |a^*\rangle p \leq p + |a^*\rangle(|a\rangle p - p) \\ \Leftarrow & \quad \{\![\text{ abbreviation } q =_{df} |a\rangle p - p \text{ and (3.15) }]\!\} \\ & p + |a\rangle(p + |a^*\rangle q) \leq p + |a^*\rangle q \\ \Leftrightarrow & \quad \{\![\ p \leq p \text{ and order theory }]\!\} \\ & |a\rangle(p + |a^*\rangle q) \leq p + |a^*\rangle q \\ \Leftrightarrow & \quad \{\![\text{ left distributivity and (2.32) }]\!\} \\ & |a\rangle p + |a\rangle|a^*\rangle q \leq p + |a^*\rangle q \\ \Leftrightarrow & \quad \{\![\text{ since } |a\rangle|a^*\rangle q = |a \cdot a^*\rangle q \leq |a^*\rangle q \text{ by multiplicativity (2.28) and} \\ & \qquad \text{star unfold (3.9) with isotony of diamond, and order theory }]\!\} \\ & |a\rangle p \leq p + |a^*\rangle q \\ \Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\ & |a\rangle p - p \leq |a^*\rangle q \\ \Leftrightarrow & \quad \{\![\text{ above abbreviation }]\!\} \\ & q \leq |a^*\rangle q \\ \Leftrightarrow & \quad \{\![\text{ by star unfold (3.9) with isotony of diamond }]\!\} \\ & \mathsf{TRUE}\ . \end{array}$$

For the reverse implication we assume $p + |a\rangle q \leq q$, which by the characterisation of supremum and shunting is equivalent to

$$p \leq q \wedge |a\rangle q - q \leq 0\ . \tag{$*$}$$

Now by the first conjunct of $(*)$ with isotony, (3.21) with shunting, the second conjunct of $(*)$, strictness of diamond and neutrality of 0 we obtain

$$|a^*\rangle p \leq |a^*\rangle q \leq q + |a^*\rangle(|a\rangle q - q) = q + |a^*\rangle 0 = q \ .$$

□

Now we turn to infinite iteration. To exemplify the interplay of tests with infinite iteration we show that an invariant of a will hold throughout the infinite iteration of a if it holds initially:

Lemma 3.5.4 $p \cdot a = p \cdot a \cdot p \Rightarrow p \cdot a^\omega = (p \cdot a)^\omega$.

Proof. $(\geq)$ We do not even need the assumption: by omega unfold (3.13), idempotence of $\cdot$ on tests, omega unfold again and isotony,

$$(p \cdot a)^\omega = p \cdot a \cdot (p \cdot a)^\omega = p \cdot p \cdot a \cdot (p \cdot a)^\omega = p \cdot (p \cdot a)^\omega \leq p \cdot a^\omega \ .$$

$(\leq)$ By omega unfold and the assumption,

$$p \cdot a^\omega = p \cdot a \cdot a^\omega = p \cdot a \cdot p \cdot a^\omega \ ,$$

which means that $p \cdot a^\omega$ is a fixed point of $\lambda x \,.\, p \cdot a \cdot x$ and hence below the greatest fixed point $(p \cdot a)^\omega$ (see Lm. 3.4.2.2) of that function. □

Lemma 3.5.5 *In a modal omega algebra, $\neg\lceil(a^\omega) \cdot a$ is progressively finite.*

Proof. Set $b =_{df} \neg\lceil(a^\omega) \cdot a$. Since $b \leq a$ we get $b^\omega \leq a^\omega$ and hence $\lceil(b^\omega) \leq \lceil(a^\omega)$. On the other hand, by omega unfold (3.13), the definition of b and (d2),

$$\lceil(b^\omega) = \lceil(b \cdot b^\omega) = \lceil(\neg\lceil(a^\omega) \cdot a \cdot b^\omega) \leq \neg\lceil(a^\omega) \ .$$

So $\lceil(b^\omega) \leq \lceil(a^\omega) \cdot \neg\lceil(a^\omega) = 0$ and hence $b^\omega = 0$ by Th. 2.4.6.2. □

3.6 Extremal Elements, Noetherity, Divergence and Convergence

Whereas the omega operator describes *actual* infinite computations, sometimes it is interesting to express that a particular transition element has the *potential* of infinite iteration. For instance, in the language IL-semiring, every language could be iterated indefinitely, but the carrier set does not actually contain languages with infinite strings. For describing this, we can again use modal operators.

In this section we abstract the notions of well-foundedness and Noetherity from the relational IL-semiring $\mathsf{REL}(M)$ to modal IL-semirings. In set theory, a relation R on a set M is well founded within a subset $N \subseteq M$ iff every non-empty subset of N has an R-minimal element. It is a standard exercise to show that this is equivalent to the absence of infinitely descending R-chains in N. An element of N is R-minimal in N iff it has no R-predecessor in N, or, equivalently, if it is not in the image $\langle R|N$ of N under R. Abstracting R to a semiring element a and N to a test p leads to the following definition.

Definition 3.6.1 For a predomain IL-semiring $(S, \ulcorner)$ and $a \in S, p \in \mathsf{test}(S)$, the function yielding the *a-maximal part* of p is $\mathsf{max}_a p = p - |a\rangle p$. In point-free style, $\mathsf{max}_a = 1 - |a\rangle$. Dually, for a precodomain IL-semiring $(S, \urcorner)$ and $a \in S, p \in \mathsf{test}(S)$, the *a-minimal part* of p is yielded by $\mathsf{min}_a = 1 - \langle a|$.

On the one hand, therefore, a is well founded iff $\mathsf{min}_a\, p$ is non-empty whenever p is. On the other hand, an infinitely descending a-chain corresponds to a $p \neq 0$ for which $\mathsf{min}_a\, p = 0$. Absence of infinitely descending a-chains therefore means that 0 is the only p that satisfies $\mathsf{min}_a\, p \leq 0$. Dual remarks apply to ascending chains.

Definition 3.6.2 An element a of a predomain IL-semiring $(S, \ulcorner)$ is *Noetherian* if, for all $p \in \mathsf{test}(S)$,

$$\mathsf{max}_a\, p \leq 0 \Rightarrow p \leq 0.$$

Dually, an element a of a precodomain IL-semiring $(S, \urcorner)$ is *well founded* if, for all $p \in \mathsf{test}(S)$,

$$\mathsf{min}_a\, p \leq 0 \Rightarrow p \leq 0.$$

Similar definitions for related structures have been given in [1, 26, 31, 60]. Since well-foundedness and Noetherity are dual with respect to opposition, and since we are mainly interested in termination, that is, absence of strictly ascending sequences of actions, we will restrict our attention to Noetherity.

The following result is immediate from the definitions in Sect. 3.1.

Corollary 3.6.3 *Assume a predomain IL-semiring $(S, \ulcorner)$ and let $a \in S, p \in \mathsf{test}(S)$.*

1. *$\mathsf{max}_a\, p \leq 0$ iff p is a post-fixed point of the endofunction $|a\rangle$ on $\mathsf{test}(S)$.*
2. *a is Noetherian iff 0 is the unique post-fixed point of $|a\rangle$, that is, iff for all $p \in \mathsf{test}(S)$,*

$$p \leq |a\rangle p \Rightarrow p \leq 0.$$

Next we show a connection between Noetherity and the existence of maximal elements which will be used in a later section.

Lemma 3.6.4 *Assume a left-distributive domain Kleene algebra $(S, \ulcorner)$. Let $a \in S$ be Noetherian and let a^* be the associated preorder. Then for any $p \in \mathsf{test}(S)$*

$$p \leq |a^*\rangle \mathsf{max}_a\, p\ .$$

Informally, this means that any point in the set abstractly represented by p is dominated w.r.t. a^* by some point in $\mathsf{max}_a\, p$.

Proof.

$$\begin{array}{ll} & p \leq |a^*\rangle \mathsf{max}_a\, p \\ \Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\ & p - |a^*\rangle \mathsf{max}_a\, p \leq 0 \\ \Leftarrow & \quad \{\![\text{ Noetherity of } a \text{ and Cor. 3.6.3.2 }]\!\} \end{array}$$

$$
\begin{array}{ll}
& p - |a^*\rangle \mathsf{max}_a\, p \leq |a\rangle(p - |a^*\rangle \mathsf{max}_a\, p) \\
\Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\
& p \leq |a^*\rangle \mathsf{max}_a\, p + |a\rangle(p - |a^*\rangle \mathsf{max}_a\, p) \\
\Leftrightarrow & \quad \{\![\text{ diamond star unfold (3.17) and distributivity }]\!\} \\
& p \leq \mathsf{max}_a\, p + |a\rangle|a^*\rangle \mathsf{max}_a\, p + |a\rangle(p - |a^*\rangle \mathsf{max}_a\, p) \\
\Leftrightarrow & \quad \{\![\text{ shunting and distributivity }]\!\} \\
& p - \mathsf{max}_a\, p \leq |a\rangle(|a^*\rangle \mathsf{max}_a\, p + (p - |a^*\rangle \mathsf{max}_a\, p)) \\
\Leftrightarrow & \quad \{\![\text{ Boolean algebra and definition of } \mathsf{max}]\!\} \\
& p \cdot |a\rangle p \leq |a\rangle(|a^*\rangle \mathsf{max}_a\, p + p) \\
\Leftarrow & \quad \{\![\text{ lattice algebra }]\!\} \\
& |a\rangle p \leq |a\rangle(|a^*\rangle \mathsf{max}_a\, p + p) \\
\Leftarrow & \quad \{\![\text{ isotony of diamond }]\!\} \\
& p \leq |a^*\rangle \mathsf{max}_a\, p + p \\
\Leftrightarrow & \quad \{\![\text{ lattice algebra }]\!\} \\
& \mathsf{TRUE}\ .
\end{array}
$$

□

Sometimes it is convenient to have an operator for calculating all starting states of a transition element from which infinite transition paths emanate. Again we restrict ourselves to the forward view, since infinite backward paths are not meaningful for transition systems.

If the test algebra of a modal Kleene algebra is complete, the Knaster/ Tarski theorem implies that for every element a the greatest fixed point $\nu|a\rangle$ exists, since $|a\rangle$ is isotone. The test $\nu|a\rangle$ characterises the greatest set of states from which infinite paths emanate. We call the test $\nu|a\rangle$ the *divergence* ∇a of a. It turns out that ∇a is more suitable for termination analysis than a^ω.

If the test algebra is not complete, the existence of ∇a is not guaranteed. Instead, one can axiomatise it, similarly to the omega operator, by the formulas [19]

$$\nabla a \leq |a\rangle\, \nabla a\ , \tag{3.22}$$

$$p \leq |a\rangle p + q \Rightarrow p \leq \nabla a + |a^*\rangle q\ , \tag{3.23}$$

which are theorems in the case of a complete test algebra.

Sometimes it is more convenient to reason in terms of the complement of $\nu|a\rangle$, i.e., about the set of states from which *no* infinite a-paths emanate. We call this test the *convergence* Δa of a. By Lm. 3.1.5 it is given by $\mu|a]$ in the case of a complete test algebra. Hence Δa corresponds to the *halting predicate* of the modal μ calculus [32]. In the general case one has to use an axiomatisation dual to the one for divergence:

Definition 3.6.5 A *convergence algebra* [19] is a pair (S, Δ) where S is a left predomain Kleene algebra and the *convergence* operator $\Delta : S \to \mathsf{test}(S)$ satisfies, for all $a \in S$ and $p, q \in \mathsf{test}(S)$, the unfold and induction laws

$$|a](\Delta a) \leq \Delta a, \qquad |a]p \cdot q \leq p \;\Rightarrow\; \Delta a \cdot |a^*]q \leq p\ .$$

This axiomatises $\Delta a \cdot |a^*]q$ as the least pre-fixed point and least fixed point of the function $\lambda p \,.\, |a]p \cdot q$; in particular, Δa is the least pre-fixed point and the least fixed point of $|a]$. For the pre-fixed points of $|a]$ we have $|a]p \leq p \Leftrightarrow \neg p \leq |a\rangle \neg p$ by definition of the modal operators.

In a convergence algebra we can *define* divergence as $\nabla a =_{df} \neg \Delta a$ and show by straightforward calculations that this satisfies (3.22) and (3.23), which entails $\nabla a = \nu |a\rangle$.

Since looping can only start from states within $\ulcorner a$ we have

Lemma 3.6.6 $\neg \ulcorner a \leq \Delta a$.

Proof. By (2.15), isotony of $|a]$ and the fixed point property of Δa,

$$\neg \ulcorner a = |a]0 \leq |a]\Delta a = \Delta a \ .$$

□

For a test p the convergence consists exactly of those states that do not satisfy p; for all other states, testing p can be repeated indefinitely and so they are not part of the convergence:

Lemma 3.6.7 *For $p \in \mathsf{test}(S)$ the axioms entail $\Delta p = \neg p$.*

Proof. By the fixed point property of Δp, (2.23) and the definition of $\rightarrow$,

$$\Delta p = |p]\Delta p = \neg p + \Delta p$$

which means $\neg p \leq \Delta p$. For the converse inequation we show that $\neg p$ is a fixed point of $|p]$. Again by (2.23) and the definition of $\rightarrow$,

$$|p]\neg p = \neg p + \neg p = \neg p \ .$$

□

By Lm. 3.1.5, if both ∇a and Δa exist then they are complements of each other, since they are greatest and least fixed point of the dual functions $|a\rangle$ and $|a]$, respectively. Thus, an element a with $\Delta a = 1$ and hence $\nabla a = 0$ is Noetherian. Contrarily, if $\Delta a \neq 1$ and hence $\nabla a \neq 0$ then a has the potential of infinite iteration.

Next we study analogues of the recursions for star and omega at the level of tests in a convergence algebra.

Theorem 3.6.8 *Assume a convergence algebra (S, Δ) with locality* (d3)*. For $a \in S$, $p \in \mathsf{test}(S)$ define $h, k : \mathsf{test}(S) \rightarrow \mathsf{test}(S)$ by*

$$h(x) =_{df} |a\rangle x + p \text{ and } k(x) =_{df} |a]x - p.$$

1. $h(x) = \neg k(\neg x)$.
2. $\mu h = |a^*\rangle p$.
3. $\nu h = |a^*\rangle p + \nabla a$.
4. $|a^*]\ulcorner a \leq \nabla a$.
5. $\mu k = |a^*]\neg p - \nabla a$.
6. $\nu k = |a^*]\neg p$.

Proof. Part 1 is clear.

Part 2 was established in Lm. 3.5.2. Symmetrically, Part 3 follows from (3.23).

Next, by Part 1, h and k are dual in the sense of Def. 1.2.11. Therefore Lm. 3.1.5 gives Parts 5 and 6.

For Part 4, we first show for all $q \in \mathsf{test}(S)$ that $\ulcorner a \cdot \lfloor a]q \leq \lfloor a\rangle q$; the proof uses shunting, distributivity and Boolean algebra:

$$\ulcorner a \cdot \lfloor a]q \leq \lfloor a\rangle q \;\Leftrightarrow\; \ulcorner a \leq \lfloor a\rangle q + \lfloor a\rangle \neg q \;\Leftrightarrow\; \ulcorner a \leq \lfloor a\rangle(q + \neg q) \;\Leftrightarrow\; \ulcorner a \leq \ulcorner a.$$

Now, we establish the claim by the co-induction law (3.23) showing that $\lfloor a^*]\ulcorner a$ is expanded by $\lfloor a\rangle$; this employs star unfold, antidisjunctivity, multiplicativity of box (2.28) and the above derivation:

$$\lfloor a^*]\ulcorner a \;=\; \lfloor 1 + a \cdot a^*]\ulcorner a \;=\; \ulcorner a \cdot \lfloor a]\lfloor a^*]\ulcorner a \;\leq\; \lfloor a\rangle\lfloor a^*]\ulcorner a.$$

□

References

1. J.-R. Abrial: The B-Book. Cambridge University Press, 1996
2. A. Arnold: Finite Transition Systems. Prentice Hall 1994
3. R. Backhouse: Galois connections and fixed point calculus. In R. Backhouse, R. Crole, J. Gibbons (eds.): Algebraic and Coalgebraic Methods in the Mathematics of Program Construction. LNCS 2297. Springer 2002, 89–148
4. R. C. Backhouse et al.: Fixed point calculus. Inform. Proc. Letters, 53:131–136 (1995)
5. R. Backhouse, J. van der Woude: Demonic operators and monotype factors. Mathematical Structures in Computer Science 3, 417–433 (1993)
6. D. Batory, P. Höfner, D. Köppl, B. Möller, A. Zelend: Structured Document Algebra in action. In: R. De Nicola, R. Hennicker (eds.): Software, services, and systems: essays dedicated to Martin Wirsing on the occasion of his retirement from the Chair of Programming and Software Engineering. LNCS 8950. Springer 2015, 291–311
7. J.A. Bergstra, I. Bethke, A. Ponse: Process algebra with iteration and nesting. The Computer Journal 37(4), 243–258 (1994)
8. J.A. Bergstra, W. Fokkink, A. Ponse: Process algebra with recursive operations. In [9], 333–389
9. J.A. Bergstra, S. Smolka, A. Ponse: Handbook of process algebra. North-Holland 2001
10. T Brunn, B. Möller, M. Russling: Layered graph traversals and Hamiltonian path problems — an algebraic approach. Technical Report 1997-08, Institute of Computer Science, University of Augsburg, December 1997
11. T Brunn, B. Möller, M. Russling: Layered graph traversals and Hamiltonian path problems — an algebraic approach. In J. Jeuring (ed.): Mathematics of Program Construction. LNCS 1422. Springer 1998, 96–121
12. E. Cohen: Separation and reduction. In R. Backhouse and J.N. Oliveira (eds.): Mathematics of Program Construction. LNCS 1837. Springer 2000, 45–59
13. J.H. Conway: Regular algebra and finite machines. London: Chapman and Hall 1971
14. P. Cousot, R. Cousot: Systematic design of program analysis frameworks. Proc. 6th POPL. ACM Press 1979, 269–282
15. H.-H. Dang, P. Höfner, B. Möller: Algebraic separation logic. Journal of Logic and Algebraic Programming 80, 221–247 (2011)
16. H.-H. Dang, B. Möller: Modal algebra and Petri nets. Acta Inf. 52(2-3): 109–132 (2015)
17. J. Desharnais, B. Möller, G. Struth: Modal Kleene algebra and applications — a survey. Journal on Relational Methods in Computer Science 1, 93–131 (2004)
18. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. ACM Transactions on Computational Logic 7, 798–833 (2006)
19. J. Desharnais, B. Möller, G. Struth: Termination in modal Kleene algebra. In J.-J. Lévy, E. Mayr, J. Mitchell (eds.): Exploring new frontiers of theoretical informatics. IFIP International Federation for Information Processing Series 155. Kluwer 2004, 653–666. Revised version in [20]
20. J. Desharnais, B. Möller, G. Struth: Algebraic Notions of Termination. Logical Methods in Computer Science 7, 1–29 (2010)
21. J. Desharnais, G. Struth: Modal Semirings Revisited. In P. Audebaud, C. Paulin-Mohring (eds.): Mathematics of Program Construction. LNCS 5133. Springer 2008, 360–387
22. J. Desharnais, G. Struth: Domain axioms for a family of near-semirings. In J. Meseguer, G. Roşu (eds.): AMAST 2008. LNCS 5140. Springer 2008, 330–345
23. J. Desharnais, G. Struth: Internal axioms for domain semirings. Science of Computer Programming 76(3), 181–203 (2011)
24. E.W. Dijkstra: A Discipline of Programming. Prentice Hall 1976
25. E. Dijkstra. Why preorders are beautiful. Manuscript 1991, `http://www.cs.utexas.edu/users/EWD/ewd11xx/EWD1102.PDF`

26. H. Doornbos, R. Backhouse, J. van der Woude: A calculational approach to mathematical induction. Theoretical Computer Science 179, 103–135 (1997)
27. T. Ehm, B. Möller, G. Struth: Kleene modules. In R. Berghammer, B. Möller, and G. Struth (eds.): Relational and Kleene-Algebraic Methods in Computer Science. LNCS 3051. Springer 2004, 112–123
28. S. Gaubert, M. Plus: Methods and applications of $(max, +)$ linear algebra. Tech. Rep. RR-3088, INRIA-Rocquencourt, Jan. 1997
29. R. Glück, B. Möller, M. Sintzoff: Model refinement using bisimulation quotients. In M. Johnson, D. Pavlovic (eds.): Algebraic Methodology and Software Technology (AMAST 2010). LNCS 6486. Springer 2010, 76–91
30. J. S. Golan, The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science, Addison-Wesley, 1992.
31. R. Goldblatt: An algebraic study of well-foundedness. Studia Logica 44, 422–437 (1985)
32. D. Harel, D. Kozen, J. Tiuryn: Dynamic Logic. MIT Press, 2000
33. U. Hebisch, H. Weinert: Semirings — Algebraic Theory and Applications in Computer Science. World Scientific 1998
34. P. Höfner, B. Möller, S. Solin: Omega algebra, demonic refinement algebra and commands. In: R. Schmidt, G. Struth (eds.): Relations and Kleene algebra in computer science. LNCS 4136. Springer 2006, 222–234
35. M. Hollenberg: An equational axiomatization of dynamic negation and relational composition. Journal of Logic, Language and Information 6, 381-401 (1997)
36. E. Huntington: New sets of independent postulates for the algebra of logic, with special reference to Whitehead and Russell's Principia Mathematica. Transactions of the American Mathematical Society¡ 35, 274–304 (1933)
37. E. Huntington: Boolean algebra. A Correction. Transactions of the American Mathematical Society 35, 557–558 (1933)
38. B. Jónsson, A. Tarski: Boolean algebras with operators, Part I. American Journal of Mathematics 73, 891–939 (1951)
39. D. Kaplan: Regular expressions and the equivalence of programs. Journal of Computer and System Sciences 3(4):361–386, 1969
40. S. Kleene: Introduction to metamathematics. Van Nostrand 1952
41. S. Kleene: Representation of events in nerve nets and finite automata. In C. Shannon, J. McCarthy (eds.): Automata Studies. Princeton University Press 1956, 3–41
42. D. Kozen: On Kleene algebras and closed semirings. In B. Rovan (ed.): Proc. MFCS'90. LNCS 452. Springer 1990, 26–47
43. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation 110, 366–390 (1994)
44. D. Kozen: Kleene algebras with tests. ACM Transactions on Programming Languages and Systems 19, 427–443 (1997)
45. D. Kozen: On Hoare logic, Kleene algebra, and types. In: P. Gärdenfors, J. Woleński, K. Kijania-Placek (eds.): In the Scope of Logic, Methodology, and Philosophy of Science: Volume One of the 11th Int. Congress Logic, Methodology and Philosophy of Science, Cracow, August 1999. Studies in Epistemology, Logic, Methodology, and Philosophy of Science, vol. 315. Kluwer 2002, 119–133
46. D. Kozen: Kleene Algebra with tests and the static analysis of programs. Cornell University, Department of Computer Science, Technical Report TR2003-1915, 2003
47. W. Kuich:. Semirings and formal power series: Their relevance to formal languages and automata. In G. Rozenberg, A. Salomaa (eds.): Handbook of Formal Language Theory, Vol. I. Springer 1997, 609–677
48. W. Kuich, A. Salomaa: emirings, automata, languages. EATCS Monographs on Theoretical Computer Science, vol. 5. Springer 1986
49. E. Manes, D. Benson: The inverse semigroup of a sum-ordered semiring. Semigroup Forum 31, 129–152 (1985)

50. A. Melton, D.A. Schmidt, G.E. Strecker: Galois connections and computer science applications. In D. Pitt, S. Abramsky, A. Poigné, D. Rydeheard, (eds.): Category Theory and Computer Programming. LNCS 240. Springer 1986, 299–312
51. B. Möller: Ideal stream algebra. In: B. Möller, J. Tucker (eds.): Prospects for hardware foundations. LNCS 1546. Springer 1998, 69–116
52. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. LNCS 3125. Springer 2004, 252–273. Revised version in [54]
53. B. Möller, B.: Complete tests do not guarantee domain. Tech. Rep. 2005-6, Universität Augsburg, Institut für Informatik 2005. `http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2005-6.pdf`.
54. B. Möller: Kleene getting lazy. Science of Computer Programming 65, 195–214 (2007)
55. B. Möller: Modal knowledge and game semirings. Computer Journal 56 (1), 53–69 (2013)
56. B. Möller, P. Roocks, M. Endres: An algebraic calculus of database preferences. In: J. Gibbons, P., Nogueira (eds.): Mathematics of Program Construction. LNCS 7342. Springer 2012, 241–262
57. D. Park. Concurrency and automata on infinite sequences. Proc. 5th GI-Conference on Theoretical Computer Science, LNCS 104. Springer 1981, 167–183
58. S. Popkorn: First steps in modal logic. Cambridge University Press 1994
59. S.I. Rosenthal: Quantales and their applications. Pitman Research Notes in Mathematics Series, Vol. 234. Longman Scientific&Technical 1990
60. G. Schmidt and T. Ströhlein. Relations and Graphs: Discrete Mathematics for Computer Scientists. EATCS Monographs on Theoretical Computer Science. Springer, 1993
61. L. Staiger: Omega languages. In G. Rozenberg, A. Salomaa (eds.): Handbook of formal languages, Vol. 3. Springer 1997, 339–387
62. A. Tarski: A lattice-theoretical fixpoint theorem and its applications. Pacific Journal of Mathematics, 5:285–309, 1955
63. R. van Glabbeek: The linear time — branching time spectrum I. The semantics of concrete, sequential processes. In [9], 3–99
64. B. von Karger. Temporal algebra. Mathematical Structures in Computer Science, 8(3):277–320, 1998.
65. J. von Wright: From Kleene algebra to refinement algebra. In E. Boiten, B. Möller (eds.): Mathematics of Program Construction. LNCS 2386. Springer 2002, 233–262. Revised version in [66]
66. J. von Wright: Towards a refinement algebra. Science of Computer Programming 51, 23–45 (2004)

Index

μ-sub-fusion and μ-fusion, 51
μ-super-fusion, 50
ν-sub-fusion, 51
ν-super-fusion and ν-fusion, 51
$\top$-determined, 33
((pre)pre)domain I-semiring, 29
(I)R-semiring, 12
(generalised) language, 15
(idempotent) right semiring, 12
(positively/universally) left-distributive, 11
(pre)codomain IL-semiring, 36
(pre)domain Kleene/omega algebra, 63
(universally) conjunctive, 5
(universally) disjunctive, 5

algebra of regular events, 57
antitone, 5
associative, 9

Boolean, 11, 12
Boolean (I-)semirings, 12
Boolean algebra, 5, 11
Boolean quantales, 12
Boolean semiring, 14
bounded, 11

cancellation properties, 40
chain, 2
co-continuous, 6
codomain operator, 36
commutative, 9
complement, 17
complete Boolean algebra, 5
complete lattice, 3
completely distributive, 4
composition, 10
computation streams, 16
continuous, 6
convergence, 67
convergence algebra, 67

De Morgan dual, 7
define, 68
dense, 60
distributive, 3
domain IL-semiring, 29
domain operator, 29

exchange law, 45
expanded, 50
extensional, 42

fixed point, 49
full, 58
full Kleene algebra, 55
fusion product, 14

Galois connection, 39
greatest (post-)fixed point, 49
greatest element, 2
greatest fixed point co-induction, 50
greatest lower bound, 3
groupoid, 9
guarded string, 15

halting predicate, 67
Hoare triple, 26

I-semiring, 11
idempotent, 10
IL-semiring, 10
infimum, 3
initial part, 60
integral, 34

invariant, 26
isotone, 5
isotone in argument i, 6

kernel, 7
Kleene algebra, 55

L-semiring, 9
language, 14, 57
lattice, 3
least (pre-)fixed point, 49
least element, 2
least fixed point induction, 49
least upper bound, 2
left, 9
left (or lazy) semiring, 9
left (pre)domain Kleene/omega algebra, 63
left codomain IL-semiring, 36
left quantale, 11
left star induction, 51
left star unfold, 51
left-distributive, 11, 58
left-distributive Kleene algebra, 55
left-inductive Kleene algebra, 51
left-inductive left Kleene algebra, 51
left-inductive left omega algebra, 58
left-strict, 10
linear, 2
locality, 29, 33
locality axiom, 36
lower semilattice, 3
lower, 39

matrix semiring, 13
max-plus semiring, 14
maximal part, 66
minimal part, 66
mirror operator, 12
modal I-semiring, 41
modal IL-semiring, 41
modal modus ponens, 44
modal modus tollens, 44
monoid, 9
monotonically decreasing, 5
monotonically increasing, 5
multiplication, 10

natural order, 10
Noetherian, 66

omega, 58
omega co-induction, 58
omega unfold, 58
opposite operator, 12

partial order, 2
path I-semiring, 15
positively/universally left-distributive, 11
post-fixed point, 49
powers, 9
pre-fixed point, 49
precodomain IL-semiring, 36
precodomain operator, 36
predomain IL-semiring, 29
predomain operator, 29
preprecodomain IL-semiring, 36
preprecodomain operator, 36
prepredomain IL-semiring, 29
prepredomain operator, 29
progressively finite, 60
purely finite, 15
purely infinite, 15

quantale, 12

regular events, 57
regular identities, 57
regular operators, 57
regular subsets, 57
relational, 13
relational Kleene algebra, 56
restriction, 22
right neutral, 9
right quantale, 12
right star induction, 55
right star unfold, 55
right unit, 9
right-distributive, 10
right-inductive, 55
Right-inductive right Kleene algebras, 55
right-strict, 11

semigroup, 9
semiring, 13
shunting rule, 5, 19
standard Kleene algebra, 12
states, 15
sub-conjunctive, 5
sub-identity, 17
super-disjunctive, 5
supremum, 2
swapping rules, 41

test, 17
test-discrete, 17
transitions, 15
transitive closure, 54
tropical semiring, 14
two-element Boolean semiring, 12

universally sub-conjunctive, 5
universally super-disjunctive, 5
upper adjoints, 39
upper semilattice, 3
valid, 42
weakest liberal precondition, 43
well founded, 66