Universität Augsburg

From Sequential Algebra to Kleene Algebra: Interval Modalities and Duration Calculus

Peter Höfner

Report 2005-5 Juli 2005

Institut für Informatik
D-86135 Augsburg

Contents

Chapter 1

Introduction

The duration calculus (DC) is a formal, algebraic system for specification and design of real-time systems, where real numbers are used to model time and (Boolean valued) functions to formulate requirements. Since its introduction in 1991 by Chaochen, Hoare and Ravn [CHR91] it has been applied to many case studies and has been extended into several directions. E.g., there is an extension for specifying liveness and safety requirements [Hun02]. In the original duration calculus the authors used knowledge about temporal logics and established a connection with security systems and intervals. In 1997 Hansen and Chaochen [HC97] showed that DC extends interval logic (IL) based on [Dut95a, Dut95b]. Many times the connection between DC and linear temporal logic have been investigated (see e.g. [LRL98]). In most of the papers with DC-related topics the examples of a leaking gas pipe and of the leaking gas burner are discussed. These examples are also given by Chaochen et al. [CHR91]. Von Karger investigated in [Kar00] the embedding of the DC in sequential algebras. For these purposes he established the proof principle of engineer's induction.

Independently of DC there is the algebraic structure of Kleene algebra (KA). It is an idempotent semiring with an additional unary operator called the Kleene star. This operation models finite iteration. Kleene algebras are well known structures. E.g., Kozen proved many of their fundamental properties ([Koz90, Koz94]). Möller and Desharnais have also shown various results, applications and algorithms of Kleene algebras. A nearly full survey is given in [DMS03, DMS04].

A first step for combining the two ideas (KA and DC) is given by Dima in 2000 [Dim00]. There he developed a Kleene algebra with the power set of real numbers $\mathcal{P}(\mathbb{R}^+)$[1] as carrier set. Furthermore he pointed out once more that the real numbers are one of the main constructs in time analysis.

This report presents the duration calculus on the basis of Kleene algebra. Doing this we will analyse the DC in a new view. For presenting the final connection between DC and KA we provide the fundamentals like the definitions of Kleene algebra and semirings together with some examples in Chapter 2. After this we establish in Chapter 3 the right and left residuals as well as the right and left detachments as special operators on semirings and Kleene algebras. Residuals and detachments are then used to define some modal operators, called interval modalities, in the following. For the presentation of the duration calculus we will need an important equation, the engineer's induction, which was introduced by von Karger in [Kar00]. The induction shows the relationship between the interval modalities and the least fixed points in an algebraic structure as a Kleene algebra. Finally, we present in Chapter 6 the duration calculus, considering as example the leaking gas pipe, and after that present the duration calculus in a more general way.

[1] In contrary of the Kleene algebra introduced by Kozen the Kleene algebra of Dima is not idempotent with respect to the addition.

Chapter 2

Fundamentals

This chapter provides the necessary basics for the theory of residuals, interval modalities and the duration calculus. It briefly defines the algebraic structure of Kleene algebra. Hence we start with partially ordered sets and semirings. For the second definition we assume that the definition of monoids is known. Furthermore we will present some examples for the introduced algebraic structures. A more detailed discussion of semirings and Kleene algebras can be found in [HW93] and [Koz94].

2.1 Semirings

Definition 2.1.1 (Partially Ordered Set)
A *partially ordered set* (or *poset* for short) $(M, \leq)$ is a set M equipped with a partial order $\leq$.

Definition 2.1.2 ((Idempotent) Semiring)
A *semiring* is a quintuple $(A, +, \cdot, 0, 1)$ satisfying the following properties for all $x \in A$:

(i) $(A, +, 0)$ is a commutative monoid.

(ii) $(A, \cdot, 1)$ is a monoid with *annihilator* 0,
i.e., $0 \cdot x = x \cdot 0 = 0$.

(iii) $(A, +, \cdot, 0, 1)$ satisfies the distributivity laws
$x \cdot (y + z) = x \cdot y + x \cdot z$, $\qquad (x + y) \cdot z = x \cdot z + y \cdot z$.

(iv) The semiring is called *idempotent* iff $+$ is idempotent, i.e., $x + x = x$.

In the previous definition as well as in the sequel we stipulate that multiplication binds stronger than addition. Defining the relation $\leq$ on an idempotent semiring A as

$$a \leq b :\Leftrightarrow a + b = b \quad \forall a, b \in A \ ,$$

makes $(A, \leq)$ into a poset. This partial order is the only one for which addition and multiplication are isotone. Thus the relation is called the *natural order* of the semiring. It induces a semilattice with $+$ as join and 0 as the least element. Since $+$ takes the role of supremum, the equation

$$a, b \leq c \Leftrightarrow a + b \leq c$$

is true for every idempotent semiring A for all $a, b, c \in A$. In calculations with partial orders, we often appeal to the principles of *indirect inequality* and *indirect equality*. Instead of $a \leq b$ we show $\forall c. c \leq a \Rightarrow c \leq b$ or $\forall c. b \leq c \Rightarrow a \leq c$. Likewise, $a = b$ can be proved by showing $\forall c. c \leq a \Leftrightarrow c \leq b$ or $\forall c. b \leq c \Leftrightarrow a \leq c$.
The class of (idempotent) semirings is quite rich. We now show some standard examples. The finite semirings with at most 4 elements are from [Con71].

Example 1

(i) $(\mathbb{Z}, +, \cdot, 0, 1)$ as well as all other rings and fields are semirings.

(ii) If $0 = 1$ in a semiring, then the semiring only consists of the element 0.

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

A semiring fulfilling the equation $0 = 1$ is called *trivial* and is obviously idempotent.

(iii) Consider the structure $(\{0, 1\}, +, \cdot, 0, 1)$ with addition and multiplication defined by the tables:

$+$	0	1
0	0	1
1	1	1

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

This structure is an idempotent semiring, called the *boolean semiring*, because $+$ and $\cdot$ take the roles of $\vee$ and $\wedge$, respectively. The natural order is $0 \leq 1$.

(iv) Another example of an idempotent semiring is given by the following tables:

$+$	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

The natural order of $(\{0, a, 1\}, +, \cdot, 0, 1)$ is characterised by $0 \leq 1 \leq a$.

(v) $(\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$ is an idempotent semiring, which is often called the *tropical semiring*. Its natural order can be calculated by

$$a \leq_{nat} b \Leftrightarrow \min(a, b) = b \Leftrightarrow a \geq b \ .$$

(vi) $(\mathbb{N} \cup \{-\infty\}, \max, +, -\infty, 0)$ is an idempotent semiring, where the natural order is the same as the ordinary one on the (natural) numbers.

(vii) Similar to (v) or (vi), we can create further idempotent semirings by using any binary idempotent function as addition. E.g. $(\mathbb{N}, \mathrm{ggT}, \cdot, 0, 1)$ forms a semiring. The natural order is the order of divisibility, i.e.,

$$a \leq b \Leftrightarrow a | b \Leftrightarrow \exists n \in \mathbb{N} : a \cdot z = b \ .$$

These examples and even more, especially examples consisting of 3 and 4 elements, can be found in [DMS03].

A special class of semirings are formed by the power set of an arbitrary partial semigroup X if we define the multiplication elementwise.

Definition 2.1.3 (Semiring over X)

Let X be an arbitrary set and $\cdot : X \times X \to X$ be a binary, associative and closed operation, which is allowed to be defined partially. Then $\mathcal{H}_X := (\mathcal{P}(X), \cup, \circ, \emptyset, 1)$ is called a *semiring over* X where

$$A \circ B \ := \ \{a \cdot b : a \in A, b \in B, a \cdot b \text{ is defined}\} \ , \quad A, B \in \mathcal{P}(X)$$

if there is a multiplicative neutral element, i.e.,

$$\exists 1 \in \mathcal{P}(A) : 1 \circ A = A \circ 1 = A \quad \forall A \in \mathcal{P}(A) \ .$$

If we use a monoid $(X, \cdot, 1_X)$ as carrier set, the multiplicative neutral element of the semiring over X is given by $\{1_X\}$. This means that $\{1_X\} \circ A = A \circ \{1_X\} = A$.
We observe that the semiring over X is idempotent with respect to the addition (set union). Therefore we calculate the natural order as

$$A \leq B \Leftrightarrow A \cup B = B \quad \forall A, B \in \mathcal{P}(X) \ .$$

The equation describes the subset relation, i.e., $A \leq B$ iff A is a subset of B. For simplification of some proofs we use the symbol $\subseteq$ instead of $\leq$ if we calculate with sets.
The class of semirings over X are again quite rich. We will give some well known examples.

Example 2

(i) Let Σ^* be the set of finite words over some alphabet Σ. Let $u{+}{+}v$ denote the concatenation of two words $u, v \in \Sigma^*$. Then the concatenation of two languages (set of words) $U, V \in \mathcal{P}(\Sigma^*)$ is defined by

$$\begin{array}{rcl} {+}{+} : \mathcal{P}(\Sigma^*) \times \mathcal{P}(\Sigma^*) & \rightarrow & \mathcal{P}(\Sigma^*) \\ U{+}{+}V & \mapsto & \{u{+}{+}v : u \in U, v \in V\} \ . \end{array}$$

$\mathrm{LAN}(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, {+}{+}, \emptyset, \{\varepsilon\})$ forms an idempotent semiring with the natural order defined by language inclusion. We call $\mathrm{LAN}(\Sigma)$ the semiring of *formal languages.* $\emptyset$ denotes the empty language and ε the empty word.

(ii) Consider a set V of vertices. Then subsets of V^* can be viewed as paths of graphs between the nodes of V. The composition of paths (*path fusion*), metaphorically speaking the gluing of two paths, is defined as a partial function. Let ε be the empty path, $x, y \in V$ and $s, t \in V^*$. $(y.t) \in V^* \backslash \{\varepsilon\}$ has the meaning that y represents the first node of a path and t describes the rest of the path excluding y. $(s.x)$ is defined similarly.

$$\begin{array}{rcl} \bowtie : V^* \times V^* & \rightarrow & V^* \\ \varepsilon \bowtie \varepsilon & \mapsto & \varepsilon \\ \varepsilon \bowtie (y.t) & & \text{undefined} \\ (s.x) \bowtie \varepsilon & & \text{undefined} \\ (s.x) \bowtie (y.t) & \mapsto & \left\{ \begin{array}{ll} s.x.t & \text{if } x = y \\ \text{undefined} & \text{if } x \neq y \ . \end{array} \right. \end{array}$$

As specified above, the operation $\bowtie$ can be lifted to a function $\bowtie : \mathcal{P}(V^*) \times \mathcal{P}(V^*) \rightarrow \mathcal{P}(V)$ by setting the operation as

$$S \bowtie T = \{s \bowtie t : s \in S, t \in T, s \bowtie t \text{ is defined}\} \ .$$

$\mathrm{PAT}(V) = (\mathcal{P}(V^*), \cup, \bowtie, \emptyset, V^{\leq 1})$ is the so-called *path semiring* over V^*, where $V^{\leq 1}$ is the set of all paths with 0 edges, i.e., all vertices itself and also the empty path. Hence

$$V^{\leq 1} = V \cup \{\varepsilon\} \ .$$

Note

In the sequel we assume the existence of the neutral element with respect to multiplication if we discuss semirings over X.

2.2 Kleene Algebras

Definition 2.2.1 (Kleene Algebra)
A *Kleene algebra* is a sextuple $(A, +, \cdot, 0, 1, ^*)$ such that $(A, +, \cdot, 0, 1)$ is an idempotent semiring and $^* : A \to A$ is a function satisfying the following unfold and induction laws:

$$1 + a \cdot a^* \leq a^* \ , \tag{$\ast$-1}$$

$$1 + a^* \cdot a \leq a^* \ , \tag{$\ast$-2}$$

$$b + a \cdot x \leq x \Rightarrow a^* \cdot b \leq x \ , \tag{$\ast$-3}$$

$$b + x \cdot a \leq x \Rightarrow b \cdot a^* \leq x \ . \tag{$\ast$-4}$$

A Kleene algebra is also called a *Kozen semiring* or *K-semiring*. A different characterisation of the operator * than the Equations ($\ast$-1)-($\ast$-4) is the definition via fixed points. $a^* \cdot b$ is the least fixed point of the function $\lambda x.b + a \cdot x$ and $b \cdot a^*$ is the least fixed point of $\lambda x.b + x \cdot a$. Further informations and properties of Kleene algebras are given for example in [Koz94]. Due to the fact that every Kleene algebra forms an idempotent semiring and that every semiring provides the structure of a semi-lattice, we can use knowledge about lattices to formulate properties of Kleene algebras.

Definition 2.2.2 (Boolean Kleene Algebra)
A Kleene algebra is called *boolean* iff the underlying lattice is boolean.

Considering the examples of the last paragraph, we show which semirings can be extended to Kleene algebras and which cannot.

Example 3

(i) The trivial semiring becomes a Kleene algebra with $0^* = 0\ (= 1)$.

(ii) The boolean semiring $(\{0, 1\}, +, \cdot, 0, 1)$ forms a Kleene algebra if we define $0^* = 1^* = 1$.

(iii) The semiring $(\{0, a, 1\}, +, \cdot, 0, 1)$ with the natural order $0 \leq 1 \leq a$ and addition and multiplication defined by the tables

$+$	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

forms a Kleene algebra if and only if $a^* = a$ and $0^* = 1^* = 1$.

(iv) We can only extend the tropical semiring $(\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$ to a Kleene algebra if we define $n^* = 0\ \forall n \in \mathbb{N} \cup \{\infty\}$. Otherwise we can show with simple calculations, that the Equations ($\ast$-1) to ($\ast$-4) cannot be satisfied.

(v) $(\mathbb{N} \cup \{-\infty\}, \max, +, -\infty, 0)$ does not form a Kleene algebra for all possibilities of the $^*-$operation. The cause is the unboundness of the set $\{a^n : n \in \mathbb{N}\} = \{n \cdot a : n \in \mathbb{N}\}$ for all $a > 0$. By Definition 2.2.1 a^* has to be the least fixed point and hence an upper bound of the set $\{a^n : n \in \mathbb{N}\}$.
This counterexample shows that there are idempotent semiring which cannot be extended to Kleene algebras. Thus the class of all Kleene algebras is a proper subset of the set of all idempotent semirings.

(vi) The semiring of formal languages LAN(Σ) is extendable if we set $L^* = \{w_1 w_2 \ldots w_n : n \geq 0, w_i \in L\}$ for all $L \subseteq \Sigma^*$.

(vii) Equivalently to (vi) we can enlarge $\mathrm{PAT}(V)$ to a Kleene algebra $(\mathcal{P}(V^*), \cup, \bowtie, \emptyset, V^{\leq 1}, ^{\leadsto})$, by defining $U^{\leadsto}$ as $\bigcup_{n\in\mathbb{N}} U^n$, $U \subseteq V^*$.

As mentioned above, every Kleene algebra contains a semi-lattice or even a lattice, as for example it is in boolean Kleene algebras. Thus we can exploit all properties of (semi-)lattices for semirings and Kleene algebras. A special property of lattices, called the μ-fusion rule, is needed for the proof of the engineer's induction (see Chapter 5).

Theorem 2.2.3 (μ-fusion)
Let $\mathcal{L}$ be a complete lattice and f, g, h isotone functions on $\mathcal{L}$. Here μ_f is an abbreviation for the least fixed point of f and μ_g describes the least fixed point of g. If h is universally disjunctive, then

$$h \circ f \leq g \circ h \Rightarrow h(\mu_f) \leq \mu_g \ .$$

Chapter 3

Residuals and Detachments

The base for the engineer's induction of Chapter 5 and for the duration calculus is formed by residuals and their relatives, the detachments. In the sequel we present these operators and prove some of their properties. Most of the proofs are based on [Möl].

In the case of existence the residuals can be smoothly defined on monoids, because we only need an arbitrary, binary operation. Due to the fact, that every Kleene algebra and every sequential algebra form at least one monoid, residuals can be defined on these structures.

3.1 Residuals

Residuals characterise largest solutions of certain linear equations. The right residual x/y is defined as the greatest element z fulfilling the equation $z \cdot y \leq x$. Similar to this, the left residual is the greatest solution of $y \cdot z \leq x$. They were studies for example in lattices by Birkhoff [Bir76]. Mostly residuals are defined by the following Galois connections.

Definition 3.1.1 (Residuals)
Consider a monoid $(A, \cdot, 1)$ over a poset $(A, \leq)$. Furthermore let x, y, z be elements of A.
The condition

$$z \leq x/y :\Leftrightarrow z \cdot y \leq x$$

defines the *right residual* x/y and

$$z \leq y \backslash x :\Leftrightarrow y \cdot z \leq x$$

characterises the *left residual* $y \backslash x$.

Since there is no guarantee for the existence of (left or right) residuals, a monoid with well-defined residuals is called *residuated monoid.* According to this we define *residuated semirings* and *residuated Kleene algebras.*

Remarkably, on each semiring $(\mathcal{P}(A), \cup, \circ, \emptyset, 1)$ over a set A (see chapter 2) the residuals are definable. In [BJ72] it is shown that in this case the residuals can be calculated by

$$\begin{array}{rcl} X/Y & = & \{z \in A : (\forall y \in Y)\, y \cdot z \in X\}, \\ Y \backslash X & = & \{z \in A : (\forall y \in Y)\, z \cdot y \in X\}. \end{array}$$

Example 4

(i) For arbitrary groups G (typed in multiplicative form) with a (partial) order, the right residual x/y is the same as multiplication by the inverse of y to x from the right, i.e.,

$$x/y = x \cdot y^{-1}.$$

Proof:

$$\begin{array}{ll} & z \leq x/y \\ \Leftrightarrow & z \cdot y \leq x \\ \Leftrightarrow & z \cdot y \cdot y^{-1} \leq x \cdot y^{-1} \\ \Leftrightarrow & z \leq x \cdot y^{-1} \\ \Rightarrow & x/y = x \cdot y^{-1} \end{array}$$

□

Similarly, the left residual coincides with multiplication by y^{-1} from the left:

$$y\backslash x = y^{-1} \cdot x.$$

(ii) The same relation between the residuals and inverse elements as in (i) are given in rings (w.r.t. addition) and fields.

(iii) In the monoid $M = (\mathbb{N} \cup \{\infty\}, \cdot, 1)$ satisfying the equation $0 \cdot \infty = \infty \cdot 0 = 0$, right and left residual coincide, because M is commutative. In M the residuals describe integer division, i.e., the residuals are the same as $\lfloor x/y \rfloor$, where $\lfloor z \rfloor$ denotes the rounding to the next integer which is smaller or equal than z. If we consider the submonoid $M' = (\mathbb{N}, \cdot, 1)$, the residuals cannot be defined anymore, because $\lfloor n/0 \rfloor \notin M', n \in \mathbb{N}\backslash\{0\}$.

(iv) A very interesting example is shown in [Jip02] and [Pra91] by Jipsen and Pratt, respectively. They describe residuals as events in 'real life'.
Consider the following events:

p : "Bet on a horse"
q : "Horse wins."
r : "Get rich."

The equation $pq \leq r$ describes the following fact:

"If you bet on a horse and it then wins you get rich."

Contrary to this, the residuals characterise the following:
$p \leq r/q$:

"If you bet on a horse you get rich if the horse then wins."

$q \leq p\backslash r$:

"If a horse wins then had you bet on it you would get rich."

Example (iii) implies directly the following simple property.

Corollary 3.1.2
Let $(A, \cdot, 1, \backslash, /)$ be a residuated monoid. If there is an annihilator 0 in A, i.e., $a \cdot 0 = 0 = 0 \cdot a \; \forall a \in A$ and is 0 also the least element, then A has also a greatest element $\top$.

Proof:

Let $a \in A$.

$$\begin{array}{ll} & x \leq a/0 \\ \Leftrightarrow & x \cdot 0 \leq a \\ \Leftrightarrow & \texttt{true} \\ \Rightarrow & \text{The (right) residual has to be } \top. \end{array}$$

□

After the presentation of lots of examples, we list many of the major properties of residuals. Most of the lemmatas and theorems are valid for the right as well as for the left residuals. We only show the properties for the first ones. The proofs for the left residuals are symmetrical and therefore we omit them. Furthermore we assume a residuated monoid $(A, \cdot, 1, \backslash, /)$ and suppose u, v, x, y, z to be elements of A.

Lemma 3.1.3
The following equations hold:

(i) $x \leq (x \cdot y)/y$

(ii) $x \leq y \backslash (y \cdot x)$

Proof:

$$\begin{array}{ll} & x \leq (x \cdot y)/y \\ \Leftrightarrow & x \cdot y \leq x \cdot y \\ \Leftrightarrow & \texttt{true} \end{array}$$

□

Lemma 3.1.4
(i) $(x/y) \cdot y \leq x$

(ii) $y \cdot (y \backslash x) \leq x$

Proof:

Replace z by (x/y) and $(y \backslash x)$, respectively, in Definition (3.1.1) of the residuals.

□

Lemma 3.1.5
(i) $x/(y \cdot z) = (x/z)/y$

(ii) $(z \cdot y) \backslash x = y \backslash (z \backslash x)$

Proof:

$$\begin{array}{ll} & u \leq x/(y \cdot z) \\ \Leftrightarrow & u \cdot y \cdot z \leq x \\ \Leftrightarrow & u \cdot y \leq x/z \\ \Leftrightarrow & u \leq (x/z)/y \end{array}$$

□

Lemma 3.1.6 (Euclid for Residuals)
(i) $x \cdot (y/z) \leq (x \cdot y)/z$

(ii) $(z \backslash y) \cdot x \leq z \backslash (y \cdot x)$

Proof:

$$\begin{array}{ll} & x \cdot (y/z) \leq (x \cdot y)/z \\ \Leftrightarrow & x \cdot (y/z) \cdot z \leq (x \cdot y) \\ \overset{3.1.4}{\Leftarrow} & x \cdot y \leq x \cdot y \\ \Leftrightarrow & \texttt{true} \end{array}$$

□

Lemma 3.1.7
Assume that the monoid A has a greatest element $\top$, then

(i) $\top/x = \top$

(ii) $x\backslash\top = \top$

<u>Proof:</u>

Because $\top$ is the greatest element we only have to show that $\top \leq \top/x$.

$$\begin{array}{ll} & \top \leq \top/x \\ \Leftrightarrow & \top \cdot x \leq \top \\ \Leftrightarrow & \texttt{true} \end{array}$$

□

Lemma 3.1.8

(i) $x/1 = x$

(ii) $1\backslash x = x$

<u>Proof:</u>

$$\begin{array}{ll} & u \leq x/1 \\ \Leftrightarrow & u \cdot 1 \leq x \\ \Leftrightarrow & u \leq x \end{array}$$

□

Lemma 3.1.9 (Isotonicity)

(i) $x \leq y \Rightarrow z/y \leq z/x$

(ii) $x \leq y \Rightarrow y\backslash z \leq x\backslash z$

<u>Proof:</u>

$$\begin{array}{ll} & u \leq z/x \\ \Leftrightarrow & u \cdot x \leq z \\ \Leftarrow & u \cdot y \leq z \\ \Leftrightarrow & u \leq z/y \end{array}$$

□

Lemma 3.1.10 (Associativity)

$x\backslash(y/z) = (x\backslash y)/z$

<u>Proof:</u>

$$\begin{array}{ll} & u \leq x\backslash(y/z) \\ \Leftrightarrow & x \cdot u \leq y/z \\ \Leftrightarrow & x \cdot u \cdot z \leq y \\ \Leftrightarrow & u \cdot z \leq x\backslash y \\ \Leftrightarrow & u \leq (x\backslash y)/z \end{array}$$

□

Now we extend the residuated monoid $(A, \cdot, 1, \backslash, /)$ and assume that $(A, +, \cdot, 0, 1, \backslash, /)$ is a residuated idempotent semiring. We assume that the residuals are defined with respect to multiplication and not to addition. Furthermore, we assume the existence of the infimum $\sqcap$ in A, i.e., $x \sqcap y := \inf\{x, y\}$.

Lemma 3.1.11 (Left-Conjunctivity)
Let X be a subset of A.

(i) $(\sqcap X)/y = \sqcap(X/y)$

(ii) $y\backslash(\sqcap X) = \sqcap(y\backslash X)$

Proof:

$$\begin{array}{ll} & u \leq (\sqcap X)/y \\ \Leftrightarrow & u \cdot y \leq \sqcap X \\ \Leftrightarrow & \forall x \in X \ : \ u \cdot y \leq x \\ \Leftrightarrow & \forall x \in X \ : \ u \leq x/y \\ \Leftrightarrow & u \leq \sqcap(X/y) \end{array}$$

□

Lemma 3.1.12 (Right-Antidisjunctivity)
Let Y be a subset of A and assume $\cdot$ to be universal disjunctive.

(i) $x/(\sqcup Y) = \sqcap(x/Y)$

(ii) $(\sqcup Y)\backslash x = \sqcap(Y\backslash x)$

Proof:

$$\begin{array}{ll} & u \leq x/\sqcup Y \\ \Leftrightarrow & u \cdot (\sqcup Y) \leq x \\ \Leftrightarrow & \sqcup(u \cdot Y) \leq x \\ \Leftrightarrow & \forall y \in Y : u \cdot y \leq x \\ \Leftrightarrow & \forall y \in Y : u \leq x/y \\ \Leftrightarrow & u \leq \sqcap(x/Y) \end{array}$$

□

3.2 Detachments

If the residuated monoids have a further operation, the negation, we can define the detachments. Detachments are special operations which simulate one possible cooperation between the residuals and the negation. In the semiring of formal languages LAN, they cut off subwords from the left and the right. First we give a formal definition of negation:

Definition 3.2.1 (Negation)
Let $(A, +, 0)$ be an idempotent semiring with $\top$ as the greatest element. (We assume that $\top$ exist.) The *negation* is an operation $\overline{} : A \to A$ satisfying the following properties for all $x, y \in A$:

- $\overline{\overline{x}} = x$,
- $x + \overline{x} = \top$,
- $x \leq y \Rightarrow \overline{y} \leq \overline{x}$ (w.r.t. the natural order).

The first two equations imply $\overline{\top} = 0$ and $\overline{0} = \top$. In addition the de Morgan's laws are valid in semirings with negation iff the existence of infima and sumprema are garuanteed (e.g. in lattices). The latter one is given by addition.

Lemma 3.2.2 (De Morgan's Laws)
For two elements x and y consider $x \sqcap y := \inf\{x, y\}$, then:

$$\overline{x + y} = \overline{x} \sqcap \overline{y} \qquad\qquad \overline{x \sqcap y} = \overline{x} + \overline{y}$$

Proof:

$$\begin{aligned} & z \leq \overline{x \sqcup y} \\ \Leftrightarrow \quad & \overline{\overline{x \sqcup y}} \leq \overline{z} \\ \Leftrightarrow \quad & x \sqcup y \leq \overline{z} \\ \Leftrightarrow \quad & x \leq \overline{z} \wedge y \leq \overline{z} \\ \Leftrightarrow \quad & z \leq \overline{x} \wedge z \leq \overline{y} \\ \Leftrightarrow \quad & z \leq \overline{x} \sqcap \overline{y} \end{aligned}$$

The second equation can be proved similarly. We remark that each two of the equations given in Definition 3.2.1 imply the laws of de Morgan.

□

Definition 3.2.3 (Detachments)
Let $H = (A, \cdot, +, 1, 0, \backslash, /, \overline{})$ be a residuated idempotent semiring with negation. The *right detachment* is defined by

$$x \lfloor y := \overline{\overline{x}/y}.$$

Symmetrically the *left detachment* is defined by

$$y \rfloor x := \overline{y \backslash \overline{x}}.$$

Example 5
We explain the detachments with the help of LAN(Σ). The negation of an element $A \in \mathcal{P}(\Sigma^*)$ (a set of words) is defined as the complementation of A, i.e., $x \in \overline{A} \Leftrightarrow x \notin A$ for all $x \in \Sigma^*$. As we showed at the beginning of this chapter the residuals of LAN are well defined and can be calculated very easily. The detachments $x \lfloor y$ and $y \rfloor x$, respectively, arise by cutting off postfixes and prefixes from words in x in all possible ways. The postfixes (prefixes) have to be in y. To illustrate the result of this operator, we give a few little examples:
Let $\Sigma = \{a, b, c\}$

- $\{abbc\} \lfloor \{bc\} = \{ab\}$,
  $\{ab\} \rfloor \{abbc\} = \{bc\}$,
- $\{ab\} \lfloor \{c\} = \{\}$,
- $\{ab, aab, abc\} \lfloor \{ab, c\} = \{\varepsilon, a, ab\}$.

In the sequel we suppose a residuated idempotent semiring with negation H as in the Definition 3.2.3, which we call *detachment semiring*. Furthermore we consider u, v, x, y, z to be elements of H. In the following we give a briefly overview over the main properties of detachments. The proofs are only done for right detachments. Similarly to the residuals, the proofs for left detachments are omitted.

Lemma 3.2.4 (Universal Disjunctivity)
If $\sqcap$ exist

(i) $(\sqcup X) \lfloor y = \sqcup (X \lfloor y)$

(ii) $y \rfloor (\sqcup X) = \sqcup (y \rfloor X)$

Proof:

$$\begin{array}{rl} & (\sqcup X)\lfloor y \\ = & \overline{(\overline{\sqcup X})/y} \\ = & \overline{(\sqcap\overline{X})/y} \\ \overset{3.1.11}{=} & \overline{\sqcap(\overline{X}/y)} \\ = & \sqcup(\overline{\overline{X}/y}) \\ = & \sqcup(X\lfloor y) \end{array}$$

□

Especially we have $(x+y)\lfloor z = x\lfloor z + y\lfloor z$ and $z\rfloor(x+y) = z\rfloor x + z\rfloor y$.

Lemma 3.2.5 (Disjunctivity)
We assume the existence of $\sqcup$ and $\sqcap$. Then:

(i) $x\lfloor(\sqcup Y) = \sqcup(x\lfloor Y)$

(ii) $(\sqcup Y)\rfloor x = \sqcup(Y\rfloor x)$

Proof:

$$\begin{array}{rl} & x\lfloor(\sqcup Y) \\ = & \overline{\overline{x}/(\sqcup Y)} \\ \overset{3.1.12}{=} & \overline{\sqcap\{\overline{x}/y : y \in Y\}} \\ \overset{3.2.2}{=} & \sqcup\{\overline{(\overline{x}/y)} : y \in Y\} \\ = & \sqcup\{x\lfloor y : y \in Y\} \\ = & \sqcup(x\lfloor Y) \end{array}$$

□

Lemma 3.2.6
(i) $x\lfloor(y\cdot z) = (x\lfloor z)\lfloor y$

(ii) $(z\cdot y)\rfloor x = (y\rfloor z)\rfloor x$

Proof:

$$\begin{array}{rl} & x\lfloor(y\cdot z) \\ = & \overline{\overline{x}/(y\cdot z)} \\ \overset{3.1.5}{=} & \overline{(\overline{x}/z)/y} \\ = & \overline{\overline{\overline{(\overline{x}/z)}}/y} \\ = & (x\lfloor z)\lfloor y \end{array}$$

□

Lemma 3.2.7
$(x\rfloor y)\lfloor z = x\rfloor(y\lfloor z)$

Proof:

$$\begin{array}{cl}
 & (x\rfloor y)\lfloor z \\
= & \overline{\overline{\overline{x\backslash\overline{y}}}/z} \\
= & \overline{(x\backslash\overline{y})/z} \\
\overset{3.1.10}{=} & \overline{x\backslash(\overline{y}/z)} \\
= & \overline{x\backslash\overline{\overline{\overline{y}}/z}} \\
= & x\rfloor(y\lfloor z)
\end{array}$$

□

Lemma 3.2.8 (Isotonicity)

(i) $u \le v \Rightarrow x\lfloor u \le x\lfloor v$

(ii) $u \le v \Rightarrow u\rfloor x \le v\rfloor x$

Proof:

Immediate from Lemma 3.2.5.

□

Lemma 3.2.9

(i) $x\lfloor 1 = x = 1\rfloor x$

(ii) $y \ge 1 \Rightarrow x\lfloor y \ge x \wedge y\rfloor x \ge y$
Especially $\top\lfloor y = \top$ (provided that $\top$ exists).

(iii) Moreover we have:

$$x\lfloor(\top\lfloor y) \le x\lfloor\top \qquad\qquad (y\rfloor\top)\rfloor x \le \top\rfloor x$$

Proof:

(i)

$$\begin{array}{cl}
 & x\lfloor 1 \\
= & \overline{\overline{x}/1} \\
\overset{3.1.8}{=} & \overline{\overline{x}} \\
= & x
\end{array}$$

(ii),(iii) Immediate from isotonicity of $\lfloor$ (3.2.8) and (i).

□

3.3 Semirings, Sequential Algebras, Residuated Kleene Algebras and Observation Spaces

In the literature concerning duration calculus, real-time systems and similar topics, the structures of *sequential algebras* ([Kar00, Kar01]), *residuated Kleene algebra* ([Jip02]) as well as *observation spaces* ([Kar96, Kar00]) are often used. For this reason we define these structures in the sequel and compare them. In contrast to detachment semirings, the sequential algebras are defined as follows.

Definition 3.3.1 (Sequential Algebra (cf. [Kar96]))
A *sequential algebra* is a complete boolean lattice $(S, \cap, \cup, \overline{})$ with greatest element $\top$ and least element $\bot$ together with three binary operators (composition $\cdot$, left division $\lfloor$ and right division $\rfloor$) satisfying the following axioms:

$$(S, \cdot, 1) \text{ is a monoid,} \qquad \text{(Monoid)}$$

$$P \rfloor Q \subseteq \overline{R} \;\Leftrightarrow\; P \cdot R \subseteq \overline{Q} \;\Leftrightarrow\; Q \lfloor R \subseteq \overline{P}, \qquad \text{(Exchange)}$$

$$P \cdot (Q \lfloor R) \subseteq (P \cdot Q) \lfloor R, \qquad \text{(Euclid)}$$

$$1 \lfloor P = P \rfloor 1. \qquad \text{(Reflection)}$$

Without the inequauation of Euclid and the reflection law this structure is equivalent to a detachment semiring with a boolean algebra as the underlying lattice. Therefore the class of sequential algebras is a proper subclass of the class of detachment semirings. As mentioned above, Kleene algebras are idempotent semirings with an additional *-operation. One possible motivation to consider residuated Kleene algebras is given by Jipsen in [Jip02]. In his paper he shows that the class of Kleene algebras is not closed under homomorphic mappings. By contrast the class of residuated Kleene algebras is closed.[1] Another characteristic feature of residuated Kleene algebras is the equivalence of the two horn clauses, i.e., $(*\text{-}3) \Leftrightarrow (*\text{-}4)$.[1]
In the following diagram (fig. 3.1) we summarise the relationships between (residuated) Kleene algebras and the other algebraic structures used in this report as idempotent semirings. Here, X can be embedded into Y iff there is a path of directed edges from X to Y.

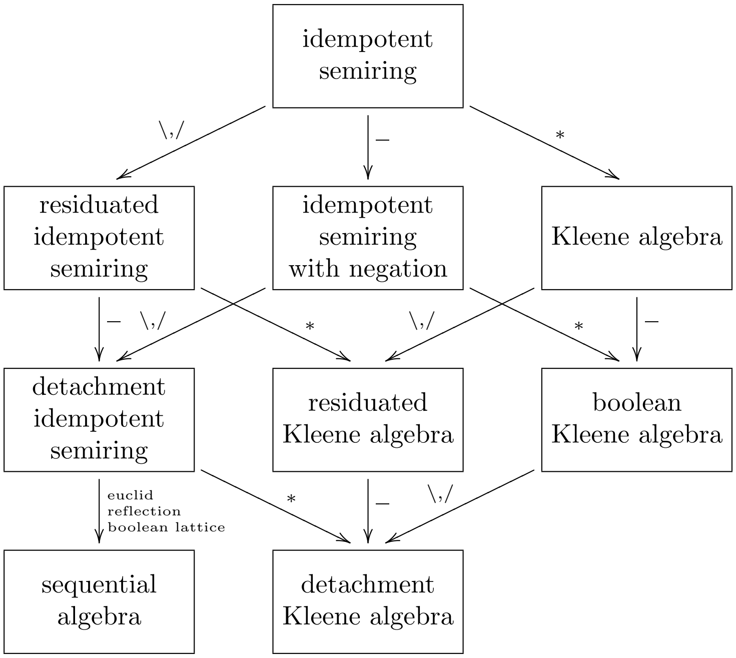

idempotent semiring
\,/
−
*
residuated idempotent semiring
idempotent semiring with negation
Kleene algebra
− \,/
*
\,/
*
−
detachment idempotent semiring
residuated Kleene algebra
boolean Kleene algebra
euclid
reflection
boolean lattice
*
−
\,/
sequential algebra
detachment Kleene algebra

Figure 3.1: Relationship between different algebraic structures

Von Karger uses in his work concerning duration calculus not only sequential algebras but also observation spaces and time diagrams. In the sequel we define these two structures and relate them to the algebraic concepts we discussed before.
An observation interval in general is an interval of time. Von Karger postulates that observation intervals are intervals of real numbers, which are finite and closed.

[1] A proof can be found in [Jip02] and in the appendix A.

Definition 3.3.2 (Time Diagram)
Let Σ be a set of possible states of an arbitrary system S. A function $x : B \to \Sigma$, which describes the behaviour of S is called a *time diagram*.
A time diagram $y : B \to \Sigma$, where B is a single point, is denoted as *unit*. The *left unit* $\overleftarrow{x}$ of a time diagram $x : [a, b] \to \Sigma$ is the restriction to the leftmost point of its observation interval, that is $\overleftarrow{x} : [a, a] \to \Sigma$ with $\overleftarrow{x}(a) = x(a)$. Corresponding to this the *right unit* $\overrightarrow{x}$ is the restriction to the rightmost points of its observation interval. Thus $\overrightarrow{x} : [b, b] \to \Sigma$ where $\overrightarrow{x}(b) = x(b)$.

$\leftarrow$ and $\rightarrow$ define two unary operators on time diagrams. Additionally we can define the sequential composition, which is a binary operation. Therefore we assume two observation intervals B_1, B_2, a set of states Σ and time diagrams x, y.

$$\begin{array}{rcl} ; : (B_1 \to \Sigma) \times (B_2 \to \Sigma) & \to & ((B_1 \cup B_2) \to \Sigma) \\ x; y & \mapsto & \begin{cases} x \cup y \text{ if } \overrightarrow{x} = \overleftarrow{y} \\ \text{undefined otherwise.} \end{cases} \end{array}$$

The definition of the sequential composition allows the construction of an idempotent semiring by lifting this operation to sets of time diagrams (cf. Chapter 2). More precisely the semiring of time diagrams is defined as $\text{TIME}(\mathcal{B}, \Sigma) := (\mathcal{P}(X), \cup, ;, \emptyset, Id)$, where

$$\begin{array}{l} \mathcal{B} \text{ is a set of observation intervals,} \\ \Sigma \text{ is a set of possible states,} \\ X = \{x : (x : B \to \Sigma), B \in \mathcal{B}\}, \\ Id = \{x : x \in X, x \text{ is a unit}\}. \end{array}$$

By setting $Y^* = \bigcup_{i \in \mathbb{N}} Y^i$, where $Y^0 = Id$ and $Y^{i+1} = Y; Y^i$, $\text{TIME}(\mathcal{B}, \Sigma)$ can be enlarged to a Kleene algebra. Furthermore, negation is given by set complementation and the existence of residuals is guaranteed. So we even get a detachment Kleene algebra. Moreover von Karger uses among time diagrams also observation spaces.

Definition 3.3.3 (Observation Space)
A set A together with two unary operators $\leftarrow$ and $\rightarrow$ and one binary operation ; is an observation space Obs iff it satisfies the following laws:

1. $x; y$ is defined if and only if $\overrightarrow{x} = \overleftarrow{y}$.

2. If $x; y$ is defined then $\overleftarrow{x; y} = \overleftarrow{x}$ and $\overrightarrow{x; y} = \overrightarrow{y}$.

3. Composition ; is associative.

4. If e is an unit, i.e., $e = \overleftarrow{x}$ or $e = \overrightarrow{x}$ then $\overleftarrow{e} = e = \overrightarrow{e}$.

5. $\overleftarrow{x}; x = x = x; \overrightarrow{x}$.

6. (Reflection) If $x; y$ is an unit then so is $y; x$.

7. (Local Linearity) If $x; y = x'; y'$, then there is a mediating element of the time diagram z, which satisfies either ($x; z = x'$ and $y = z; y'$) or ($x = x'; z$ and $z; y = y'$).

It is easy to show that $\text{TIME}(\mathcal{B}, \Sigma)$ forms an observation space. For this we lift $\leftarrow$ and $\rightarrow$ from time diagrams to sets of time diagrams, i.e., let $Y \in \mathcal{P}(\{x : (x : B \to \Sigma), B \in \mathcal{B}\})$, then

$$\begin{array}{rcl} \overleftarrow{Y} & := & \{\overleftarrow{y} : y \in Y\}, \\ \overrightarrow{Y} & := & \{\overrightarrow{y} : y \in Y\}. \end{array}$$

By straightforward calculations, we see that $\text{TIME}(\mathcal{B}, \Sigma)$ satisfies the inequality of Euclid and the exchange law (see 3.3.1). For this reason it is also a sequential algebra.

Chapter 4

Interval Modalities

Normally the interval modalities are used to describe behaviours of a specification that must never occur, for example explosions or an illegal allocation. Because we want to never reach such a situation, we will define a special operator for this behaviour. Categorically we distinguish between two different kinds of operators. On the one hand the positive interval modalities describe the situations where a state appears at least at once or always. In the algebraic point of view they are based on the multiplication of a semiring. On the other hand the negative interval modalities describe situations that must never arise or that a desirable behaviour will occur eventually. These modalities are closely connected to the detachments of the previous chapter.
In the sequel we define the interval modalities and present some examples. Accordingly we will give some properties of the interval modalities with regard to the engineer's induction (Chapter 5) and the duration calculus (Chapter 6). For further details we point out the articles by von Karger [Kar00] and [Kar96].

4.1 Definition and Examples

Definition 4.1.1 (Positive Interval Modalities)
Let $H = (A, +, \cdot, 0, 1, \overline{})$ be a negated semiring and let $a \in A$. Then the *positive interval operators* are defined as:

$$\begin{aligned} \diamondplus a &:= \top \cdot a \cdot \top, \\ \boxplus a &:= \overline{\diamondplus \overline{a}}. \end{aligned}$$

If we examine the semiring of formal languages $LAN(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, ++, \emptyset, \varepsilon)$ over an alphabet Σ with respect to this definition, the greatest element is described by $\top = \Sigma^* = \{a : a \in \Sigma^*\}$ and therefore $\diamondplus a = \Sigma^* ++ a ++ \Sigma^*$. This means that $\diamondplus a$ includes all and only all the words x which have a as a part.

$$x \in \diamondplus a \Leftrightarrow \exists u_1, u_2 \in \Sigma^* \; \exists \hat{a} \in a : u_1 ++ \hat{a} ++ u_2 = x.$$

The other positive modality $\boxplus a = \overline{\diamondplus \overline{a}} = \overline{\Sigma^* ++ \overline{a} ++ \Sigma^*}$ is the set of all words x which has no sub-word not equal to an element of a, i.e.,

$$x \in \boxplus a \Leftrightarrow \forall u_1, u_2 \in \Sigma^* \; \forall \hat{a} \in \overline{a} : u_1 ++ \hat{a} ++ u_2 \neq x.$$

In other words each part of an element of $\boxplus a$ has to be a word in a.
Due to $\Sigma^* ++ \overline{a} ++ \Sigma^* = \Sigma^*$ if $\varepsilon \in \overline{a}$, $\boxplus a$ forms the empty language.

$$\boxplus a = \overline{\Sigma^* ++ \overline{a} ++ \Sigma^*} = \overline{\Sigma^*} = \emptyset \text{ if } \varepsilon \in \overline{a}.$$

This property can be formulated for semirings in general.

Lemma 4.1.2
Let $H = (A, +, \cdot, 0, 1, \overline{})$ be a negated semiring with greatest element $\top$. Then

$$1 \leq \overline{a} \Rightarrow \boxplus a = 0.$$

Proof:

$$\begin{array}{ll} & \overline{a} \geq 1 \\ \Rightarrow & \top \cdot \overline{a} \cdot \top \geq \top \cdot 1 \cdot \top = \top \\ \Rightarrow & \boxplus a = \overline{\top} = 0 \end{array}$$

$\square$

The positive interval modalities describe the relationship between any element a and $\top$ with respect to the multiplication. But, the relationship to $\top$ w.r.t. the detachment is also of interest.

Definition 4.1.3 (Negative Interval Operators)
Let $H = (A, +, \cdot, 0, 1, \backslash, /, \overline{})$ be a detachment semiring and $a \in A$. The *negative interval* modalities are defined as:

$$\begin{array}{rcl} \diamondminus a & := & \top\rfloor(a\lfloor\top) = (\top\rfloor a)\lfloor\top = \top\rfloor a\lfloor\top, \\ \boxminus a & := & \overline{\diamondminus \overline{a}}. \end{array}$$

Note
Straightforward calculations show the following relation between the second interval modality and residuals:

$$\boxminus a = \top\backslash a/\top.$$

We give again an interpretation of the modalities in the semiring of formal languages $LAN(\Sigma)$ over a finite alphabet Σ. $b\rfloor a$ cuts off the words of b from the left of elements of a, if the elements of b are prefixes of elements of a (cf. Section 3.2). Therefore $\diamondminus a = \Sigma^*\rfloor a\lfloor\Sigma^*$ is the set of all (connected) sub-words of elements of a, i.e.,

$$x \in \diamondminus a \Leftrightarrow \exists u_1, u_2 \in \Sigma^* : u_1{+\!+}x{+\!+}u_2 \in a.$$

Now we calculate $\boxminus a$:

$$\begin{array}{rcl} x \in \boxminus a & \Leftrightarrow & x \in \overline{\diamondminus \overline{a}} \\ & \Leftrightarrow & x \notin \diamondminus \overline{a} \\ & \Leftrightarrow & \nexists u_1, u_2 \in \Sigma^* \ : \ u_1{+\!+}x{+\!+}u_2 \in \overline{a} \\ & \Leftrightarrow & \forall u_1, u_2 \in \Sigma^* : u_1{+\!+}x{+\!+}u_2 \in a. \end{array}$$

In words $\boxminus a$ is the set of all words which are closed under the left and right addition of $\top$ to a. Similar to the property of $\boxplus a$, shown above, we can give a relation between 1 and $\boxminus a$:

Lemma 4.1.4
Let H be the same as in Definition 4.1.3 then:

$$a = \top \quad \Leftrightarrow \quad 1 \leq \boxminus a.$$

<u>Proof:</u>

$$\begin{array}{ll} & 1 \le \boxminus a \\ \Leftrightarrow & 1 \le \top\backslash a/\top \\ \Leftrightarrow & \top \cdot 1 \cdot \top \le a \\ \Leftrightarrow & \top \le a \end{array}$$

□

Together with straightforward calculations for residuals the definitions of the interval modalities imply the following coherence between the modalities and the elements of $\top$ and 0.

Corollary 4.1.5
$\diamondplus\top = \top,\ \diamondplus 0\ = 0,\ \diamondminus\top = \top,\ \diamondminus 0\ = 0.$

4.2 Properties

The remaining chapter presents properties of the positive and the negative modalities. In particular the properties required for the engineer's induction and the duration calculus are shown. For simplification we assume that $H = (A, +, \cdot, 0, 1, \backslash, /, \overline{})$ is a detachment semiring with greatest element $\top$. Further we assume elements a, b of A.
At first we show that the positive and negative interval modalities are isotone and idempotent. Further one positive (negative) modality is disjunctive and the other one conjunctive.

Lemma 4.2.1 (Isotony)
Let $a \le b$, then:

(i) $\diamondplus a \le \diamondplus b$

(ii) $\boxplus a \le \boxplus b$

(iii) $\diamondminus a \le \diamondminus b$

(iv) $\boxminus a \le \boxminus b$

<u>Proof:</u>

(i)

$$\begin{array}{ll} & \diamondplus a \le \diamondplus b \\ \Leftrightarrow & \quad \{\text{definition of } \diamondplus\} \\ & \top \cdot a \cdot \top \le \top \cdot b \cdot \top \\ \Leftarrow & \quad \{\text{isotonicity w.r.t. multiplication}\} \\ & a \cdot \top \le b \cdot \top \\ \Leftarrow & \quad \{\text{isotonicity w.r.t. multiplication}\} \\ & a \le b \end{array}$$

(ii)

$$\begin{array}{ll} & \boxplus a \le \boxplus b \\ \Leftrightarrow & \overline{\diamondplus \overline{a}} \le \overline{\diamondplus \overline{b}} \\ \Leftrightarrow & \diamondplus \overline{b} \le \diamondplus \overline{a} \\ \overset{(i)}{\Leftarrow} & \overline{b} \le \overline{a} \\ \Leftrightarrow & a \le b \end{array}$$

(iii)

$$\begin{array}{ll}
 & \diamondminus a \leq \diamondminus b \\
\Leftrightarrow & \quad \{\text{definition of } \diamondminus\} \\
 & \top\rfloor a\lfloor\top \leq \top\rfloor b\lfloor\top \\
\Leftarrow & \quad \{\text{isotonicity (3.2.8)}\} \\
 & a\lfloor\top \leq b\lfloor\top \\
\Leftarrow & \quad \{\text{isotonicity (3.2.8)}\} \\
 & a \leq b
\end{array}$$

(iv) Similar to (ii).

□

Lemma 4.2.2 (Idempotency)

(i) $\diamondplus\diamondplus a = \diamondplus a$

(ii) $\boxplus\boxplus a = \boxplus a$

(iii) $\diamondminus\diamondminus a = \diamondminus a$

(iv) $\boxminus\boxminus a = \boxminus a$

Proof:

(i)

$$\begin{array}{rcl}
\diamondplus\diamondplus a & = & \top\cdot\top\cdot a\cdot\top\cdot\top \\
 & = & \top\cdot a\cdot\top \\
 & = & \diamondplus a
\end{array}$$

(ii)

$$\begin{array}{rcl}
\boxplus\boxplus a & = & \overline{\diamondplus(\overline{\boxplus a})} \\
 & = & \overline{\diamondplus(\overline{\overline{\diamondplus\overline{a}}})} \\
 & = & \overline{\diamondplus(\diamondplus\overline{a})} \\
 & \overset{(i)}{=} & \overline{\diamondplus\overline{a}} \\
 & = & \boxplus a
\end{array}$$

(iii)

$$\begin{array}{ll}
 & \diamondminus\diamondminus a \\
= & \quad \{\text{definition of } \diamondminus a\} \\
 & (\top\rfloor((\top\rfloor a)\lfloor\top))\lfloor\top \\
= & \quad \{3.2.7\} \\
 & \top\rfloor(((\top\rfloor a)\lfloor\top)\lfloor\top) \\
= & \quad \{3.2.6\} \\
 & \top\rfloor((\top\rfloor a)\lfloor(\top\cdot\top)) \\
= & \quad \{\text{3.2.7 and idempotency of } \top\} \\
 & (\top\rfloor(\top\rfloor a))\lfloor\top \\
= & \quad \{3.2.6\} \\
 & ((\top\cdot\top)\rfloor a)\lfloor\top \\
= & \quad \{\text{idempotency of } \top\} \\
 & (\top\rfloor a)\lfloor\top \\
= & \quad \{\text{definition of } \diamondminus a\} \\
 & \diamondminus a
\end{array}$$

(iv) Similar to (ii).

□

Lemma 4.2.3 (Disjunctivity)

(i) $\diamondplus(a+b) = \diamondplus a + \diamondplus b$

(ii) $\diamondminus(a+b) = \diamondminus a + \diamondminus b$

Proof:

(i)

$$\begin{aligned}
\diamondplus(a+b) &= \top \cdot (a+b) \cdot \top \\
&= \top \cdot a \cdot \top + \top \cdot b \cdot \top \\
&= \diamondplus a + \diamondplus b
\end{aligned}$$

(ii)

$$\begin{aligned}
\diamondminus(a+b) &= \top\rfloor(a+b)\lfloor\top \\
&\overset{3.2.4}{=} \top\rfloor(a\lfloor\top + b\lfloor\top) \\
&\overset{3.2.4}{=} \top\rfloor a\lfloor\top + \top\rfloor b\lfloor\top \\
&= \diamondminus a + \diamondminus b
\end{aligned}$$

□

Lemma 4.2.4 (Conjunctivity)
If we assume the existence of join ($\sqcup$) and meet ($\sqcap$), then

(i) $\boxplus(a \sqcap b) = \boxplus a \sqcap \boxplus b$

(ii) $\boxminus(a \sqcap b) = \boxminus a \sqcap \boxminus b$

Proof:

(i)

$$\begin{aligned}
& \boxplus(a \sqcap b) \\
= \quad & \{\text{definition of } \boxplus\} \\
& \overline{\top \cdot \overline{(a \sqcap b)} \cdot \top} \\
= \quad & \{\text{de Morgan (3.2.2)}\} \\
& \overline{\top \cdot (\overline{a} \sqcup \overline{b}) \cdot \top} \\
= \quad & \{4.2.3\} \\
& \overline{(\top \cdot \overline{a} \cdot \top) \sqcup (\top \cdot \overline{b} \cdot \top)} \\
= \quad & \{\text{de Morgan (3.2.2)}\} \\
& \overline{(\top \cdot \overline{a} \cdot \top)} \sqcap \overline{(\top \cdot \overline{b} \cdot \top)} \\
= \quad & \{\text{definition of } \boxplus\} \\
& \boxplus a \sqcap \boxplus b
\end{aligned}$$

(ii) Immediate from 3.1.11.

□

Not only these fundamental properties are of particular interest, but also the relationship between the interval modalities. Because of isotony and disjunctivity or conjectivity we conjecture the existence of Galois connections which have to fulfil these properties. In the sequel we present two Galois connections.

Lemma 4.2.5
$\diamondminus$ and $\diamondplus$ are the lower adjoints and $\boxplus$ and $\boxminus$ are the upper adjoints of Galois connections. More precisely:

$$\diamondminus a \le b \Leftrightarrow a \le \boxplus b \qquad \diamondplus a \le b \Leftrightarrow a \le \boxminus b.$$

Proof:

(i)

$$\begin{array}{ll}
 & \diamondminus a \leq b \\
\Leftrightarrow & \overline{\top \rfloor a \lfloor \top} \leq b \\
\Leftrightarrow & \overline{\top \backslash \overline{a} / \top} \leq b \\
\Leftrightarrow & \overline{b} \leq \top \backslash \overline{a} / \top \\
\Leftrightarrow & \top \cdot \overline{b} \cdot \top \leq \overline{a} \\
\Leftrightarrow & \diamondplus \overline{b} \leq \overline{a} \\
\Leftrightarrow & a \leq \overline{\diamondplus \overline{b}} \\
\Leftrightarrow & a \leq \boxplus b
\end{array}$$

(ii)

$$\begin{array}{ll}
 & \diamondplus a \leq b \\
\Leftrightarrow & \top \cdot a \cdot \top \leq b \\
\Leftrightarrow & a \leq \top \backslash b / \top \\
\Leftrightarrow & a \leq \boxminus b
\end{array}$$

□

Two immediate consequences of these Galois connections are formulated in the following lemma.

Lemma 4.2.6

(i) $a \leq \overline{\diamondplus b} \Leftrightarrow \diamondminus a \leq \overline{b}$

(ii) $\overline{\boxplus b} \leq a \Leftrightarrow \overline{b} \leq \boxminus a$

Proof:

$$\begin{array}{ll}
 & a \leq \overline{\diamondplus b} \\
\Leftrightarrow & \quad \{\text{negation}\} \\
 & \diamondplus b \leq \overline{a} \\
\Leftrightarrow & \quad \{\text{Galois connection (4.2.5)}\} \\
 & b \leq \boxminus \overline{a} \\
\Leftrightarrow & \quad \{\text{definition of } \boxminus a\} \\
 & b \leq \overline{\diamondminus \overline{\overline{a}}} \\
\Leftrightarrow & \quad \{\text{negation}\} \\
 & \diamondminus a \leq \overline{b}
\end{array}$$

□

After the presentation of the relationship between the positive and negative interval modalities, we give a possibility to estimate these operators. One possibility is given by the cancellative laws of Galois connections. All together we show the following

Lemma 4.2.7 (Kernel and Hull)

(i) $\boxplus a \leq a \leq \diamondplus a$

(ii) $\boxminus a \leq a \leq \diamondminus a$

(iii) $\diamondplus \boxminus a \leq a \leq \boxminus \diamondplus a$ (cancellative law)

(iv) $\diamondminus \boxplus a \leq a \leq \boxplus \diamondminus a$ (cancellative law)

Proof:

(i)

$$\begin{array}{ll}
 & a \leq \diamondplus a \\
\Leftrightarrow & \quad \{\text{definition of } \diamondplus\} \\
 & a \leq \top \cdot a \cdot \top \\
\Leftarrow & \quad \{\text{isotony w.r.t. multiplication}\} \\
 & \texttt{true}
\end{array}$$

$$\begin{array}{ll}
 & \boxplus a \leq a \\
\Leftrightarrow & \quad \{\text{definition of } \boxplus\} \\
 & \overline{\diamondplus \overline{a}} \leq a \\
\Leftrightarrow & \quad \{\text{negation}\} \\
 & \overline{a} \leq \diamondplus \overline{a} \\
\Leftrightarrow & \quad \{\text{first part}\} \\
 & \texttt{true}
\end{array}$$

(ii) Since $x \lfloor 1 = x = 1 \rfloor x$, we calculate:

$$\begin{array}{ll}
 & 1 \leq \top \\
\overset{3.2.8}{\Rightarrow} & a \lfloor 1 \leq a \lfloor \top \\
\overset{3.2.8}{\Rightarrow} & 1 \rfloor a \lfloor 1 \leq \top \rfloor a \lfloor \top \\
\Leftrightarrow & a \leq \diamondminus a
\end{array}$$

$$\begin{array}{ll}
 & \boxminus a \leq a \\
\Leftrightarrow & \quad \{\text{definition of } \boxminus\} \\
 & \overline{\diamondminus \overline{a}} \leq a \\
\Leftrightarrow & \quad \{\text{negation}\} \\
 & \overline{a} \leq \diamondminus \overline{a} \\
\Leftrightarrow & \quad \{\text{first part}\} \\
 & \texttt{true}
\end{array}$$

(iii)

$$\begin{array}{ll}
 & \diamondplus \boxminus a \leq a \\
\overset{4.2.5}{\Leftrightarrow} & \boxminus a \leq \boxminus a \\
\Leftrightarrow & \texttt{true}
\end{array}$$

$$\begin{array}{ll}
 & a \leq \boxminus \diamondplus a \\
\overset{4.2.5}{\Leftrightarrow} & \diamondplus a \leq \diamondplus a \\
\Leftrightarrow & \texttt{true}
\end{array}$$

(iv) Similar to (iii).

□

At the end of this chapter about interval modalities and their properties we show a further property of $\diamondplus$, which is simple and normally nonrelevant. But we will need it for the proof of the engineer's induction.

Lemma 4.2.8

(i) $x \cdot (\diamondplus a) \leq \diamondplus a$

(ii) $(\diamondplus a) \cdot y \leq \diamondplus a$

(iii) $x \cdot (\diamondplus a) \cdot y \leq \diamondplus a$

Proof:

(i)

$$\begin{aligned} x \cdot (\diamondplus a) &= x \cdot (\top \cdot a \cdot \top) \\ &\leq \top \cdot \top \cdot a \cdot \top \\ &= \top \cdot a \cdot \top \\ &= \diamondplus a \end{aligned}$$

(ii) Similar to (i).

(iii) Immediate from (i) and (ii).

□

Chapter 5

Engineer's Induction

Most of robots and machines in industry perform repetitive tasks. For the proof of correctness of those iterative programs, one starts normally with the first few iterations and then one hopes that this implies the total correctness. But this implication cannot be used without loss of generality. A famous counterexample for such a phenomenon is the mathematical equation $2^n \geq n^2$. For the natural numbers $n = 0, 1, 2$ the equation is correct. But, if we replace n by 3, we get $8 \geq 9$ which is obviously false. Therefore we show in the sequel one possible case where we can guarantee the correctness of the implication mentioned above. This case is based on Kleene algebra because we can use our knowledge about the least fixed point a^*.

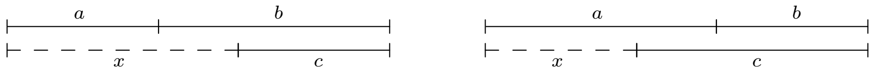
5.1 Local Linearity

For the desired induction, we make use of local linearity, which is a sufficient condition for the Kleene algebras involved. In the literature there are many different definitions of local linearity. Here we use the notion of von Karger [Kar00].

Definition 5.1.1 (Local Linearity)
A detachment semiring S is called *locally linear* iff all $a, b, c \in S$ satisfy the following equations.

$$\begin{array}{rcl} (a \cdot b)\lfloor c &=& a \cdot (b \lfloor c) + a \lfloor (c \lfloor b), \\ c \rfloor (b \cdot a) &=& (c \rfloor b) \cdot a + (b \rfloor c) \rfloor a). \end{array}$$

The first law describes the case analysis that appears when c is cut off $a \cdot b$ from the right. We distinguish two different cases – c is a postfix of b or b is a postfix of c. We illustrate this behaviour in the following figure.



The second law describes the analogous behaviour when c is cut off the left. An example of a locally linear semiring is the semiring of the binary relations REL. It is defined as $\mathrm{REL}(\mathcal{M}) = (\mathcal{P}(\mathcal{M} \times \mathcal{M}), \cup, ;, \emptyset, Id)$ over an arbitrary set $\mathcal{M}$, where multiplication is defined partial and elementwise.

$$\begin{array}{rcl} (\mathcal{M} \times \mathcal{M}) \times (\mathcal{M} \times \mathcal{M}) & \rightarrow & \mathcal{M} \times \mathcal{M} \\ (a, b); (c, d) & \mapsto & \left\{ \begin{array}{l} (a, d), \text{ if } b = c \\ \text{undefined otherwise.} \end{array} \right. \end{array}$$

Id forms the multiplicative neutral element and is characterised by $Id = \{(a, a) : a \in \mathcal{M}\}$. The negation is the ordinary complement of set theory, i.e., $x \in M \Leftrightarrow x \notin \overline{M}$. Furthermore the detachments can be calculated in REL as:

$$\begin{aligned} A\lfloor B &= A;B^{\smile}, \\ A\rfloor B &= A^{\smile};B, \end{aligned}$$

where $A, B \in \mathcal{P}(\mathcal{M}\times\mathcal{M})$ and $A^{\smile} := \{(b,a) \,:\, (a,b) \in A\}$ is the converse relation. Now we can prove local linearity of REL by calculating the three terms of the local linearity equation.

$$\begin{aligned} (A;B)\lfloor C &= A;B;C^{\smile}, \\ A;(B\lfloor C) &= A;B;C^{\smile}, \\ A\lfloor(C\lfloor B) &= A;(C\lfloor B)^{\smile} \\ &= A;(C;B^{\smile})^{\smile} \\ &= A;(B^{\smile\smile};C^{\smile}) \\ &= A;B;C^{\smile} \end{aligned}$$

5.2 Engineer's Induction

We present the engineer's induction as a rule for estimating the least fixed point a^* by the interval modalities of chapter 4. For this estimation we only use a relation between the modalities and the elements 1, a and a^2. This inductive law holds provided the underlying Kleene algebra is locally linear.

Theorem 5.2.1 (Engineer's Induction)
Let $\mathcal{K}$ be a locally linear detachment Kleene algebra and let $b \leq \overline{\diamondplus a}$, then

$$1 + a + a\cdot a \leq \overline{\diamondplus b} \;\Rightarrow\; a^* \leq \overline{\diamondplus b}.$$

Note
The reverse implication $a^* \leq \overline{\diamondplus b} \Rightarrow 1 + a + a\cdot a \leq \overline{\diamondplus b}$ is valid without any condition and follows immediately from $a^n \leq a^*\ \forall n \in \mathbb{N}$.

Before proving the engineer's induction we will have a look at the term $\overline{\diamondplus a}$. We present the meaning in LAN(Σ) over an alphabet Σ and REL(M) over a set M.

(a) $\underline{\text{LAN}(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, \text{++}, \emptyset, \varepsilon)}$
As we showed in section 3.1 $\diamondplus a$, $a \in \mathcal{P}(\Sigma^*)$, describes the set of all words having a part (sub-word) which is in a. Thus $\overline{\diamondplus a}$ contains all words which have no sub-word in a. From the mathematical point of view we get:

$$x \in \overline{\diamondplus a} \Leftrightarrow \forall y \in \Sigma^* \,:\, \exists u_1, u_2 \in \Sigma^*, x = u_1\text{++}y\text{++}u_2 \Rightarrow y \notin a.$$

To use the engineer's induction, we first have to show that LAN(Σ) satisfies the equalities of local linearity. To prove this, we look at single words of LAN(Σ). In Chapter 3 we have demonstrated the behaviour of the detachments in LAN(Σ). So, assuming words a, b and c with $a \in A$, $b \in B$, $c \in C$ and A, B, $C \in \mathcal{P}(\Sigma^*)$, we calculate the three inequalities which then imply the local linearity of LAN(Σ)

(i) First we show $(A\text{++}B)\lfloor C \subseteq A\text{++}(B\lfloor C) \cup A\lfloor(C\lfloor B)$

- Let c be a postfix of b, i.e., $\exists c_1 \in \Sigma^* \,:\, b = c_1\text{++}c$
$$\begin{aligned} (a\text{++}b)\lfloor c &= (a\text{++}c_1\text{++}c)\lfloor c \\ &= a\text{++}c_1 \\ &= a\text{++}((c_1\text{++}c)\lfloor c) \\ &= a\text{++}(b\lfloor c) \end{aligned}$$

- Let b be a postfix of c, i.e., $\exists b_1 \in \Sigma^* : c = b_1{+}{+}b$
  $$\begin{aligned}(a{+}{+}b)\lfloor c &= (a{+}{+}b)\lfloor(b_1{+}{+}b)\\ &= a\lfloor b_1\\ &= a\lfloor((b_1{+}{+}b)\lfloor b)\\ &= a\lfloor(c\lfloor b)\end{aligned}$$
- Consider now the situation where b is no postfix of c and c is no postfix of b
  $(a{+}{+}b)\lfloor c = \{\}$

(ii) Second we show $A{+}{+}(B\lfloor C) \subseteq (A{+}{+}B)\lfloor C$

- Let c be a postfix of b, i.e., $\exists c_1 \in \Sigma^* : b = c_1{+}{+}c$
  $a{+}{+}(b\lfloor c) \overset{(i)}{=} (a{+}{+}b)\lfloor c$
- Let c not be a postfix of b
  $a{+}{+}(b\lfloor c) = \{\}$

(iii) Last we have to show $A\lfloor(C\lfloor B) \subseteq (A{+}{+}B)\lfloor C$

- Let b be a postfix of c
  $a\lfloor(c\lfloor b) \overset{(i)}{=} (a{+}{+}b)\lfloor c$
- Let b be no postfix of c
  $a\lfloor(c\lfloor b) = \{\}$

Summarising these inequalities we get local linearity:

$$\forall A, B, C \subseteq \Sigma^* : (A{+}{+}B)\lfloor C = A{+}{+}(B\lfloor C) \cup A\lfloor(C\lfloor B)$$

Because LAN(Σ) forms also a residuated Boolean Kleene algebra, we can use the engineer's induction. In the case of the formal language, the engineer's induction can be interpreted not only as an induction rule, but also as a relation of sub-words. The assumption $b \le \overline{\diamondplus a}$ says that there are no elements of b which are parts of elements in a. $\varepsilon \cup a \cup a{+}{+}a \le \overline{\diamondplus b}$ describes the situation that neither the empty word ε and elements of a nor elements of $a{+}{+}a$ are not parts of words of b. Using Theorem 5.2.1, we can suggest that there are no words in a^* are sub-words of elements in b.

(b) $\underline{\mathrm{REL}(\mathcal{M}) = (\mathcal{P}(\mathcal{M} \times \mathcal{M}), \cup, ;, \emptyset, Id)}$
First we mention that REL($\mathcal{M}$) can be extended to a Kleene by setting $A^* := \bigcup_{i=0}^{\infty} A^i$ $\forall A \subseteq \mathcal{M} \times \mathcal{M}$. This Kleene algebra is also named REL($\mathcal{M}$). In the semiring and the Kleene algebra of binary relations, respectively, the greatest element is characterised by

$$\top = \{(a, b) : a, b \in \mathcal{M}\} = \mathcal{M} \times \mathcal{M}.$$

Therefore the rule of Tarski holds, i.e., for $A \in \mathcal{P}(\mathcal{M} \times \mathcal{M}) - \{\emptyset\}$ and an element $(a, b) \in A$

$$\diamondplus A = \top; A; \top \ge \top; \{(a, b)\}; \top = \top.$$

By negating the Tarski rule we get

$$\overline{\diamondplus A} = \overline{\top} = \emptyset.$$

For this reason we can only make use of 5.2.1 if $b = \emptyset$ or $a = \emptyset$. For the first case ($b = \emptyset$) the conclusion is trivial because $\overline{\diamondplus b} = \overline{\diamondplus \emptyset} = \overline{\emptyset} = \top$. In the second case, we have $a = \emptyset$ which implies $a^* = Id$ and so the righthand side of the engineer's induction is the same as the assumption.

We summarise the behaviour of the second example by the following note.

Note
Consider $\mathcal{K}$ as a locally linear, residuated Boolean Kleene algebra. If all $x \in \mathcal{K}$, $x \neq 0$, fulfil

$$\diamondplus x = \top,$$

the conditions of the engineer's induction (5.2.1) can only be satisfied if $a = 0$ or $b = 0$. In both cases the conclusion of the induction is trivial.
If we apply the engineer's induction to elements $a \leq 1$ we can show that neither the local linearity nor the property $b \leq \overline{\diamondplus a}$ is needed to prove the equation $1 + a + a \cdot a \leq \overline{\diamondplus b} \Rightarrow a^* \leq \overline{\diamondplus b}$. Since the addition represents join, the supremum $1 + a + a \cdot a$ is equal to 1 and we get the following

Lemma 5.2.2
Assume two elements a, x with $a \leq 1 \leq x$, then $a^* \leq x$.

Proof:

Using the Horn rule ($*$-3), we get:

$$\begin{array}{ll} & a \leq 1 \\ \Leftrightarrow & 1 + a \cdot 1 \leq 1 \\ \overset{(*\text{-}3)}{\Rightarrow} & a^* \leq 1. \end{array}$$

On the other hand we can calculate with ($*$-1) that $1 \leq a^*$.
This implies $a^* = 1$ for all $a \leq 1$ and therefore we get $a^* \leq x$.

□

When setting $x = \overline{\diamondplus b}$ we get a proof of the engineer's induction for elements $a \leq 1$.
For simplifying the general proof of the engineer's induction we first show two properties for a locally linear detachment Kleene algebra $\mathcal{K}$.

Theorem 5.2.3
Assuming that $\top$ is the greatest element in $\mathcal{K}$, we have:

$$1 \lfloor \top + a^* \cdot (a \lfloor \top) = a^* \lfloor \top,$$

$$\top \rfloor 1 + (\top \rfloor a) \cdot a^* = \top \rfloor a^*.$$

Proof:

(i)

$$\begin{array}{ll} & 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \leq & \quad \{\text{local linearity (5.1.1)}\} \\ & 1 \lfloor \top + (a^* \cdot a) \lfloor \top \\ = & \quad \{\text{distributivity of } \lfloor \text{ (3.2.4)}\} \\ & (1 + a^* \cdot a) \lfloor \top \\ = & \quad \{a^* = 1 + a^* \cdot a \ (*\text{-}2)\} \\ & a^* \lfloor \top \end{array}$$

(ii)

$$\begin{array}{ll} & a^* \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{a^* = 1 + a^* \cdot a \ (*\text{-}2)\} \\ & (1 + a^* \cdot a) \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{\text{distributivity of } \lfloor \text{ (3.2.4)}\} \\ & 1 \lfloor \top + (a^* \cdot a) \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{\text{supremum}\} \\ & (a^* \cdot a) \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{\text{definition of fixed points: } .^* \ (x^* = \mu_y : 1 + x \cdot y)\} \\ & ((\mu_y : 1 + a \cdot y) \cdot a) \lfloor \top \leq 1 \lfloor \top + (\mu_y : 1 + a \cdot y) \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{2.2.1\} \\ & (\mu_y : a + a \cdot y) \lfloor \top \leq 1 \lfloor \top + (\mu_y : a \lfloor \top + a \cdot y) \end{array}$$

$$\begin{array}{ll}
\Leftarrow & \quad\{\mu\text{-fusion(2.2.3)}\} \\
 & \forall x : (a + a \cdot x)\lfloor\top \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftrightarrow & \quad\{\text{distributivity of } \lfloor \text{ (3.2.4)}\} \\
 & \forall x : a\lfloor\top + (a \cdot x)\lfloor\top \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftrightarrow & \quad\{\text{supremum}\} \\
 & \forall x : (a \cdot x)\lfloor\top \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftrightarrow & \quad\{\text{local linearity (5.1.1)}\} \\
 & \forall x : a \cdot (x\lfloor\top) + a\lfloor(\top\lfloor x) \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftarrow & \quad\{\text{isotonicity of } +\} \\
 & \forall x : a\lfloor(\top\lfloor x) \leq a\lfloor\top \\
\Leftrightarrow & \quad\{3.2.9\} \\
 & \texttt{true}
\end{array}$$

In the first part of the proof we do not use the local linearity in its completeness. We only take advantage of the inequation of Euclid, i.e., $a^* \cdot (a\lfloor\top) \leq (a^* \cdot a)\lfloor\top$. Therefore the first part is also correct in all algebraic structures which fulfil only this inequation, like sequential algebras with an added Kleene star.

□

Furthermore it is possible to estimate $\diamondminus a^*$ by terms without the star-operator.

Theorem 5.2.4
Let $a \in \mathcal{K}$

$$\begin{array}{rcl}
\diamondminus a^* & = & \diamondminus 1 + \diamondminus a + (\top\rfloor a) \cdot a^* \cdot (a\lfloor\top) \\
 & \leq & \diamondminus(1 + a + a \cdot a) + \diamondplus a
\end{array}$$

<u>Proof:</u>

$$\begin{array}{ll}
 & \diamondminus a^* \\
= & \quad\{\text{definition of } \diamondminus\} \\
 & \top\rfloor(a^*\lfloor\top) \\
= & \quad\{5.2.3\} \\
 & \top\rfloor(1\lfloor\top + a^* \cdot (a\lfloor\top)) \\
= & \quad\{\text{distributivity of } \lfloor \text{ (3.2.4) and definition of } \diamondminus\} \\
 & \diamondminus 1 + \top\rfloor(a^* \cdot (a\lfloor\top)) \\
= & \quad\{\text{local linearity (5.1.1)}\} \\
 & \diamondminus 1 + (a^*\rfloor\top)\rfloor(a\lfloor\top) + (\top\rfloor a^*) \cdot (a\lfloor\top) \\
= & \quad\{3.2.9\} \\
 & \diamondminus 1 + \top\rfloor(a\lfloor\top) + (\top\rfloor a^*) \cdot (a\lfloor\top) \\
= & \quad\{\text{definition of } \diamondminus \text{ and } 5.2.3\} \\
 & \diamondminus 1 + \diamondminus a + (\top\rfloor 1 + (\top\rfloor a) \cdot a^*) \cdot (a\lfloor\top) \\
= & \quad\{\text{distributivity of } \lfloor \text{ (3.2.4)}\} \\
 & \diamondminus 1 + \diamondminus a + (\top\rfloor 1) \cdot (a\lfloor\top) + (\top\rfloor a) \cdot a^* \cdot (a\lfloor\top) \\
= & \quad\{\text{note 5.2.5}\} \\
 & \diamondminus 1 + \diamondminus a + (\top\rfloor a) \cdot a^* \cdot (a\lfloor\top) \\
\leq & \quad\{a^* \leq 1 + \diamondplus a\} \\
 & \diamondminus 1 + \diamondminus a + (\top\rfloor a) \cdot (1 + \diamondplus a) \cdot (a\lfloor\top) \\
= & \quad\{\text{distributivity of } \lfloor \text{ (3.2.4)}\} \\
 & \diamondminus 1 + \diamondminus a + (\top\rfloor a) \cdot (a\lfloor\top) + (\top\rfloor a) \cdot \diamondplus a \cdot (a\lfloor\top)
\end{array}$$

$$\begin{array}{ll}
\leq & \{4.2.8\} \\
 & \diamondminus 1 + \diamondminus a + (\top\rfloor a)\cdot(a\lfloor\top) + \diamondplus a \\
\leq & \{\text{local linearity (5.1.1)}\} \\
 & \diamondminus 1 + \diamondminus a + \top\rfloor(a\cdot a)\lfloor\top + \diamondplus a \\
= & \{\text{definition of } \diamondminus\} \\
 & \diamondminus 1 + \diamondminus a + \diamondminus(a\cdot a) + \diamondplus a \\
= & \{\text{distributivity of } \diamondminus \text{ (4.2.3)}\} \\
 & \diamondminus(1 + a + a\cdot a) + \diamondplus a
\end{array}$$

□

Note 5.2.5

$$\begin{array}{ll}
 & (\top\rfloor 1)\cdot(a\lfloor\top) \\
\leq & \{\text{local linearity (5.1.1)}\} \\
 & \top\rfloor(1\cdot(a\lfloor\top)) \\
= & \{\text{1 is neutral element}\} \\
 & \top\rfloor(a\lfloor\top) \\
= & \{\text{definition of } \diamondminus\} \\
 & \diamondminus a
\end{array}$$

$$\Rightarrow \quad \diamondminus a + (\top\rfloor 1)\cdot(a\lfloor\top) = \diamondminus a$$

With the help of these two theorems, we now prove the engineer's induction.
Proof of 5.2.1 (Engineer's Induction):

$$\begin{array}{ll}
 & 1 + a + a\cdot a \leq \overline{\diamondplus b} \text{ and } b \leq \overline{\diamondplus a} \\
\Leftrightarrow & \{\text{4.2.6 and negation}\} \\
 & \diamondminus(1 + a + a\cdot a) \leq \bar{b} \text{ and } \diamondplus a \leq \bar{b} \\
\Leftrightarrow & \{\text{supremum}\} \\
 & \diamondminus(1 + a + a\cdot a) + \diamondplus a \leq \bar{b} \\
\Rightarrow & \{5.2.4\} \\
 & \diamondminus a^* \leq \bar{b} \\
\Leftrightarrow & \{4.2.6\} \\
 & a^* \leq \overline{\diamondplus b}
\end{array}$$

□

Chapter 6

Duration Calculus

The duration calculus provides a method for developing a specific design for a system and to prove its correctness if safety requirements for this system are known. For this goal we make use of the engineer's induction from the last chapter. Therefore the basis for developing and formulating the requirements and a design has to be a locally linear Kleene algebra. Before formulating the duration calculus we give some definitions and properties for measure sets.

6.1 Measures and Measure Sets

To formulate safety requirements for an arbitrary system, we have to add some measure functions to the underlying Kleene algebra. E.g., it should be possible to calculate the duration of an element. In the sequel we show a possibility for characterising such functions. Furthermore we show how to collect elements with the same properties concerning the given functions in so-called measure sets.

Definition 6.1.1
Consider X, Σ as arbitrary sets and $f : X \to \Sigma$ as a function. The *set of measure* σ *under* f is defined by

$$M^f_{=\sigma} := \{x : x \in X, f(x) = \sigma\}, \quad \sigma \in \Sigma.$$

We call f a *measure function.* In an arbitrary semiring over a set X $M^f_{=\sigma}$ is a special element which contains all elements of X having the same value of f.
Note
Let X, Σ, f the same as in definition 6.1.1. If f is totally defined, then the relation

$$a \sim b \;:\Leftrightarrow\; f(a) = f(b)$$

is an equivalence relation where $M^f_{=\sigma}$, $\sigma \in \Sigma$, form the equivalence classes.

Definition 6.1.2
Let $(\Sigma, \leq)$ be a poset, X a set and $f : X \to \Sigma$. We define for an element $\sigma \in \Sigma$ more sets of measure σ under f.

$$\begin{array}{rcl} M^f_{\leq\sigma} &:=& \{x : x \in X, f(x) \leq \sigma\}, \\ M^f_{<\sigma} &:=& \{x : x \in X, f(x) < \sigma\} = M^f_{\leq\sigma} \cap \overline{M^f_{=\sigma}}, \\ M^f_{\geq\sigma} &:=& \{x : x \in X, f(x) \geq \sigma\}, \\ M^f_{>\sigma} &:=& \{x : x \in X, f(x) > \sigma\} = M^f_{\geq\sigma} \cap \overline{M^f_{=\sigma}}. \end{array}$$

With these definitions we get an obvious relationship between these measure sets.

$$\begin{aligned}
M^f_{<\sigma} &\subseteq M^f_{\leq\sigma}, \\
M^f_{=\sigma} &\subseteq M^f_{\leq\sigma}, \\
M^f_{>\sigma} &\subseteq M^f_{\geq\sigma}, \\
M^f_{=\sigma} &\subseteq M^f_{\geq\sigma}, \\
M^f_{=\sigma} &= M^f_{\leq\sigma} \cap M^f_{\geq\sigma}.
\end{aligned}$$

Since all measure sets under a function f are elements of the semiring $(\mathcal{P}(X), \cup, \cdot, \emptyset, 1)$ over X we can use addition and multiplication of the semiring to combine the sets $M^f_{=\sigma}, M^f_{\leq\sigma}$, $M^f_{<\sigma}$, $M^f_{\geq\sigma}$ and $M^f_{>\sigma}$.

Example 6 (Semirings of Time)
For verifying the correctness of a system we have to observe the system along a 'time-line'. To simulate this behaviour with the help of algebraic methods we present two semirings of time. We assume time to be a linear, one-dimensional space. This is the 'normal' description of time in most of (technical) applications. The set of time can be interpreted in geometry as a (semi) straight line and in numerical calculations as sets of numbers like $\mathbb{N}$, $\mathbb{R}$, $\mathbb{R}^+$, ...
In the sequel we restrict ourselves to $\mathbb{R}$ and $\mathbb{R}^+$, respectively. If we want to use subsets of $\mathbb{R}$ like $\mathbb{N}$ it is also possible without any changes in the following calculations.
In the case that we observe our system for some time, we describe the observation period as an interval of real numbers if the observation time is connected, that means we have no break in the observation. For this reason we construct semirings over sets of intervals consisting of real numbers. We define

$$\begin{aligned}
\texttt{Int} &:= \{[a,b] : a \leq b,\, a,b \in \mathbb{R}_\infty = \mathbb{R} \cup \{\infty\}\}, \\
\texttt{Int}_0 &:= \{[a,b] : [a,b] \in \texttt{Int},\, a \geq 0\}.
\end{aligned}$$

In most of applications we set 0 as the point in time which is 'now'; positive numbers are points in time which we will reach in the future and negative numbers stand for points that we have already passed.
The intervals $[a,\infty] := [a,\infty)$ are intervals where the observation starts at a point a and never ends (ends at the point infinity). To construct semirings over $\texttt{Int}$ and $\texttt{Int}_0$ we have to define a multiplication for these sets. We use interval composition which is defined on $\texttt{Int}$ as

$$\begin{aligned}
;: \texttt{Int} \times \texttt{Int} &\rightarrow \texttt{Int} \\
[a,b];[c,d] &= \begin{cases} [a,d] \text{ if } b = c \\ \text{undefined otherwise.} \end{cases}
\end{aligned}$$

The concatenation of $\texttt{Int}_0$ is only a restriction of the one of $\texttt{Int}$, because $\texttt{Int}_0$ is a proper subset of $\texttt{Int}$. Due to this we will only have a look at the set of intervals $\texttt{Int}$ in the sequel. The results for $\texttt{Int}_0$ are similar. Using ; as multiplication and $\cup$ as addition we get two semirings over $\texttt{Int}$ and $\texttt{Int}_0$ which we call *semirings of time*

$$\begin{aligned}
\mathcal{H}_{\texttt{Int}} &:= (\mathcal{P}(\texttt{Int}), \cup, ;, \emptyset, 1_{\texttt{Int}}), \\
\mathcal{H}_{\texttt{Int}_0} &:= (\mathcal{P}(\texttt{Int}_0), \cup, ;, \emptyset, 1_{\texttt{Int}_0}).
\end{aligned}$$

The multiplicative neutral element is given by $1_{\texttt{Int}} = \{[a,a] : a \in \mathbb{R}_\infty\}$ and $1_{\texttt{Int}_0} = \{[a,a] : a \in \mathbb{R}_\infty, a \geq 0\}$, respectively. To illustrate the above definitions, we give two explicit examples for functions which define sets of measure.

(i) The first one calculates the length of an interval.

$$\begin{array}{rcl} L:\texttt{Int} & \longrightarrow & \mathbb{R}_\infty \\ {[a,b]} & \longmapsto & \begin{cases} b-a & \text{if } a,b\in\mathbb{R},\\ \infty & \text{if } a\in\mathbb{R}, b=\infty,\\ 0 & \text{if } a=b=\infty.\end{cases}\end{array}$$

As an example $M^L_{=30}$ describes the the set of all intervals of lengths 30.

(ii) The second example shows the so-called χ-function. For this purpose let $N \subseteq \mathbb{R}_\infty$ and let χ_N be Lebesgue integrable.

$$\begin{array}{rcl} \chi_N:\mathbb{R} & \longrightarrow & \{0,1\} \\ x & \longmapsto & \chi_N(x) = \begin{cases} 1 & \text{if } x\in N\\ 0 & \text{if } x\notin N,\end{cases} \\ F:\texttt{Int} & \longrightarrow & \mathbb{R}_\infty \\ {[a,b]} & \longmapsto & \displaystyle\int_a^b \chi_N(t)\,dt,\end{array}$$

where $\int$ is the Lebesgue integral. $M^F_{<4}$ is the set of all those intervals $[a,b]$ which have at most a Lebesgue measure of 4, i.e., $\int_a^b \chi_N(t)\,dt < 4$.

To reduce the number of indices we left the upper index which describes the function appropriating the measure sets when it is possible without losing the uniqueness. Furthermore we assume sets X, Σ where we can define a multiplication on X and use $\mathcal{H}_X$ as the corresponding semiring over X and a function $f : X \to \Sigma$. In the sequel we present lots of properties of sets of measure σ under f, where $\sigma \in \Sigma$.

Theorem 6.1.3
Let $(\Sigma, +, 0_\sigma)$ be a partial monoid and $(\Sigma, \leq)$ a poset. Furthermore let $f : X \to \Sigma$ be a homomorphism, i.e., $f(a \cdot b) = f(a) + f(b)\ \forall a, b \in X$ iff $a \cdot b$ is defined. Then for $x, y \in \Sigma$ we have:

(i) If f is surjective, then $1 \in M_{=0_\sigma}$.

(ii) $M_{=x} \cdot M_{=y} \subseteq M_{=(x+y)}$.

(iii) If $+$ is left and right isotone, i.e., $a \leq b \Rightarrow a+c \leq b+c$ and $a \leq b \Rightarrow c+a \leq c+b$, $\forall a, b, c \in \Sigma$, then we get

$$M_{op\,x} \cdot M_{op\,y} \subseteq M_{op\,(x+y)}$$

where $op \in \{\leq, <, \geq, >\}$ is an arbitrary logical operator.

Proof:

(i) Let $a \in X$.

$$\begin{array}{rl} & f(a) = f(1\cdot a) = f(1) + f(a) \\ \Rightarrow & f(1) = 0_\sigma \text{ if } f \text{ is surjective.} \\ \Rightarrow & 1 \in M_{=0_\sigma} = \{x \,:\, x\in X, f(x) = 0_\sigma\}\end{array}$$

(ii)

$$\begin{array}{rcl} M_{=x}\cdot M_{=y} & = & \{a\cdot b \,:\, a\in M_{=x}, b\in M_{=y}\} \\ & = & \{a\cdot b \,:\, a,b\in X, f(a)=x, f(b)=y\} \\ & \subseteq & \{a\cdot b \,:\, a,b\in X, f(a)+f(b)=x+y\} \\ & = & \{a\cdot b \,:\, a,b\in X, f(a\cdot b)=x+y\} \\ & \subseteq & \{c \,:\, c\in X, f(c)=x+y\} \\ & = & M_{=(x+y)}\end{array}$$

(iii)

$$\begin{array}{rcl} M_{\leq x} \cdot M_{\leq y} & = & \{a \cdot b \,:\, a \in M_{\leq x}, b \in M_{\leq y}\} \\ & = & \{a \cdot b \,:\, a, b \in X, f(a) \leq x, f(b) \leq y\} \\ & \subseteq & \{a \cdot b \,:\, a, b \in X, f(a) + f(b) \leq x + y\} \\ & = & \{a \cdot b \,:\, a, b \in X, f(a \cdot b) \leq x + y\} \\ & \subseteq & \{c \,:\, c \in X, f(c) \leq x + y\} \\ & = & M_{\leq (x+y)} \end{array}$$

For all the other logical operators the proof is similar.

□

Definition 6.1.4
Consider measure sets under two different functions $f, g : X \to \Sigma$ and assume two logical operators $op, \widetilde{op} \in \{=, \leq, <, \geq, >\}$. We define a *measure set under* f *and* g in a natural way.

$$M^f_{op\,x} \cap M^g_{\widetilde{op}\,x} := \{a \,:\, a \in X, f(a)\, op\, x, g(a)\, \widetilde{op}\, y\} \in \mathcal{P}(X)$$

Obviously we have the following subset relation:

$$\begin{array}{rcl} M^f_{op\,x} \cap M^g_{\widetilde{op}\,x} & \subseteq & M^f_{op\,x}, \\ M^f_{op\,x} \cap M^g_{\widetilde{op}\,x} & \subseteq & M^g_{\widetilde{op}\,x}. \end{array}$$

Example 7
Using the functions $L, F : \texttt{Int} \to \mathbb{R}_\infty$ of Example 6 we formulate the set of all intervals which have at most a Lebesgue integral of 4 w.r.t. χ_N and a length not longer than 60 seconds as

$$M^L_{\leq 60} \cap M^F_{>4} = \{[a, b] \,:\, [a, b] \in \texttt{Int}, L([a, b]) \leq 60, F([a, b]) > 4\}$$

Lemma 6.1.5
For a poset $(\Sigma, \leq)$, we have:

$$\begin{array}{rcl} M_{\leq x} \subseteq M_{\leq y} & \Leftarrow & x \leq y, \\ M_{< x} \subseteq M_{< y} & \Leftarrow & x \leq y, \\ M_{\geq x} \subseteq M_{\geq y} & \Leftarrow & y \leq x, \\ M_{> x} \subseteq M_{> y} & \Leftarrow & y \leq x. \end{array}$$

Proof:

$$\begin{array}{rl} & M_{\leq x} \subseteq M_{\leq y} \\ \Leftrightarrow & \{a : a \in X, f(a) \leq x\} \subseteq \{a : a \in X, f(a) \leq y\} \\ \Leftarrow & x \leq y \end{array}$$

□

Lemma 6.1.6
If $(\Sigma, \leq)$ is a totally ordered set, i.e., $\forall x, y \in \Sigma : x \leq y \vee y \leq x$, we can show some relationships for complementation.

$$\begin{array}{rcl} \overline{M_{\leq x}} & = & M_{> x}, \\ \overline{M_{\geq x}} & = & M_{< x}. \end{array}$$

Proof:

$$\begin{aligned}
\overline{M_{\leq x}} &= \overline{\{a : a \in X, f(a) \leq x\}} \\
&= \{a : a \in X, f(a) \not\leq x\} \\
&= \{a : a \in X, f(a) > x\} \\
&= M_{>x}
\end{aligned}$$

The second equation can be shown similarly.

□

Lemma 6.1.7
Consider a poset $(\Sigma, \leq)$ with the least element $\perp$, then

$$M_{\geq \perp} = X.$$

Therefore $M_{\geq \perp}$ is the greatest element in $\mathcal{P}(X)$ with respect to the subset relation. In particular $M_{\geq \perp}$ is the greatest element of the semiring H_X

Proof:

Since $\perp$ represents the least element in Σ, we have $f(a) \geq \perp$ for all $a \in X$.

$$\begin{aligned}
M_{\geq \perp} &= \{a : a \in X, f(a) \geq \perp\} \\
&= \{a : a \in X\} \\
&= X
\end{aligned}$$

□

Corollary 6.1.8
If $(\Sigma, \leq)$ has a greatest element $\top$ we can dualise 6.1.7:

$$M_{\leq \top} = X.$$

Corollary 6.1.9
For a homomorphism f and a poset $(\Sigma, \leq)$ with least element 0 the Lemmata 6.1.5 and 6.1.7 immediately imply

$$\begin{aligned}
M_{\geq x} \subseteq M_{\geq y}/X &\quad\Leftarrow\quad y \leq x, \\
M_{\geq x} \subseteq X \backslash M_{\geq y} &\quad\Leftarrow\quad y \leq x
\end{aligned}$$

and also

$$\begin{aligned}
\diamondminus M_{<x} = M_{<x}, &\quad \boxminus M_{\geq x} = M_{\geq x}, \\
\boxplus M_{<x} = M_{<x}, &\quad \diamondplus M_{\geq x} = M_{\geq x}.
\end{aligned}$$

Proof:

(i)

$$\begin{aligned}
& M_{\geq x} \subseteq M_{\geq y}/X \\
\overset{6.1.7}{\Leftrightarrow} \quad & M_{\geq x} \subseteq M_{\geq y}/M_{\geq 0} \\
\Leftrightarrow \quad & M_{\geq x} \cdot M_{\geq 0} \subseteq M_{\geq y} \\
\overset{6.1.3}{\Leftarrow} \quad & M_{\geq x} \subseteq M_{\geq y} \\
\overset{6.1.5}{\Leftarrow} \quad & y \leq x
\end{aligned}$$

(ii)

$$\begin{array}{cl}
 & \diamondminus M_{<x} \\
= & \overline{X\backslash\overline{M_{<x}}/X} \\
\overset{6.1.6}{=} & \overline{X\backslash M_{\geq x}/X} \\
\overset{(i)}{\subseteq} & \overline{M_{\geq x}} \\
\overset{6.1.6}{=} & M_{<x}
\end{array}$$

$$\begin{array}{cl}
 & \boxminus M_{\geq x} \\
= & X\backslash M_{\geq x}/X \\
\overset{(i)}{\supseteq} & M_{\geq x}
\end{array}$$

$$\overset{4.2.7}{\Rightarrow} \qquad \diamondminus M_{<x} = M_{<x}, \quad \boxminus M_{\geq x} = M_{\geq x}$$

$$\overset{4.2.5}{\Rightarrow} \qquad \boxplus M_{<x} = M_{<x}, \quad \diamondplus M_{\geq x} = M_{\geq x}$$

□

Note
Since $\mathbb{R}^+$ has an underlying total order and 0 is the least element in $\mathbb{R}^+$, the given corollary is especially true for all measure sets under $f : X \to \mathbb{R}^+$ as the functions L and F of Example 6.

6.2 The Leaking Gas Burner - Duration Calculus considered as example

Standard examples for usage of duration calculus are the *leaking gas pipe* and the *leaking gas burner*, respectively. Zhou, Hoare and Ravn already used the second one in [CHR91] to introduce the duration calculus. Von Karger describes the leaking gas pipe with the help of observation spaces [Kar00]. In these papers the authors give two possibilities to formulate safety requirements for a fixed specification.

We present an algebraic approach to the duration calculus based on detachment Kleene algebras. The main advantage of an algebraic characterisation is to avoid complicated formulas with many temporal operators like the ∃- and the ∀-operator. This offers the possibility to formulate safety requirements in a short and elegant way. Doing this, we can calculate very easily with the safety specifications and other requirements coming from duration calculus. When calculating the requirements, we use the interval modalities of Chapter 4.

6.2.1 The Problem

First we start with describing the example of the *leaking gas burner*, which was introduced in [SRR89] in the following way:

"A gas burner is either heating when the flame is burning or idling when the flame is not burning. Usually, no gas is flowing while it is idling. However, when changing from idling to heating, gas must be flowing for a short time before it can be ignited, and when a flame failure appears, gas must be flowing before the failure is detected and the gas valve is closed".

Obviously, there can exist some time (intervals) where the flame is not burning but gas is flowing. In that case gas is *leaking*. The same effect we get at valves and at seals of gas pipes. In the literature this effect is modelled by the *leaking gas pipe*.

If too much gas is leaking the gas burner or the gas pipe is a security risk. For this reason we want to construct a system that observes the gas burner and shuts off the supply of gas if too much gas is leaking. Therefore we want to give possible safety requirements for such a system.

First we give a requirement similar to the one of [CHR91].

> “For any observation interval that is longer than 60 seconds the accumulation of leakage has to be less than a 15th of the time.” (Req1)

To see that this requirement is sufficient for modelling an easy and safe design for gas burners we have to discuss the following (wrong) argumentation:
Let us assume an observation interval with a length of 15 hours. Then there can be an hour where gas is leaking without any interrupt and without breaching the safety requirement (Req1). But 60 minutes of leaking gas seems to be dangerous.
The argumentation fails because we have to take all subintervals of the interval of 15 hours into account. If there would be such an interval of 60 minutes length where gas is leaking, this interval does not achieve (Req1) because there are 60 minutes of leaking time instead of the allowed 4 minutes.
To avoid the wrong argumentation von Karger [Kar00] gives another safety requirement of a leaking gas burner. Here he uses intervals with a given maximum length.

> “A gas burner system is safe iff for any observation interval that is shorter than 60 seconds the accumulation of leakage is less than 4 seconds.” (Req2)

Which requirement is better? The one of Zhou et al. (Req1) or the one of von Karger (Req2)? Of course the second one avoids the discussion presented. In the next sections we will derive a mathematical formulation of both safety requirements. Then we point out that (Req1) looks very similar to (Req2) in an algebraic characterisation.

6.2.2 Algebraic Characterisation

Using intervals for safety requirements like (Req1) and (Req2) we formulate these requirements as mathematical formulas by using the semirings of time $\mathtt{Int}$ and $\mathtt{Int}_0$. For this we need two functions of type $\mathtt{Int} \to \mathbb{R}_\infty$. The one which calculates the length of intervals was already defined in Example 6. The other one has to calculate a measure for the leakage of an interval. We choose $N \subseteq \mathbb{R}_\infty$ as the set of time points and time intervals where gas is leaking. Analogously to the function F (Example 6) we define the function $Leak$ as

$$\begin{array}{rcl} Leak : \mathtt{Int} & \to & \mathbb{R} \\ {[a,b]} & \mapsto & \displaystyle\int_a^b \chi_N(t)\,dt, \end{array}$$

where we consider that $\chi_N(t)$ is Lebesgue integrable. All possibilities of N where χ_N becomes non Lebesgue integrable are ‘unnatural’ and constructed functions. Therefore we can restrict ourselves to integrable functions without loss of generality. Having the two functions L and $Leak$ available we can reformulate (Req2):

$$\begin{array}{rl} & \text{The system of the gas burner is safe} \\ \Leftrightarrow & \forall a \in \mathtt{Int} \,:\, L(a) < 60 \Rightarrow Leak(a) \leq 4 \\ \Leftrightarrow & \forall a \in \mathtt{Int} \,:\, L(a) \geq 60 \vee Leak(a) \leq 4 \\ \Leftrightarrow & \forall a \in \mathtt{Int} \,:\, \neg(L(a) < 60 \wedge Leak(a) > 4). \end{array} \qquad \text{(Req)}$$

In the last step we use the law of de Morgan. Similar to this we get for (Req1)

$$\begin{array}{rl} & \forall a \in \mathtt{Int} \,:\, L(a) > 60 \Rightarrow Leak(a) < \frac{1}{15}L(a) \\ \Leftrightarrow & \forall a \in \mathtt{Int} \,:\, \neg(L(a) > 60 \wedge Leak(a) \geq \frac{1}{15}L(a)) \\ \Leftarrow & \forall a \in \mathtt{Int} \,:\, \neg(L(a) > 60 \wedge Leak(a) \geq 4) \end{array} \qquad \text{(Req1')}$$

Now let’s have a closer look at $\boxplus M$ for a (measure) set M in $\mathcal{H}_{\mathtt{Int}}$.

$$x \in \boxplus M \Leftrightarrow x \in \overline{\diamond \overline{M}} \Leftrightarrow x \notin \mathtt{Int} \cdot \overline{M} \cdot \mathtt{Int}.$$

Therefore an interval I is an element of $\boxplus M$ if and only if all subsets of I are elements of M. Using this we can reformulate again the safety requirement (Req) and get an algebraic characterisation of the specification:

$$\mathrm{g}as\_spec \;=\; \boxplus\overline{b}, \quad \text{where } b \;:=\; M^{L}_{<60} \cap M^{Leak}_{>4}.$$

Analogously we get $\mathrm{g}as\_spec' \;=\; \boxplus\overline{c}$, $\quad$ where $c \;:=\; M^{L}_{>60} \cap M^{Leak}_{\geq 4}$ for (Req1') which imply the requirement of Zhou et al. Now we see that both specification have the same algebraic character since we can write them as $\boxplus x$.

6.2.3 Duration Calculus considered as example

To build a safe gas burner one has to construct a concrete design gas_design that fulfils the specification for the safety requirement gas_spec, i.e., $\mathrm{g}as\_design \subseteq \mathrm{g}as\_spec$. In our interpretation of time points and time intervals negative (real) numbers present time points of the past. Since such numbers are of no interest for a design we use $\mathtt{Int}_0$ instead of $\mathtt{Int}$ in the sequel.
We are particularly interested in a design of the gas burner which repeats one concrete routine. After constructing such a system a robot or another machine can take on this work.
To present a possible design with repetition we use Kleene algebras (see Chapter 2). Therefore we extend the semiring $\mathcal{H}_{\mathtt{Int}_0}$ to a Kleene algebra $\mathcal{H}_{\mathtt{Int}_0} = (\mathcal{P}(\mathtt{Int}_0), \cup, ;, \emptyset, 1, ^*)$ by setting

$$\begin{array}{rcl} a^0 & = & 1, \\ a^{i+1} & = & a^i; a, \\ a^* & = & \bigcup\limits_{i \geq 0} a^i, \end{array}$$

where $a \in \mathcal{P}(\mathtt{Int}_0)$. Now we formulate a design of a safe system for controlling a gas burner.

$$\mathrm{g}as\_design = a^*, \quad \text{where } a \;:=\; M^{L}_{=60} \cap M^{Leak}_{<2}.$$

This design is characterised by using only intervals of the same length. Therefore the gas_design is much easier as gas_spec and we would be able to build a robot that does this monotonous work by observing intervals of the length of 60 seconds. To show the correctness and the safety of the design we have to prove the following

Lemma 6.2.1

(i) $\mathrm{g}as\_design \subseteq \mathrm{g}as\_spec.$

(ii) A system, that starts at a time point x, has to run indefinitely, i.e, 'forever' if there is no breach of security. Mathematically that means: $\forall x \in \mathbb{R}_\infty, x \geq 0 \;:\; [x, \infty] \in \lim\limits_{n \to \infty} (M^{L}_{=30})^n$, where $(M^{L}_{=30})^{n+1} = (M^{L}_{=30}); (M^{L}_{=30})^n$.

Proof:

(i) (a) First we show the local linearity of $\mathcal{H}_{\mathtt{Int}_0}$.
Calculating detachments of intervals we get for intervals $[a, b], [c, d] \in \mathtt{Int}_0$

$$[a, b] \lfloor [c, d] \quad = \quad \begin{cases} [a, c] & \text{if } a \leq c \text{ and } b = d, \\ \{\} & \text{otherwise.} \end{cases}$$

We see that detachments in the semirings of time have the same behaviour as detachments of the semiring of formal languages. So the proof for local linearity is similar to the one of $LAN(\Sigma)$ given in chapter 5.

(b) Due to the local linearity of $\mathcal{H}_{\mathtt{Int}_0}$ we can freely use the engineer's induction to show the desired subset relation. So we only have to show

(1) $1 \cup a \cup a; a \subseteq \overline{\diamondplus b} \overset{4.2.6}{\Leftrightarrow} \diamondminus(1 \cup a \cup a; a) \subseteq \overline{b}$

(2) $b \subseteq \overline{\diamondplus a}$,
where $a, b \in \mathcal{P}(\mathtt{Int}_0)$ are given by gas_spec and gas_design.

First we show (1):

$$
\begin{array}{ll}
 & \diamondminus(1 \cup a \cup a; a) \\
= & \quad \{\text{definition of } a\} \\
 & \diamondminus(1 \cup (M^L_{=60} \cap M^{Leak}_{<2}) \\
 & \cup(M^L_{=60} \cap M^{Leak}_{<2}); (M^L_{=30} \cap M^{Leak}_{<2})) \\
\subseteq & \quad \{\text{subset}\} \\
 & \diamondminus(1 \cup M^{Leak}_{<2} \cup M^{Leak}_{<2}; M^{Leak}_{<2}) \\
\subseteq & \quad \{\text{isotonicity, 6.1.3}\} \\
 & \diamondminus(M^{Leak}_{=0} \cup M^{Leak}_{<2} \cup M^{Leak}_{<2}; M^{Leak}_{<2}) \\
\subseteq & \quad \{6.1.3\} \\
 & \diamondminus(M^{Leak}_{=0} \cup M^{Leak}_{<2} \cup M^{Leak}_{<(2+2)}) \\
\subseteq & \quad \{6.1.5\} \\
 & \diamondminus M^{Leak}_{<4} \\
= & \quad \{6.1.9\} \\
 & M^{Leak}_{<4} \\
\subseteq & \quad \{\text{subset}\} \\
 & M^{Leak}_{\leq 4} \\
= & \quad \{\text{complementation (6.1.6)}\} \\
 & \overline{M^{Leak}_{>4}} \\
\subseteq & \quad \{\text{subset}\} \\
 & \overline{M^L_{<60} \cap M^{Leak}_{>4}} \\
= & \quad \{\text{definition of } b\} \\
 & \overline{b}
\end{array}
$$

Now we show (2):

$$
\begin{array}{ll}
 & \diamondplus a \\
= & \quad \{\text{definition of } a\} \\
 & \diamondplus(M^L_{=60} \cap M^{Leak}_{<2}) \\
\subseteq & \quad \{\text{isotonicity}\} \\
 & \diamondplus M^L_{=60} \\
= & \quad \{\text{definition of } \diamondplus\} \\
 & \mathtt{Int}_0; M^L_{=60}; \mathtt{Int}_0 \\
= & \quad \{6.1.7\} \\
 & M^L_{\geq 0}; M^L_{=30}; M^L_{\geq 0} \\
\subseteq & \quad \{6.1.3\} \\
 & M^L_{\geq 60} \\
= & \quad \{\text{negation (6.1.6)}\} \\
 & \overline{M^L_{<60}} \\
\subseteq & \quad \{\text{subset}\} \\
 & \overline{M^L_{<60} \cap M^{Leak}_{>4}} \\
= & \quad \{\text{definition of } b\} \\
 & \overline{b}
\end{array}
$$

(ii) $\forall x \in \mathbb{R}_\infty$ where $x \geq 0$ we calculate

$$
\begin{array}{lcl}
[x, \infty] & = & [x, x+60]; [x+60, \infty] \\
 & = & [x, x+60]; [x+60, x+120]; [x+120, \infty] \\
 & = & \ldots
\end{array}
$$

This equation implies that $[x, \infty]$ can be split into a product by

$$\forall x \in \mathbb{R}_\infty, x \geq 0 \,:\, [x, \infty] = \prod_{i \in \{k \cdot 60 \,:\, k \in \mathbb{N}_\infty\}} [x+i, x+i+60]$$

Since all intervals have the form $[x+i, x+i+60] \in M^L_{=60}$ and length $L([x+i, x+i+60]) = 60$, we have

$$[x, \infty] \in \lim_{n\to\infty} (M^L_{=60})^n \quad \forall x \in \mathbb{R}_\infty, x \geq 0.$$

□

6.3 Duration Calculus in General

Now we present a generalisation of the correctness-calculations of the previous section.

Theorem 6.3.1 (Duration Calculus)
Assume a locally linear detachment Kleene algebra $\mathcal{H}_X = (\mathcal{P}(X), \cup, \cdot, 0, 1, ^*)$ over a set X, a totally ordered set $(\Sigma_1, \leq)$ and a monoid $(\Sigma_2, +, 0)$ with least element 0. Then for $a := M^{f_1}_{=x} \cap M^{f_2}_{<y} \cap A_j$ and $b := M^{f_1}_{<x} \cap M^{f_2}_{>(y+y)} \cap B_k$ we have

$$a^* \leq \overline{\diamondplus b} = \boxplus \overline{b},$$

where $f_i : X \to \Sigma_i$, $i = 1, 2$, are homomorphisms, f_2 is surjective and $A_j, B_k \subseteq X$, $j \in J$, $k \in K$ are arbitrary.

Proof:

> The proof is similar to the one of 6.2.1. We emphasise that the sets A_j and B_k can be chosen freely. E.g., we can take more measure sets to formulate more complicated safety requirements or we use A_j and B_k to restrict ourselves to some special intervals.

□

6.4 Further Applications

In this chapter we showed how to use duration calculus for the gas burner example. But there are many other applications besides the leaking gas. To conclude the chapter we give two other applications for duration calculus.

(i) Similarly to the gas burner we can formulate safety requirements for elevators and railroad crossings. E.g., a gate should be closed at least 60 seconds before a train arrives at the crossing.
A possible safety requirement for elevators is:

> 'Persons waiting for the elevator need not to wait over 5 minutes.'

(ii) The second example uses the Kleene algebra of paths $PAT(V) = (\mathcal{P}(V^*), \cup, \bowtie, \emptyset, V^{\leq 1}, ^{\leadsto})$ (see section 2.2). Consider that the paths of length 2 are weighted, i.e., there is a function $w : V^2 \to \mathbb{N}$. In other words, the edges of the underlying graph are weighted. Using the set of edges (paths of length 2) we define two functions like L and F of section 6.1.

$$\begin{array}{rcl} l : E & \to & \mathbb{N} \\ \varepsilon & \mapsto & 0 \\ ut & \mapsto & 1 + l(t) \\ & & \end{array} \qquad \begin{array}{rcl} weight : E & \to & \mathbb{N} \\ \varepsilon & \mapsto & 0 \\ u & \mapsto & 0 \\ uvt & \mapsto & w(uv) + weight(vt), \end{array}$$

where $u, v \in V$ and $t \in V^*$.
Here l gives the length of paths and *weight* calculates for any path its specific weight as the sum of the weight of the used edges. (In the example we assume that there is at most one edge between two vertices.)

Using the functions l and $weight$ we can now use the duration calculus. $\overline{\diamondplus P}$ descibes the set of all paths having no subpaths in P. Using measure sets we can formulate statements about sets of paths with a specific lengths and weight. For example starting with all paths of length x and weight smaller than y $(M^{l}_{=x} \cap M^{weight}_{<y})$ we can calculate an upper bound for a^* with the help of duration calculus. In particular we get that a^* does not contain paths having a length smaller than x and a weight greater than $2y$. Such formulation could be of interest in calculating graph algorithms.

Chapter 7

Conclusion and Outlook

In this report we presented a variation of duration calculus using Kleene algebras. For developing DC we first defined and analysed additional operators for semirings. In detail we presented residuals and detachments. Then we defined interval modalities with their help. Interval modalities are already used for example by von Karger [Kar01]. After the definition we specified many properties for interval modalities.

Afterwards we showed that the engineer's induction for sequential algebras [Kar00] can be used for detachment Kleene algebras, too. The engineer's induction provides the opportunity to estimate the least fixed point a^* by $1 + a + a^2$. Thus we avoid the explicit calculation of the fixed point that is in many cases complicated or completely impossible. Another advantage of the engineer's induction is obtained by using set-based semirings. Here the cardinal number of the fixed point A^* is normally much greater than the cardinal numbers of A and A^2. So we are able to calculate with smaller sets.

Before showing duration calculus we gave definitions for measure sets and semirings of time. That allowed us to formulate quantitative requirements like 'for all intervals longer than' by usage of measure functions. Furthermore we gave a possibility to embed 'time' into semirings and defined Kleene algebras with the aid of these definitions. As the final result we specified safety requirements for a leaking gas burner [CHR91] and re-formulated them by algebraic formulas using interval modalities. To prove the correctness of the given gas burner design we used detachments, Kleene algebras and duration calculus. At last we presented further applications for the usage of duration calculus.

At present we have proven the engineer's induction only for detachment Kleene algebras that are locally linear. Hence we want to know if one can generalise the inductive law to Kleene algebra that are not locally linear. Until now, we have not found a proof or a counterexample for a Kleene algebra which does not fulfils the engineer's induction. By searching such a counter example we checked most of all known Kleene algebras. Even the 'exotic' ones like the semiring of polygons [IS90] were checked.

If we could prove the engineer's induction in general, the duration calculus would work for all detachment Kleene algebras, too, since we use local linearity in the proof only when using the engineer's induction.

Acknowledgement

I am very greatful to B. Möller for many fruitful discussions, suggestions and comments.

Appendix A

Residuated Kleene Algebras

The calculations can also be found in [Jip02].

Theorem A.1
Kleene algebras are not closed under homomorphic mappings.

Proof:

Let $\mathrm{LAN}(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, +\!\!+, \emptyset, \{\varepsilon\})$ be the Kleene algebra of formal languages over a finite alphabet Σ. Further let $A = \{0, e, a, 1\}$ (especially $a \neq 1$) and h be a homomorphism defined as:

$$\begin{array}{rcl} h : \mathcal{P}(\Sigma^*) & \rightarrow & A \\ h(X) & \mapsto & \begin{cases} 0 \text{ if } X = \emptyset \\ e \text{ if } X = \{\varepsilon\} \\ a \text{ if } |X| < \infty, X \neq \emptyset, X \neq \{\varepsilon\} \\ 1 \text{ if } |X| = \infty. \end{cases} \end{array}$$

Under this mapping A becomes the homomorphic image of $\mathcal{P}(\Sigma^*)$. In general (independently of the homomorphism h), the triangle inequality holds for arbitrary sets M and N of $\mathcal{P}(\Sigma^*)$:

$$|M +\!\!+ N| \leq |M| \cdot |N| \,.$$

This inequality implies the finiteness of $X +\!\!+ Y$ for finite sets $X, Y \subseteq \Sigma^*$ satisfying $X, Y \neq \emptyset, \{\varepsilon\}$. Therefore we calculate:

$$a \cdot a = h(X) \cdot h(Y) \overset{Hom.}{=} h(X +\!\!+ Y) = a.$$

Now we assume that A forms a Kleene algebra, then following ($*$-3) the equation

$$a \cdot a \leq a \Rightarrow a^* \cdot a \leq a. \tag{A.1}$$

have to be true. But on the other hand we can calculate $a^* \cdot a$ as:

$$\begin{array}{rl} & X^* = \bigcup\limits_{i \geq 0} X^i \\ \Rightarrow & |X^*| = \infty \\ \Rightarrow & h(X^*) = 1. \end{array}$$

$$\Rightarrow a^* \cdot a = h(X^* +\!\!+ X) = 1$$

The last step holds because of $|X^* +\!\!+ X| \geq |X^*| = \infty$ and $X \neq \emptyset$. But then we have a contradiction to (A.1).

□

Theorem A.2
A residuated Kleene algebra $(A, +, \cdot, 0, 1, ^*)$ is a variety, which is clearly defined by a residuated semiring and the following equations for $a \in A$.

$$
\begin{aligned}
1 + a + a \cdot a^* &\leq a^*, &\text{(A.2)}\\
1 + a + a^* \cdot a &\leq a^*, &\text{(A.3)}\\
(a/a)^* &\leq (a/a), &\text{(A.4)}\\
(a\backslash a)^* &\leq (a\backslash a). &\text{(A.5)}
\end{aligned}
$$

This implies in contrary to Kleene algebras, that residuated Kleene algebras are closed under homomorphic mappings.

Proof:

We only show the equivalence of $(*\text{-}3)$ and $((x/x)^* \leq (x/x))$. Then, the equivalence of $(*\text{-}4)$ and $(x\backslash x)^* \leq (x\backslash x)$ as well as the calculation w.r.t. $(*\text{-}1)$ and $(*\text{-}2)$ are obvious.

"$\Rightarrow$"

$$
\begin{array}{cl}
 & (b + a \cdot x \leq x \Rightarrow a^* \cdot b \leq x)\\
\overset{b=x}{\Rightarrow} & (x + a \cdot x \leq x \Rightarrow a^* \cdot x \leq x)\\
\Leftrightarrow & (a \cdot x \leq x \Rightarrow a^* \cdot x \leq x)\\
\Leftrightarrow & (a \leq x/x \Rightarrow a^* \leq x/x)\\
\overset{a=x/x}{\Rightarrow} & (x/x)^* \leq (x/x)
\end{array}
$$

"$\Leftarrow$" Let $(x/x)^* \leq (x/x)$, then:

$$
\begin{array}{cl}
 & a \cdot x \leq x\\
\Leftrightarrow & a \leq x/x\\
\Rightarrow & a^* \leq (x/x)^*\\
\Rightarrow & a^* \leq x/x\\
\Leftrightarrow & a^* \cdot x \leq x
\end{array}
$$

Using this calculation we can following the truth of $(*\text{-}3)$.

$$
\begin{array}{cl}
 & b + a \cdot x \leq x\\
\Leftrightarrow & b \leq x \wedge a \cdot x \leq x\\
\Rightarrow & b \leq x \wedge a^* \cdot x \leq x\\
\Rightarrow & a^* \cdot b \leq x
\end{array}
$$

□

Lemma A.3
In residuated Kleene algebras the two induction laws $(*\text{-}3)$ and $(*\text{-}4)$ are equivalent, i.e.,

$$(b + a \cdot x \leq x \Rightarrow a^* \cdot b \leq x) \Leftrightarrow (b + x \cdot a \leq x \Rightarrow b \cdot a^* \leq x).$$

Proof:

"$\Rightarrow$" (i) First we show $1 \leq x\backslash x$.

$$
\begin{array}{cl}
 & 1 \leq x\backslash x\\
\Leftrightarrow & x \leq x\\
\Leftrightarrow & \texttt{true}
\end{array}
$$

(ii) Now we can show the Idempotency of $(x\backslash x)$w.r.t. multiplication, i.e., $(x\backslash x)\cdot(x\backslash x) = (x\backslash x)$

$$\begin{array}{ll}
 & (x\backslash x)\cdot(x\backslash x) \le (x\backslash x) \\
\Leftrightarrow & x\cdot(x\backslash x)\cdot(x\backslash x) \le x \\
\overset{3.1.4}{\Leftarrow} & x\cdot(x\backslash x) \le x \\
\overset{3.1.4}{\Leftarrow} & x \le x \\
\Leftrightarrow & \texttt{true}
\end{array}$$

$(x\backslash x) \le (x\backslash x)\cdot(x\backslash x)$ follows directly of (i).

(iii) Before calculating the final result, we have to show $(b + a\cdot x \le x \Rightarrow a^*\cdot b \le x) \Rightarrow (1 + a + x\cdot x \le x \Rightarrow a^* \le x)$

$$\begin{array}{ll}
 & a \le x \\
\Rightarrow & \quad\{\text{isotonicity w.r.t. multiplication}\} \\
 & a\cdot x \le x\cdot x \\
\Rightarrow & \quad\{\text{assumption: } x\cdot x \le x\} \\
a\cdot x \le x & \\
\Rightarrow & \quad\{x \le x \text{ and supremum}\} \\
 & x + a\cdot x \le x \\
\Rightarrow & \quad\{\text{assumption}\} \\
 & a^*\cdot x \le x \\
\Rightarrow & \quad\{\text{assumption: } 1 \le x\} \\
 & a^*\cdot 1 \le x \\
\Leftrightarrow & a^* \le x
\end{array}$$

(iv) Finally, we can show $b + x\cdot a \le x \Rightarrow b\cdot a^* \le x$

$$\begin{array}{ll}
 & b + x\cdot a \le x \\
\Leftrightarrow & \quad\{\text{supremum}\} \\
 & b \le x \wedge x\cdot a \le x \\
\Leftrightarrow & \quad\{\text{definition of } \backslash\} \\
 & b \le x \wedge a \le x\backslash x \\
\Leftrightarrow & \quad\{\text{(i) and (ii)}\} \\
 & b \le x \wedge a \le x\backslash x \wedge 1 \le x\backslash x \wedge (x\backslash x)\cdot(x\backslash x) \le (x\backslash x) \\
\Leftrightarrow & \quad\{\text{supremum}\} \\
 & b \le x \wedge 1 + a + (x\backslash x)\cdot(x\backslash x) \le x\backslash x \\
\Rightarrow & \quad\{\text{(iii)}\} \\
 & b \le x \wedge a^* \le x\backslash x \\
\Leftrightarrow & \quad\{\text{definition of } \backslash\} \\
 & b \le x \wedge x\cdot a^* \le x \\
\Rightarrow & \quad\{\text{isotony of multiplication}\} \\
 & b\cdot a^* \le x
\end{array}$$

"$\Leftarrow$"

Similar to "$\Rightarrow$".

□

Bibliography

[Beh98] R. Behnke. *Transformationelle Programmentwicklung im Rahmen Relationaler und Sequentieller Algebren*. 1998.

[Bir76] G. Birkhoff. *Lattice Theory.* American Mathematical Society Colloquium Publications, vol XXV, American Mathematical Society, Rhode Island, 1976.

[BJ72] T.S. Blyth and M.F. Janowitz. *Residuation Theory*, *Pure and Applied Mathematics*, volume 102. Pergamon Press, 1972.

[CHR91] C. Zhou, C.A.R Hoare, and A.P. Ravn. A Calculus of Durations. *Information Processing Letters*, volume 40, pages 269–276. 1991.

[Con71] J. H. Conway. *Regular Algebra and Finite State Machines.* Chapman & Hall, 1971.

[Dim00] Cătălin Dima. *Real-time Automata and the Kleene Algebra of Sets of Real Numbers. Proceedings of STACS'2000*, pages 279–289. 2000.

[DMS03] J. Desharnais, B. Möller, and G. Struth. *Kleene Algebra with Domain.* Technical report, Universität Augsburg, 2003.
http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2003-7.pdf.

[DMS04] J. Desharnais, B. Möller, and G. Struth. *Modal Kleene Algebra and Applications – A Survey. Journal on Relational Methods in Computer Science*, volume 1, pages 93–131. 2004.

[Dut95a] B. Dutertre. *Complete Proof Systems for First Order Interval Temporal Logic. Tenth Annual IEEE Symb. on Logic in Computer Science*, IEEE Press, pages 36–43. 1995.

[Dut95b] B. Dutertre. *On First Order Interval Temporal Logic.* Technical Report CSD-TR-94-3, Departement of Computer Science, Royal Holloway, University of London, Egham, Surray TW20 0EX, England. 1995.

[HC97] M.R. Hansen and Zhou Chaochen. *Duration Calculus: Logical Foundations. Formal Aspects of Computing*, volume 9, pages 283–330. 1997.

[Heh98] E.C.R. Hehner. *Formalization of Time and Space. Formal Aspects of Computing*, volume 10, pages 290–306. 1998.

[Hun02] D. Van Hung. *Real-time Systems Development with Duration Calculi: An Overview.* In Bernhard K. Aichernig and T. S. E. Maibaum, editors, *Formal Methods at the Crossroads. From Panacea to Foundational Support, 10th Anniversary Colloquium of UNU/IIST, the International Institute for Software Technology of The United Nations University, Lisbon, Portugal, March 18-20, 2002, Revised Papers. Lecture Notes in Computer Science*, volume 2757, pages 81–96. 2002.

[HW93] U. Hebisch and H.J. Weinert. *Halbringe. Algebraische Theorie und Anwendungen in der Informatik.* Teubner-Studienbücher: Mathematik. Teubner. 1993.

[IS90] K. Iwano and K. Steiglitz. *A Semiring on Convex Polygons and Zero-sum Cycle Problems. SIAM Journal on Computing*, volume 19(5), pages 883–901. 1990.

[Jip02] P. Jipsen. *An Overview of Residuated Kleene Algebras and Lattices. Workshop: Algebra Substructural Logics (A sub L) take two.* 2002.
http://www.chapman.edu/ jipsen/mathml/AsubLTalk20021.pdf.

[Kar96] B. von Karger. *Temporal Algebra*, Habilitationsschrift. Math. Structures in Computer Science, 1996.

[Kar00] B. von Karger. *A Calculational Approach to Reactive Systems. Science of Computer Programming*, volume 37, pages 139–161. 2000.

[Kar01] B. von Karger. *Temporal Algebra.* In Roland Backhouse, Roy Crole, and Jeremy Gibbons, editors, *Algebraic and Coalgebraic Methods in the Mathematics of Program Construction*, *Lecture Notes in Computer Science*, volume 2297, pages 309–385. Springer. 2001.

[Koz90] D. Kozen. *On Kleene Algebras and Closed Semirings.* In Rovan, editor, *Mathematical Foundation in Compututer Science 1990*, *Lecture Notes in Computer Science*, volume 452, pages 26–47. Springer. 1990. http://www.cs.cornell.edu/kozen/papers/kacs.ps.

[Koz94] D. Kozen. *A Completeness Theorem for Kleene Algebras and the Algebra of Regular Events. Information and Computation*, volume 110(2), pages 366–390. 1994.

[LRL98] Z. Liu, A.P. Ravn, and X. Li. *Unifying Proof Methodologies of DC and LTL. Duration Calculus Workshop, ESSLLI'98*, pages 99–109. 1998.

[Möl] B. Möller. *Residuals and Detachments.* unpublished paper.

[Pra91] V. Pratt. *Action Logic and Pure Induction, Logics in AI. European Workshop JELIA '90, ed J. van Eijck*, *Lectures in Computer Science*, volume 478, pages 97–120. 1991. http://boole.stanford.edu/pub/jelia.ps.gz.

[SRR89] E.V. Sørensen, A.P. Ravn, and H. Rischel. *Control Program for a Gas Burner: Part 1: Informal Requirements.* Technical Report ID/DTH EVS2, ProCoS, ESPRIT BRA 3104, ID/DTH, Lyngby, Denmark. 1989.