Von sequentieller Algebra zu Kleene-Algebra: Intervalloperatoren und Zeitdauer-Kalkül

Diplomarbeit
für den Studiengang Mathematik
Lehrstuhl für Datenbanken und Informationssysteme
Institut für Informatik
Universität Augsburg

von

Peter Höfner

9.Oktober 2003

Erstgutachter: Prof. Dr. Bernhard Möller
Zweitgutachter: Prof. Dr. Walter Vogler

Inhaltsverzeichnis

Kapitel 1

Einleitung

Der Zeitdauer-Kalkül (Duration Calculus, DC) ist ein formales, algebraisches System für die Spezifikation und das Design eines Echtzeit-Sicherheitssystems. Seit seiner ersten Erwähnung im Jahr 1991 durch Z. Chaochen, C.A.R. Hoare und A.P. Ravn in [CHR91] wurde er mehrfach unter verschiedensten Aspekten betrachtet. In der ursprünglichen Version gingen die Autoren von temporaler Logik aus und stellten durch den Zeitdauer-Kalkül eine Verknüpfung zu Sicherheitssystemen und Intervallen her. M.R. Hansen und Z. Chaochen zeigten 1997 in [HC97], dass der Zeitdauer-Kalkül die Intervall-Logik (IL), welche auf [Dut95a, Dut95b] beruht, in gewisser Weise erweitert. Auch wurde häufig der Zusammenhang zwischen DC und linearer temporaler Logik (Linear Temporal Logic, LTL) betrachtet (vgl. z.B. [LRL98]). In den meisten dieser Schriften wird das Beispiel der Gasleitung mit einem Leck (gas burner example) dargestellt. Es beruht ebenfalls auf dem Artikel von Z. Chaochen et al. ([CHR91]). B. von Karger betrachtet den Zeitdauer-Kalkül in [Kar00] unter dem Aspekt der Einbettung in sequentielle Algebren. Er führt zudem erstmalig den Begriff der Ingenieurs-Induktion (Engeneer's induction) ein.

Unabhängig hiervon existiert die algebraische Struktur der Kleene-Algebra (KA). Diese erweitert Halbringe um einen weiteren unären Operator, den Kleene-Stern. Kleene-Algebren wurden schon auf vielfältigste Weise untersucht. So bewies beispielsweise D. Kozen viele ihrer grundlegenden Eigenschaften ([Koz90, Koz94]). Auch B. Möller und J. Desharnais lieferten viele Resultate über Kleene-Algebren, ihre Eigenschaften und Algorithmen auf ihnen (vgl. z.B. [DMS03]).

Einen ersten Schritt zur Verknüpfung dieser beiden Ideen (KA und DC) lieferte im Jahr 2000 C. Dima in [Dim00]. Er entwickelte hierzu eine Kleene-Algebra über der Potenzmenge der positiven reellen Zahlen $\mathcal{P}(\mathbb{R}^+)$[1]. Weiterhin zeigte er, dass die reellen Zahlen bei zeit-theoretischen Überlegungen, wie sie für den Zeitdauer-Kalkül benötigt werden, eine zentrale Rolle spielen.

[1] Die dort dargestellte Kleene-Algebra unterscheidet sich gegenüber der von D. Kozen vorgestellten Definition in der Art, dass diese Struktur nicht additiv idempotent ist.

Ziel dieser Arbeit soll es sein, den Zeitdauer-Kalkül auf der Grundlage von Kleene-Algebren zu analysieren und zu präsentieren. Zu diesem Zweck wird in Kapitel 2 der Begriff der Kleene-Algebra erläutert und an einigen Beispielen illustriert. In Kapitel 3 werden spezielle Operatoren, die Residuen und die Abtrennungsoperatoren, eingeführt und im darauf folgenden Kapitel zu bestimmten modalen Operatoren, den so genannten Intervalloperatoren, erweitert. Um in Kapitel 6 den Zeitdauer-Kalkül herleiten zu können, wird in Kapitel 5 die Ingenieurs-Induktion dargestellt, bei der es sich um einen Satz handelt, welcher die Intervalloperatoren mit dem kleinsten Fixpunkt eines Elementes in einer Kleene-Algebra verbindet. Sie wurde erstmalig, wie oben erwähnt, von B. von Karger in [Kar00] vorgestellt. Schließlich wird in Kapitel 6 der Zeitdauer-Kalkül zunächst an Hand des Gasleitungs-Beispiels erläutert und anschließend in einer sehr allgemeinen Form gezeigt.

Kapitel 2

Grundlagen

In diesem Kapitel werden kurz die Grundlagen bereitgestellt, die später für die Theorie von Residuen, Intervalloperatoren und den Zeitdauer-Kalkül benötigt werden. Dazu gehören Halbringe und Kleene-Algebren. Beispiele werden diese algebraischen Strukturen veranschaulichen. Für weitere Informationen eignen sich zum Beispiel [HW93] und [Koz94].

2.1 Halbringe

Definition 2.1.1 (geordnete Menge)
Ein Paar $(M, \leq)$ mit einer partiellen Ordnung $\leq$ auf einer Menge M heißt *geordnete Menge*.

Definition 2.1.2 ((idempotenter) Halbring)
Ein *Halbring* ist ein Quintupel $(A, +, \cdot, 0, 1)$ mit folgenden Eigenschaften:

(i) $(A, +, 0)$ ist ein kommutatives Monoid

(ii) $(A, \cdot, 1)$ ist ein Monoid mit *Annihilator* 0,
d.h. $0 \cdot x = x \cdot 0 = 0 \quad \forall x \in A$

(iii) Es gelten die Distributivgesetze
$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z \\ (x + y) \cdot z &= x \cdot z + y \cdot z \end{aligned}$$

(iv) Gilt zusätzlich stets $x + x = x$, so heißt der Halbring *idempotent*.

Wird die Relation $\leq$ auf einem idempotenten Halbring durch

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

definiert, so wird $(A, \leq)$ zu einer geordneten Menge. Diese Ordnung ist die einzige, die monoton bezüglich der Addition und der Multiplikation ist und

für die $0 \leq a$ für alle $a \in A$ gilt. Aus diesem Grund wird sie häufig auch die *natürliche Ordnung* des Halbrings genannt.
Offensichtlich ist jeder idempotente Halbring auch ein Halbverband bezüglich der natürlichen Ordnung und der Addition. Daher gilt in idempotenten Halbringen für $a, b, c \in A$:

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

Die folgenden Beispiele veranschaulichen diese Definition.

Beispiel 1

(i) $(\mathbb{Z}, +, \cdot, 0, 1)$ sowie alle anderen Ringe und Körper sind Halbringe.

(ii) Gilt in einem Halbring $0 = 1$, so enthält er genau ein Element, nämlich $A = \{0\}$, da

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

Aus diesem Grund wird ein Halbring, in dem $0 = 1$ gilt, als *trivialer Halbring* bezeichnet.

(iii) Die Struktur $(\{0, 1\}, +, \cdot, 0, 1)$ wird durch die unten aufgeführten Verknüpfungstafeln zu einem idempotenten Halbring.

$+$	0	1
0	0	1
1	1	1

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

Die natürliche Ordnung dieses Halbrings ist $0 \leq 1$. Da hier $+$ die Rolle des logischen Oder $\vee$ und $\cdot$ die Rolle des logischen Und $\wedge$ übernimmt, wird er häufig auch als *boolescher Halbring* bezeichnet.

(iv) Ein Beispiel für einen idempotenten Halbring mit drei Elementen ist durch folgende Verknüpfungstafeln gegeben.

$+$	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

Die natürliche Ordnung von $(\{0, a, 1\}, +, \cdot, 0, 1)$ ist $0 \leq 1 \leq a$.

(v) $(\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$ ist ein idempotenter Halbring und wird oft auch als *tropischer Halbring* bezeichnet. Seine natürliche Ordnung $\leq_{nat}$ ergibt sich folgendermaßen:

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

(vi) $(\mathbb{N} \cup \{-\infty\}, \max, +, -\infty, 0)$ ist ein idempotenter Halbring, dessen natürliche Ordnung mit der üblichen Standardordnung übereinstimmt.

(vii) Analog zu (v) oder (vi) können auch andere idempotente Funktionen als Addition verwendet werden. So ist beispielsweise $(\mathbb{N}, \mathrm{ggT}, \cdot, 0, 1)$ ebenfalls ein Halbring, dessen Ordnung der Teilbarkeitsrelation entspricht.

Weitere Beispiele, insbesondere mit drei oder vier Elementen, finden sich in [DMS03].
Die Betrachtung der Potenzmenge über einer beliebigen Menge X, die mit einem Produkt versehen ist, und die Definition einer Multiplikation auf der Potenzmenge als elementweises Produkt, ergibt eine spezielle Klasse von Halbringen.

Definition 2.1.3 (Halbring über X)
Sei X eine Menge und $\cdot : X \times X \to X$ eine (partiell definierte) binäre, assoziative und abgeschlossene Operation. Dann ist $\mathcal{H}_X := (\mathcal{P}(X), \cup, \circ, \emptyset, 1)$ der *Halbring über X* mit

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

sofern ein neutrales Element bezüglich der Multiplikation existiert, d.h.

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

Durch Verwendung eines Monoids $(X, \cdot, 1_X)$ als Grundmenge entsteht das neutrale Element bezüglich der Multiplikation im Halbring über X durch $\{1_X\}$. Dies bedeutet $\{1_X\} \circ A = A \circ \{1_X\} = A$.
Weiterhin ist zu beachten, dass der Halbring über X idempotent bezüglich der Addition (Vereinigung) ist. Aus diesem Grund ist es zudem möglich, die natürliche Ordnung zu betrachten:

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

Dies ist genau die Teilmengenbeziehung, d.h. $A \leq B$ gilt genau dann, wenn A eine Teilmenge von B ist. Um manche Beweise übersichtlicher zu gestalten, wird bei Mengen im Folgenden häufig auch das Teilmengensymbol $\subseteq$ anstelle von $\leq$ verwendet.
Für solche Halbringe sind einige Beispiele angegeben.

Beispiel 2

(i) Sei Σ^* die Menge aller Wörter über einem endlichen Alphabet Σ. Definiert man die Konkatenation zweier Worte $u, v \in \Sigma^*$ als $u{+}{+}v$, so ist folgende Abbildung zweier Mengen von Wörtern $U, V \in \mathcal{P}(\Sigma^*)$ gegeben:

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

$LAN(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, {+}{+}, \emptyset, \varepsilon)$ stellt den Halbring der formalen Sprachen dar. Hierbei entspricht $\emptyset$ der leeren Sprache und ε dem leeren Wort.

(ii) Sei V eine Menge von Knoten. Dann stellen Teilmengen von V^* mögliche Pfade in Graphen zwischen den Knoten V dar. Die Pfadkomposition, bildlich gesprochen das Verkleben zweier Pfade, kann als partielle Funktion definiert werden. Sei ε der leere Pfad, $x, y \in V$ und $s, t \in V^*$. $(y.t) \in V^* \backslash \{\varepsilon\}$ bedeute, dass y der erste Knoten eines Pfades ist und t den restlichen Pfad ohne y beinhaltet, $(s.x)$ kann dementsprechend definiert werden:

$$\begin{aligned}
\bowtie\colon V^* \times V^* &\to V^* \\
\varepsilon \bowtie \varepsilon &\mapsto \varepsilon \\
\varepsilon \bowtie (y.t) & \quad \text{ist undefiniert} \\
(s.x) \bowtie \varepsilon & \quad \text{ist undefiniert} \\
(s.x) \bowtie (y.t) &\mapsto \begin{cases} s.x.t & \text{, falls } x = y \\ \text{undefiniert,} & \text{falls } x \neq y. \end{cases}
\end{aligned}$$

Diese Operation auf V^* kann wie oben beschrieben auch zu einer Funktion $\bowtie\colon \mathcal{P}(V^*) \times \mathcal{P}(V^*) \to \mathcal{P}(V)$ erweitert werden, indem man folgende Operation definiert:

$$S \bowtie T = \{s \bowtie t : s \in S, t \in T, s \bowtie t \text{ ist definiert}\}.$$

$PAT(V) = (\mathcal{P}(V^*), \cup, \bowtie, \emptyset, V^{\leq 1})$ ist somit der Halbring über V^* und wird auch als *Pfad-Halbring* bezeichnet, wobei $V^{\leq 1}$ die Menge aller Knoten mit 0 Kanten ist, also alle Knoten selbst und der leere Pfad. Daher gilt:

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

Anmerkung
Im Weiteren sei vorausgesetzt, dass, wenn von einem Halbring über einer beliebigen Menge X, die mit einer Multiplikation versehen ist, die Rede ist, stets das dazu nötige neutrale Element in $\mathcal{P}(X)$ bezüglich der Multiplikation existiert.

2.2 Kleene-Algebren

Definition 2.2.1 (Kleene-Algebra)
Eine *Kleene-Algebra* ist ein Sextupel $(A, +, \cdot, 0, 1, ^*)$, so dass $(A, +, \cdot, 0, 1)$ ein idempotenter Halbring und $^* : A \to A$ eine Funktion mit folgenden Eigenschaften ist:

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

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

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

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

Eine Kleene-Algebra wird häufig auch als *Kozen-Halbring* oder *K-Halbring* bezeichnet. Soll der $*$-Operator nicht über die Gleichungen ($*$-1)-($*$-4) definiert werden, so kann er auch als Fixpunkt ausgedrückt werden. So ist $a^* \cdot b$ der kleinste Fixpunkt der Funktion $\lambda x.b + ax$ und $b \cdot a^*$ der kleinste Fixpunkt der Funktion $\lambda x.b + xa$. Weitere Informationen und Eigenschaften von Kleene-Algebren werden zum Beispiel von D. Kozen in [Koz94] beschrieben. Da jede Kleene-Algebra ein idempotenter Halbring ist und jeder von diesen eine Halbverbandstruktur besitzt, ist es möglich, auch Verbandeigenschaften hinzuzunehmen, um spezielle Eigenschaften von Kleene-Algebren zu charakterisieren.

Definition 2.2.2 (boolesche Kleene-Algebra)
Eine Kleene-Algebra heißt *boolesch*, falls der zu Grunde liegende Verband boolesch ist.

Anhand der Beispiele des vorherigen Paragraphen wird gezeigt, welche Halbringe zu Kleene-Algebren erweitert werden können.

Beispiel 3

(i) Der triviale Halbring lässt sich mit $0^* = 0\,(= 1)$ zu einer Kleene-Algebra erweitern.

(ii) Der boolesche Halbring $(\{0,1\}, +, \cdot, 0, 1)$ wird durch $0^* = 1^* = 1$ zu einer Kleene-Algebra.

(iii) Der Halbring $(\{0, a, 1\}, +, \cdot, 0, 1)$ mit $0 \leq 1 \leq a$ und den Verknüpfungstafeln

$+$	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

wird genau dann zu einer Kleene-Algebra, wenn $a^* = a$ und $0^* = 1^* = 1$ gesetzt wird.

(iv) Der tropische Halbring $(\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$ kann nur dann zu einer Kleene-Algebra erweitert werden, wenn $n^* = 0\ \forall n \in \mathbb{N} \cup \{\infty\}$ ist. In allen anderen Fällen lässt sich leicht nachweisen, dass die Gleichungen ($*$-1) bis ($*$-4) nicht erfüllt werden können.

(v) $(\mathbb{N} \cup \{-\infty\}, \max, +, -\infty, 0)$ kann nicht zu einer Kleene-Algebra erweitert werden. Der Grund hierfür liegt in der Tatsache, dass in dieser algebraischen Struktur für $a > 0$ die Menge $\{a^n : n \in \mathbb{N}\} = \{na : n \in \mathbb{N}\}$ unbeschränkt ist. Nach Definition 2.2.1 sollte aber a^* der kleinste Fixpunkt und somit obere Schranke dieser Menge sein.
Dadurch ist auch gezeigt, dass sich nicht jeder idempotente Halbring zu einer Kleene-Algebra erweitern lässt und daher die Menge aller Kleene-Algebren eine echte Teilmenge der Menge aller idempotenten Halbringe ist.

(vi) Der Halbring der formalen Sprachen $LAN(\Sigma)$ hingegen lässt sich erweitern, indem man $L^* = \{w_1 w_2 \dots w_n : n \geq 0, w_i \in L\}$ für alle $L \subseteq \Sigma^*$ setzt.

(vii) Äquivalent zu (vi) kann auch $PAT(V)$ zu einer booleschen Kleene-Algebra $(\mathcal{P}(V^*), \cup, \bowtie, \emptyset, V^{\leq 1}, ^{\rightsquigarrow})$ ausgebaut werden, indem man $U^{\rightsquigarrow} := \bigcup_{n \in \mathbb{N}} U^n$, $U \subseteq V^*$ setzt.

Wie oben erwähnt beruht jede Kleene-Algebra auf einem Halbverband oder sogar einem Verband, wie etwa in booleschen Kleene-Algebren. Daher können auch alle Eigenschaften von (Halb-)Verbänden eins zu eins auf Halbringe und Kleene-Algebren übernommen werden. Da beim Beweis der Ingenieurs-Induktion (vgl. Kapitel 5) die μ-Fusion, eine verbandstheoretische Eigenschaft, benötigt wird, sei sie hier exemplarisch angegeben.

Satz 2.2.3 (μ-Fusion)
Sei $\mathcal{L}$ ein vollständiger Verband und f, g, h monotone Funktionen auf $\mathcal{L}$. Wenn h universell disjunktiv ist, gilt

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

Hierbei ist μ_f der kleinste Fixpunkt der Funktion f und μ_g der zu g gehörende kleinste Fixpunkt.

Kapitel 3

Residuen und Abtrennungsoperatoren

Grundlage der später vorgestellten Ingenieurs-Induktion und den Zeitdauer-Kalkül bilden die sogenannten Residuen und die eng damit verbundenen Abtrennungsoperatoren. Im Folgenden werden diese Operatoren vorgestellt und einige ihrer Eigenschaften bewiesen, wobei sich die meisten Beweise nach [Möl] richten.
Im Falle ihrer Existenz lassen sich Residuen problemlos auf Monoiden definieren, da sie lediglich von einer beliebigen, binären Verknüpfung abhängen. Auf Grund der Tatsache, dass jede Kleene-Algebra und jede sequentielle Algebra auch Monoide bildet, können Residuen auf diesen entsprechend erklärt werden.

3.1 Residuen und ihre Eigenschaften

"Residuen sind größte Lösungen spezieller Ungleichungen." [Beh98]. Das Rechtsresiduum x/y beschreibt das größte Element z so, dass $z \cdot y \leq x$ ist. Äquivalent hierzu lässt sich das Linksresiduum beschreiben. Daraus ergibt sich folgende Definition.

Definition 3.1.1 (Residuen)
Gegeben sei ein Monoid $(A, \cdot, 1)$ und sei auf A eine Ordnung $\leq$ definiert. Weiterhin seien $x, y, z \in A$.
Dann beschreibt die Relation

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

das *Rechtsresiduum* und

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

das *Linksresiduum*.

Da auf algebraischen Strukturen im Allgemeinen keine Residuen existieren müssen, wird ein Monoid, auf dem eine Ordnung und Residuen existieren, auch *Residuums-Monoid* genannt.
Interessanterweise existieren auf dem Halbring $(\mathcal{P}(A), \cup, \circ, \emptyset, 1)$ über einer Menge A (vgl. Kapitel 2) stets Residuen. T.S. Blyth und M.F. Janowitz zeigen in [BJ72], dass die Residuen in diesem Fall folgende Form haben:

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

Bei den folgenden Beispielen und Eigenschaften von Residuen spielt häufig das Beweisprinzip der indirekten Gleichheit eine wichtige Rolle. Es besagt, dass auf beliebigen Ordnungen nachstehende Beziehung gilt:

$$\begin{aligned} x = y &\Leftrightarrow (\forall z : z \leq x \Leftrightarrow z \leq y) \\ &\Leftrightarrow (\forall z : x \leq z \Leftrightarrow y \leq z). \end{aligned}$$

Beispiel 4

(i) In Gruppen G (multiplikativ geschrieben), welche mit einer Ordnung versehen sind, beschreibt das rechte Residuum x/y die Rechtsmultiplikation mit dem Inversen von y, d.h.

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

Beweis:

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

□

Analog bedeutet das linke Residuum die Linksmultiplikation:

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

(ii) Auf Grund von (i) gilt das Gleiche in Ringen (hier jedoch nur bezüglich der Addition) und Körpern.

(iii) Betrachtet man das Monoid $M = (\mathbb{N} \cup \{\infty\}, \cdot, 1)$ mit $0 \cdot \infty = \infty \cdot 0 = 0$, so beschreiben beide Residuen zunächst dasselbe Element, da M kommutativ ist. Die obige Definition beschreibt die ganzzahlige Division, d.h. die Residuen sind $\lfloor x/y \rfloor$, wobei $\lfloor z \rfloor$ das Abrunden auf die nächste natürliche Zahl bedeutet, welche kleiner oder gleich z ist. Hierbei fällt auf, dass im Fall $M' = (\mathbb{N}, \cdot, 1)$ die Residuen nicht mehr definiert sind, da $\lfloor n/0 \rfloor \notin M', n \in \mathbb{N}\backslash\{0\}$.

(iv) Ein sehr interessantes Beispiel zeigt P. Jipsen in [Jip02] bzw. V. Pratt in [Pra91]. Sie erklären Residuen als Ereignisse im menschlichen Leben.

Seien folgende Ereignisse gegeben:

p : "Man setzt Geld auf ein Pferd (in einem Pferderennen)."
q : "Das Pferd gewinnt."
r : "Man wird reich."

Dann beschreibt die Ungleichung $pq \leq r$ nachstehende Tatsache:

"Wenn man Geld auf ein Pferd setzt und dieses dann gewinnt, wird man reich."

Im Gegensatz hierzu beschreiben die Residuen jeweils etwas Anderes:
$p \leq r/q$:

"Wenn man Geld auf ein Pferd setzt, wird man reich, falls das Pferd gewinnt."

$q \leq p\backslash r$:

"Wenn ein Pferd gewinnt und hätte man dann auf dieses Geld gesetzt, so wäre man reich geworden."

Aus Beispiel (iii) folgt unmittelbar eine einfache Eigenschaft.

Korollar 3.1.2
Sei $(A, \cdot, 1, \backslash, /)$ ein Monoid mit Residuen. Besitzt A einen Annihilator 0, d.h. $a \cdot 0 = 0 = 0 \cdot a \ \forall a \in A$ und ist 0 kleinstes Element, so existiert auch ein größtes Element $\top$.

Beweis:

Wähle $a \in A$ beliebig. Dann gilt:

$$\begin{array}{ll} & x \leq a/0 \\ \Leftrightarrow & x \cdot 0 \leq a \\ \Leftrightarrow & \texttt{true} \\ \Rightarrow & \text{Das Residuum ist } \top. \end{array}$$

□

Nach der Vorstellung zahlreicher Beispiele für Residuen beschäftigt sich der Rest dieses Paragraphen mit wichtigen Eigenschaften von diesen. Da die folgenden Sätze sowohl für rechte Residuen als auch für linke gelten, beschränken sich die Beweise nur auf rechte Residuen. Die Beweise für die linken Residuen sind symmetrisch hierzu und können deshalb ohne Einschränkungen weggelassen werden. Außerdem sei im Weiteren, sofern nicht anders angegeben, $(A, \cdot, 1, \backslash, /)$ ein Residuums-Monoid und $u, v, x, y, z \in A$.

Lemma 3.1.3
Es gilt:

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

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

Beweis:

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

□

Lemma 3.1.4
Es gilt:

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

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

Beweis:

Setze $z = (x/y)$ bzw. $z = (y\backslash x)$ in der Definition (3.1.1).

□

Lemma 3.1.5
Es gilt:

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

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

Beweis:

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

□

Lemma 3.1.6 (Euklid für Residuen)
Es gilt:

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

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

Beweis:

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

□

Lemma 3.1.7
Besitzt das Monoid ein größtes Element $\top$, so ist

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

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

Beweis:

Da $\top$ das größte Element darstellt, reicht es zu zeigen, dass $\top \leq \top/x$ ist.

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

□

Lemma 3.1.8
Es gilt:

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

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

Beweis:

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

□

Lemma 3.1.9
Es gilt:

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

Beweis:

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

□

Bei den nun folgenden Sätzen sei nicht nur ein Monoid vorausgesetzt, sondern jeweils ein idempotenter Halbring auf dem Residuen definiert sind. Diese beziehen sich dabei auf die Multiplikation und nicht auf die Addition. Außerdem existiere ein Infimumsoperator $\sqcap$ und ein Supremumsoperator $\sqcup$, also $x \sqcap y := \inf\{x, y\}, x \sqcup y := \sup\{x, y\}$.

Lemma 3.1.10 (Links-Konjunktivität)
Falls X eine Menge von Elementen aus A ist, gilt:

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

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

Beweis:

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

□

Lemma 3.1.11 (Rechts-Antidisjunktion)
Sei Y eine Menge von Elementen aus A. Dann gilt:

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

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

Beweis:

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

□

3.2 Abtrennungsoperatoren

Ergänzt man Residuums-Monoide noch um eine weitere Operation, die Negation, so ist es möglich, zusätzliche Operatoren, die sogenannten Abtrennungsoperatoren, zu definieren und deren Eigenschaften zu untersuchen. Diese Abtrennungsoperatoren spielen vor allem in dem Halbring der formalen Sprachen eine große Rolle, da sie hier das Abschneiden von Teilwörtern beschreiben.

Definition 3.2.1
Sei $(A, +, 0)$ ein idempotentes Monoid mit größtem Element $\top$. Die *Negation* ist eine Abbildung $\overline{} : A \to A$ mit folgenden Eigenschaften:

- $\overline{\overline{a}} = a$, $\forall a \in A$,
- $a + \overline{a} = \top$,
- $x \leq y \Rightarrow \overline{y} \leq \overline{x}$ (bzgl. der natürlichen Ordnung).

Aus den ersten beiden Eigenschaften folgt unmittelbar, dass $\overline{\top} = 0$ und $\overline{0} = \top$. Des Weiteren folgen aus dieser Definition direkt die Gesetze von de Morgan, falls zu je zwei Elementen ein Infimum und ein Supremum existiert (wie zum Beispiel in Verbänden).

Lemma 3.2.2 (de Morgan'sche Gesetze)
Existieren Infima und Suprema mit $x \sqcap y := \inf\{x, y\}$ und $x \sqcup y := \sup\{x, y\}$, so gilt:

$$\overline{x \sqcup y} = \overline{x} \sqcap \overline{y}$$

$$\overline{x \sqcap y} = \overline{x} \sqcup \overline{y}$$

Beweis:

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

Rest analog.

□

Definition 3.2.3 (Abtrennungsoperatoren)
Sei ein idempotenter Halbring mit einer zusätzlichen Negationsabbildung und Residuen gegeben, also ein 8-Tupel $H = (A, \cdot, +, 1, 0, \backslash, /, \overline{})$. Dann ist die *Rechtsabtrennung* wie folgt definiert:

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

Symmetrisch hierzu wird die *Linksabtrennung* als

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

gesetzt.

Beispiel 5
Am besten zu verdeutlichen sind diese Operatoren an dem Halbring $LAN(\Sigma)$, also jenem der formalen Zeichenketten über einem Alphabet Σ. Die Negation eines Elementes $A \in \mathcal{P}(\Sigma)$ ist die Komplementbildung von A, d.h. $x \in \overline{A} \Leftrightarrow x \notin A$. Die Residuen können direkt ausgerechnet werden. Die Abtrennungsoperatoren $x\lfloor y$ bzw. $y\rfloor x$ entstehen durch Abschneiden von Post- bzw. Präfixen der Wörter aus x. Es werden genau die end- bzw anfangsständigen Wörter abgeschnitten, welche in y liegen. Zur Verdeutlichung einige kleine Beispiele:
Sei $\Sigma = \{a, b, c\}$

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

Im Weiteren gelte der Einfachheit halber wieder, dass H ein "erweiterter", idempotenter Halbring wie in Definition 3.2.3 und $u, v, x, y, z \in A$ sei.
Im restlichen Teil dieses Paragraphen werden noch Eigenschaften über die Abtrennungsoperatoren bewiesen. Wie bei Residuen reicht es, die Beweise nur für die Rechtsabtrennung zu zeigen. Diejenigen für den Linksabtrennungsoperator sind hierzu wieder symmetrisch.

Lemma 3.2.4 (Distributivität)
Es gilt:

(i) $(x + y)\lfloor z = x\lfloor z + y\lfloor z$

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

Beweis:

$$
\begin{aligned}
& (x+y)\lfloor z \leq u \\
\Leftrightarrow\ & \overline{\overline{(x+y)}/z} \leq u \\
\Leftrightarrow\ & \overline{u} \leq \overline{(x+y)}/z \\
\Leftrightarrow\ & \overline{u} \cdot z \leq \overline{(x+y)} \\
\Leftrightarrow\ & x + y \leq \overline{\overline{u} \cdot z} \\
\Leftrightarrow\ & x \leq \overline{\overline{u} \cdot z} \wedge y \leq \overline{\overline{u} \cdot z} \\
\Leftrightarrow\ & \overline{u} \cdot z \leq \overline{x} \wedge \overline{u} \cdot z \leq \overline{y} \\
\Leftrightarrow\ & \overline{u} \leq \overline{x}/z \wedge \overline{u} \leq \overline{y}/z \\
\Leftrightarrow\ & \overline{\overline{x}/z} \leq \overline{\overline{u}} \wedge \overline{\overline{y}/z} \leq \overline{\overline{u}} \\
\Leftrightarrow\ & \overline{\overline{x}/z} + \overline{\overline{y}/z} \leq u \\
\Leftrightarrow\ & x\lfloor z + y\lfloor z \leq u
\end{aligned}
$$

□

Damit gelten auch folgende Gleichungen, falls $X \subseteq A$:
$(\sqcup X)\lfloor z = \sqcup(X\lfloor z)$ und $z\rfloor(\sqcup X) = \sqcup(z\rfloor X)$.

Lemma 3.2.5 (Disjunktion)
Existieren neben den bereits vorausgesetzten Eigenschaften auch die $\sqcup-$ und $\sqcap-$Operatoren, so gilt:

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

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

Beweis:

$$\begin{aligned}
& x\lfloor(\sqcup Y) \\
= \quad & \overline{\overline{x}/(\sqcup Y)} \\
\overset{3.1.11}{=} \quad & \overline{\sqcap\{\overline{x}/y : y \in Y\}} \\
\overset{3.2.2}{=} \quad & \sqcup\{\overline{(\overline{x}/y)} : y \in Y\} \\
= \quad & \sqcup\{x\lfloor y : y \in Y\} \\
= \quad & \sqcup(x\lfloor Y)
\end{aligned}$$

□

Lemma 3.2.6
Es gilt:

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

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

Beweis:

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

□

Lemma 3.2.7
Es gilt:

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

Beweis:

$$\begin{aligned}
& \overline{\overline{\overline{(x\rfloor y)\lfloor z}}} \\
= \quad & \overline{\overline{\overline{x\backslash\overline{y}/z}}} \\
= \quad & \overline{\overline{(x\backslash\overline{y})/z}} \\
\overset{3.1.9}{=} \quad & \overline{x\backslash\overline{(\overline{y}/z)}} \\
= \quad & x\backslash\overline{\overline{\overline{\overline{y}/z}}} \\
= \quad & x\rfloor(y\lfloor z)
\end{aligned}$$

□

Lemma 3.2.8
Es gilt:

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

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

Beweis:

Direkt aus Lemma 3.2.5.

□

Lemma 3.2.9
Falls der Halbring $(A, +, \cdot, 0, 1)$ ein größtes Element $\top$ besitzt, so gilt:

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

(ii) In einer Kleene-Algebra gilt daher auch für ein Element a
$\top\lfloor a^* = \top$
$a^*\rfloor\top = \top$

(iii) Außerdem gilt:
$x\lfloor(\top\lfloor y) \leq x\lfloor\top$
$(y\rfloor\top)\rfloor x \leq \top\rfloor x$

Beweis:

(i)

$$\begin{aligned}
& \top \leq \top\lfloor 1 \\
\Leftrightarrow \quad & \top \leq \overline{\overline{\top}/1} \\
\Leftrightarrow \quad & \overline{\top}/1 \leq \overline{\top} \\
\Leftrightarrow \quad & \overline{\top} \leq \overline{\top}\cdot 1 \\
\Leftrightarrow \quad & \texttt{true}
\end{aligned}$$

(ii)

$$
\begin{array}{ll}
 & 1 + a \cdot a^* \leq a^* \quad (*\text{-}1) \\
\Rightarrow & 1 \leq a^* \\
\overset{3.2.8}{\Rightarrow} & \top \rfloor 1 \leq \top \rfloor a^* \\
\overset{(i)}{\Leftrightarrow} & \top \leq \top \rfloor a^*
\end{array}
$$

(iii)

$$
\begin{array}{ll}
 & x \lfloor (\top \rfloor y) \leq x \lfloor \top \\
\overset{3.2.8}{\Leftarrow} & \top \rfloor y \leq \top \\
\Leftrightarrow & \texttt{true}
\end{array}
$$

□

3.3 Halbringe, sequentielle Algebren, Kleene-Algebren mit Residuen und Beobachtungsräume

In der Literatur über den Zeitdauer-Kalkül oder damit verwandte Themen fallen häufig die Begriffe *sequentielle Algebra* ([Kar00, Kar01]), *Kleene-Algebren mit Residuen* ([Jip02]) sowie auch *Beobachtungsräume* (Observation Spaces) ([Kar96, Kar00]). Daher sollen diese Begriffe definiert und miteinander verglichen werden, um ein Gefühl dafür zu bekommen, wie sie miteinander zusammenhängen. Ein Halbring $(A, +, \cdot, 0, 1)$ kann, wie in diesem Kapitel beschrieben, unter Umständen zusätzlich mit Residuen und einer Negationsabbildung versehen werden. Im Weiteren soll ein solcher Halbring *Abtrennungs-Halbring* genannt werden, da, wie oben gezeigt, die Residuen und die Negationsabbildung zur Definition der Abtrennungsoperatoren genügen. Im Vergleich zu diesen speziellen Halbringen sind sequentielle Algebren wie folgt charakterisiert:

Definition 3.3.1 (Sequentielle Algebra (vgl.[Kar96]))
Eine *sequentielle Algebra* ist ein vollständiger boolescher Verband $(S, \cap, \cup, \overline{})$ mit größtem Element $\top$ und kleinstem Element $\bot$, auf dem zusätzlich drei binäre Operatoren (Komposition $\cdot$, Linksdivision $\rfloor$ und Rechtsdivision $\lfloor$) definiert sind, welche folgende Axiome erfüllen:

$(S, \cdot, 1)$ ist ein Monoid, (Monoid)

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

$P \cdot (Q \lfloor R) \subseteq (P \cdot Q) \lfloor R$, (Euklid)

$1 \lfloor P = P \rfloor 1$. (Reflection)

Ohne die beiden Axiome Euklid und Reflection ist diese algebraische Struktur äquivalent zu den Abtrennungs-Halbringen, wenn letzteren ein boolescher Verband zu Grunde liegt. Daher ist offensichtlich, dass jede sequentielle Algebra ein Abtrennungs-Halbring ist, aber nicht umgekehrt.

Kleene-Algebren ergeben sich, wie oben erwähnt, durch idempotente Halbringe, welche um den $*$-Operator erweitert werden. Eine mögliche Motivation, Kleene-Algebren mit Residuen zu versehen, liefert P. Jipsen in [Jip02]. So kann gezeigt werden, dass Kleene-Algebren unter homomorphen Abbildungen nicht abgeschlossen sind. Betrachtet man hingegen nur jene Kleene-Algebren, die mit Residuen versehen werden können, sind diese homomorph abgeschlossen.[1] Des Weiteren kann in Kleene-Algebren mit Residuen leicht nachgerechnet werden, dass die beiden Horn-Regeln ($*$-3) und ($*$-4) zueinander äquivalent sind.[1]

Mit obigen Erkenntnissen ist es möglich, ein Diagramm (Abb. 3.1) zu erstellen, welches die Teilmengenbeziehungen zwischen den in dieser Arbeit verwendeten algebraischen Strukturen verdeutlicht. Hierbei ist eine algebraische Struktur X genau dann in einer anderen Y enthalten, wenn eine Pfeilkette von Y nach X existiert.

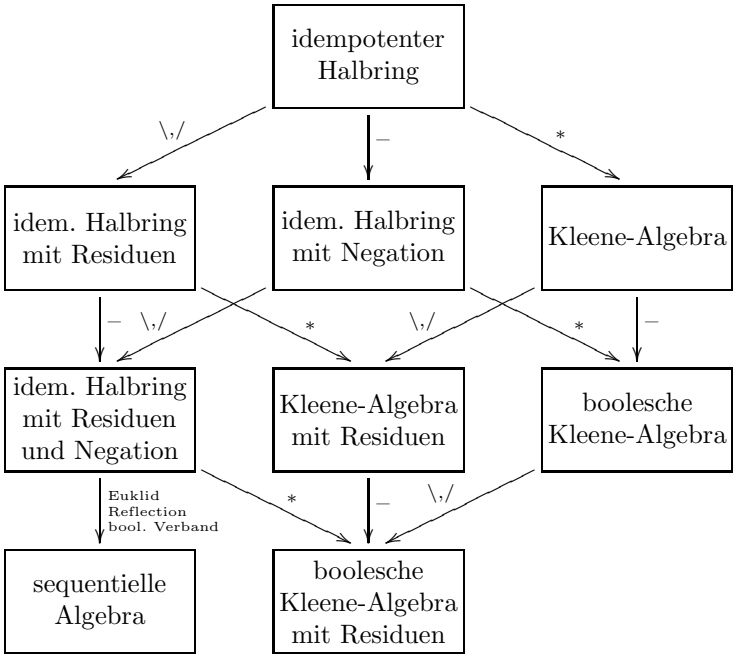

Abbildung 3.1: Beziehungen der verschiedenen algebraischen Strukturen

[1] Ein ausführlicher Beweis findet sich in [Jip02] sowie in Anhang A

B. von Karger beschreibt in seinen Arbeiten über Sequentielle Algebren und den Zeitdauer-Kalkül ([Kar96, Kar00]) auch Beobachtungsintervalle und Zeit-Diagramme. Im Folgenden sollen diese Begriffe definiert und in die bisher erläuterten algebraischen Strukturen eingebettet werden.
Ein *Beobachtungsintervall (observation interval)* ist ein Intervall der Zeit. B. von Karger nimmt ohne Einschränkung an, dass die Beobachtungsintervalle endlich, abgeschlossen und Intervalle reeller Zahlen sind.

Definition 3.3.2 (Zeit-Diagramm)
Sei Σ eine feste Menge von möglichen Zuständen eines Systems und B ein Beobachtungsintervall auf diesem System. Eine Funktion $x : B \to \Sigma$, welche das Verhalten eines Systems beschreibt, wird *Zeit-Diagramm (time diagram)* genannt.
Ein Zeit-Diagramm $y : B \to \Sigma$, bei dem B aus genau einem Punkt besteht, wird als *Einheit* bezeichnet. Die *linke Einheit* $\overleftarrow{x}$ eines Zeit-Diagramms $x : [a, b] \to \Sigma$ ist die Beschränkung des Beobachtungsintervalls auf den linken Rand, d.h. $\overleftarrow{x} : [a, a] \to \Sigma$ mit $\overleftarrow{x}(a) = x(a)$. Entsprechend ist die *rechte Einheit* $\overrightarrow{x}$ als die Einschränkung auf die rechte Grenze des Intervalls definiert, also $\overrightarrow{x} : [b, b] \to \Sigma$ mit $\overrightarrow{x}(b) = x(b)$.

Durch $\overleftarrow{\ }$ und $\overrightarrow{\ }$ sind auf Zeit-Diagrammen zwei unäre Operatoren gegeben. Zusätzlich kann eine sequentielle Komposition, also eine binäre Operation, definiert werden. Hierzu seien B_1, B_2 Beobachtungsintervalle, Σ eine Menge von Zuständen und x, y Zeit-Diagramme.

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

Durch diese Definition kann ein Halbring über der Menge aller Zeit-Diagramme konstruiert werden, indem man die Multiplikation komponentenweise auf die Potenzmenge erweitert (vgl. Kapitel 2). Genauer ist $TIME(\mathcal{B}, \Sigma) := (\mathcal{P}(X), \cup, ;, \emptyset, Id)$ der Halbring der Zeit-Diagramme, wobei Folgendes gilt:

$$\begin{array}{l} \mathcal{B} \text{ ist eine Menge von Beobachtungsintervallen,} \\ \Sigma \text{ ist eine Menge von möglichen Zuständen,} \\ X = \{x : (x : B \to \Sigma), B \in \mathcal{B}\}, \\ Id = \{x : x \in X, x \text{ ist Einheit}\}. \end{array}$$

Definiert man für eine Menge von Zeit-Diagrammen Y den $*$-Sternoperator $Y^* := \bigcup_{i \in \mathbb{N}} Y^i$, mit $Y^0 = Id$ und $Y^{i+1} = Y ; Y^i$, so kann man $TIME(\mathcal{B}, \Sigma)$ auch zu einer Kleene-Algebra erweitern. Ferner ist es möglich, in natürlicher Weise die Negation und die Residuen zu definieren. Zudem spricht B. von Karger auch von Beobachtungsräumen.

Definition 3.3.3 (Beobachtungsraum)
Eine Menge A zusammen mit zwei unären Operatoren $\overleftarrow{}$ und $\overrightarrow{}$, sowie einer binären Operation ; ist ein *Beobachtungsraum (observation space) Obs*, falls folgende Axiome erfüllt sind:

1. $x; y$ ist genau dann definiert, falls $\overrightarrow{x} = \overleftarrow{y}$ gilt.
2. Ist $x; y$ definiert, so gilt $\overleftarrow{x; y} = \overleftarrow{x}$ und $\overrightarrow{x; y} = \overrightarrow{y}$.
3. ; ist assoziativ.
4. Ist e eine Einheit, d.h.: $e = \overleftarrow{x}$ oder $e = \overrightarrow{x}$, dann gilt $\overleftarrow{e} = e = \overrightarrow{e}$.
5. $\overleftarrow{x}; x = x = x; \overrightarrow{x}$.
6. (Reflection) Ist $x; y$ eine Einheit, so auch $y; x$.
7. (Lokale Linearität) Gilt $x; y = x'; y'$, so existiert ein Zeit-Diagramm z, welches entweder ($x; z = x'$ und $y = z; y'$) oder ($x = x'; z$ und $z; y = y'$) erfüllt.

Es ist leicht nachzurechnen, dass $TIME(\mathcal{B}, \Sigma)$ einen Beobachtungsraum darstellt, falls man ähnlich wie bei der Komposition $\overleftarrow{}$ und $\overrightarrow{}$ auch auf Elementen der Potenzmenge definiert. Sei $Y \in \mathcal{P}(\{x : (x : B \to \Sigma), B \in \mathcal{B}\})$:

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

Eine Überprüfung zeigt, dass der Halbring der Zeit-Diagramme sowohl die Exchange-Regel, als auch die Euklidsche Ungleichung erfüllt (vgl. 3.3.1) und somit auch eine sequentielle Algebra bildet.

Kapitel 4

Intervalloperatoren

Intervalloperatoren sind in der Regel nützlich, um gefährliche Situationen einer Systemspezifikation, wie zum Beispiel eine unzulässige Zuweisung, zu beschreiben. Soll eine Situation nie erreicht werden, ist hierfür ein entsprechender Operator nötig. Grundsätzlich wird zwischen zwei Arten von Intervalloperatoren, den positiven und den negativen, unterschieden.
Die positiven vermögen Situationen zu beschreiben, an denen ein Zustand irgendwo, aber mindestens an einer Stelle, bzw. überall auftritt. Dadurch ist es auch möglich durch Negation Mengen zu beschreiben, an denen ein bestimmter Zustand nie auftritt. Algebraisch gesehen lassen sich diese Operatoren durch die Multiplikation charakterisieren.
Die negativen Intervalloperatoren hingegen werden durch die im letzten Kapitel vorgestellten Abtrennungsoperatoren definiert. Sie beschreiben Situationen an denen bei allen "Teilsituationen" bzw. an mindestens einer ein bestimmter Zustand gilt.
Im folgenden Abschnitt werden daher die Intervalloperatoren definiert, an einfachen Beispielen dargestellt und wichtige Eigenschaften über sie bewiesen. Für weitere Informationen seien hier die beiden Texte von B. von Karger [Kar00] und [Kar96] erwähnt.

4.1 Definitionen der Intervalloperatoren und einfache Beispiele

Definition 4.1.1 (Positive Intervalloperatoren)
Sei $H = (A, +, \cdot, 0, 1, \overline{\ })$ ein Halbring mit einer Negationsabbildung und $a \in A$. Dann sind die *positiven Intervalloperatoren* folgendermaßen definiert:

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

Betrachtet man diese Definitionen im Halbring $LAN(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, \mathbin{+\!\!+}, \emptyset, \varepsilon)$ über einem Zeichenvorrat Σ, so gilt $\top = \Sigma^* = \{a : a \in \Sigma^*\}$ und damit auch $\diamondsuit a = \Sigma^* \mathbin{+\!\!+} a \mathbin{+\!\!+} \Sigma^*$. Dies bedeutet, dass $\diamondsuit a$ jene Menge beschreibt, welche alle Wörter x enthält, die an einer beliebigen Stelle mindestens ein Wort aus a enthalten. Somit gilt

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

Der andere positive Intervalloperator $\boxplus a = \overline{\diamondsuit \overline{a}} = \overline{\Sigma^* \mathbin{+\!\!+} \overline{a} \mathbin{+\!\!+} \Sigma^*}$ beschreibt die Menge aller Wörter x, welche an keiner Stelle ein Teilwort enthalten, dass nicht in a ist. Dies bedeutet

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

Anders ausgedrückt bedeutet dies, dass jedes Teilwort von einem Element aus $\boxplus a$ ein Wort aus a ist. Da jedoch gilt, dass $\Sigma^* \mathbin{+\!\!+} \overline{a} \mathbin{+\!\!+} \Sigma^* = \Sigma^*$, falls $\varepsilon \in \overline{a}$, wird $\boxplus a$ in diesem Fall die leere Menge, d.h.

$$\boxplus a = \overline{\Sigma^* \mathbin{+\!\!+} \overline{a} \mathbin{+\!\!+} \Sigma^*} = \overline{\Sigma^*} = \emptyset, \text{ falls } \varepsilon \in \overline{a}.$$

Dieses Phänomen gilt jedoch nicht nur in formalen Sprachen, sondern kann allgemein in folgendem Lemma zusammengefasst werden.

Lemma 4.1.2
Sei $H = (A, +, \cdot, 0, 1, \overline{})$ ein idempotenter Halbring mit Negation und größtem Element $\top$. Dann gilt

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

Beweis:

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

□

Beschäftigen sich die positiven Intervalloperatoren mit der Beziehung zwischen einem beliebigen Element a und dem größten Element $\top$ bezüglich der Multiplikation, ist es auch von Interesse, wie sich a und $\top$ bezüglich den im letzten Kapitel vorgestellten Abtrennungsoperatoren verhalten.

Definition 4.1.3 (Negative Intervalloperatoren)
Sei $H = (A, +, \cdot, 0, 1, \backslash, /, \overline{})$ ein Halbring mit Residuen und Negation. Sei weiterhin $a \in A$. Dann sind die *negativen Intervalloperatoren* in folgender Weise definiert:

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

Bemerkung 1
Mit einfachen Berechnungen ergibt sich folgende Beziehung der negativen Intervalloperatoren zu Residuen:

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

Betrachtet man diese Definitionen wiederum im speziellen Halbring $LAN(\Sigma)$ über einem Alphabet Σ, lässt sich $\diamondminus a$ anschaulich erklären. In $LAN(\Sigma)$ beschreibt $a \lfloor b$ das Abschneiden von endständigen Teilwörtern von Elementen aus a und $b \rfloor a$ das Abschneiden von Präfixen (vgl. Paragraph 3.2). Aus diesem Grund beschreibt $\diamondminus a = \Sigma^* \rfloor a \lfloor \Sigma^*$ genau die Menge, welche die zusammenhängenden Teilwörter von Wörtern aus a enthält, also

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

Auf Grund dieses Wissens kann $\boxminus a$ folgendermaßen charakterisiert werden:

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

In Worten ausgedrückt enthält $\boxminus a$ all jene Wörter, deren Komposition mit beliebigen Wörtern wieder in a liegt. Ähnlich zu der oben gezeigten Eigenschaft von $\boxplus a$ kann man auch eine Beziehung zwischen 1 und $\boxminus a$ herstellen.

Lemma 4.1.4
Sei H wie in Definition 4.1.3 und zusätzlich auch idempotent, dann gilt

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

Beweis:

$$\begin{aligned} & 1 \leq \boxminus a \\ \Leftrightarrow \quad & 1 \leq \top \backslash a / \top \\ \Leftrightarrow \quad & \top \cdot 1 \cdot \top \leq a \\ \Leftrightarrow \quad & \top \leq a \end{aligned}$$

□

Aus den obigen Definitionen der Intervalloperatoren lassen sich zusammen mit den Rechenregeln über Residuen Beziehungen zwischen diesen und den Elementen 0 und $\top$ erklären.

Korollar 4.1.5
Es gilt:

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

4.2 Eigenschaften

Der Rest dieses Kapitels beschäftigt sich speziellen Eigenschaften der positiven und negativen Intervalloperatoren. Um den nachstehenden Abschnitt übersichtlicher zu gestalten, sei deshalb vorausgesetzt, dass $H = (A, +, \cdot, 0, 1, \backslash, /, \overline{\ })$ ein Abtrennungs-Halbring mit größtem Element $\top$ und $a, b \in A$ ist.
Zunächst stellt sich heraus, dass sämtliche Intervalloperatoren monoton und idempotent sind. Ferner verhalten sich je ein positiver als auch ein negativer Intervalloperator distributiv, die anderen dagegen konjunktiv. Diese Eigenschaften sollen in den folgenden Lemmata bewiesen werden.

Lemma 4.2.1 (Monotonie)
Sei $a \leq b$. Dann gilt:

(i) $\diamondsuit a \leq \diamondsuit b$

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

(iii) $\diamondsuit a \leq \diamondsuit b$

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

Beweis:

(i)

$$
\begin{aligned}
& \diamondsuit a \leq \diamondsuit b \\
\Leftrightarrow \quad & \{\text{Definition von } \diamondsuit\} \\
& \top \cdot a \cdot \top \leq \top \cdot b \cdot \top \\
\Leftarrow \quad & \{\text{Monotonie bzgl. der Multiplikation}\} \\
& a \cdot \top \leq b \cdot \top \\
\Leftarrow \quad & \{\text{Monotonie bzgl. der Multiplikation}\} \\
& a \leq b
\end{aligned}
$$

(ii)

$$
\begin{aligned}
& \boxplus a \leq \boxplus b \\
\Leftrightarrow \quad & \overline{\diamondsuit \overline{a}} \leq \overline{\diamondsuit \overline{b}} \\
\Leftrightarrow \quad & \diamondsuit \overline{b} \leq \diamondsuit \overline{a} \\
\overset{(i)}{\Leftarrow} \quad & \overline{b} \leq \overline{a} \\
\Leftrightarrow \quad & a \leq b
\end{aligned}
$$

(iii)

$$
\begin{aligned}
& \diamondsuit a \leq \diamondsuit b \\
\Leftrightarrow \quad & \{\text{Definition von } \diamondsuit\} \\
& \top \rfloor a \lfloor \top \leq \top \rfloor b \lfloor \top \\
\Leftarrow \quad & \{\text{Monotonie bzgl. der Abtrennungsoperatoren (3.2.4)}\} \\
& a \lfloor \top \leq b \lfloor \top \\
\Leftarrow \quad & \{\text{Monotonie bzgl. der Abtrennungsoperatoren (3.2.4)}\} \\
& a \leq b
\end{aligned}
$$

(iv) Analog zu (ii).

□

Lemma 4.2.2 (Idempotenz)
Es gilt:

(i) $\diamondsuit\diamondsuit a = \diamondsuit a$

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

(iii) $\diamondsuit\diamondsuit a = \diamondsuit a$

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

Beweis:

(i)

$$\begin{aligned}\diamondsuit\diamondsuit a &= \top \cdot \top \cdot a \cdot \top \cdot \top \\ &= \top \cdot a \cdot \top \\ &= \diamondsuit a\end{aligned}$$

(ii)

$$\begin{aligned}\boxplus\boxplus a &= \overline{\diamondsuit(\overline{\overline{\boxplus a}})} \\ &= \overline{\diamondsuit(\overline{\overline{\diamondsuit\overline{a}}})} \\ &= \overline{\diamondsuit(\diamondsuit\overline{a})} \\ &\overset{(i)}{=} \overline{\diamondsuit\overline{a}} \\ &= \boxplus a\end{aligned}$$

(iii)

$$\begin{aligned}&\diamondsuit\diamondsuit a \\ = \quad &\{\text{Definition von } \diamondsuit a\} \\ &(\top\rfloor((\top\rfloor a)\lfloor\top))\lfloor\top \\ = \quad &\{3.2.7\} \\ &\top\rfloor(((\top\rfloor a)\lfloor\top)\lfloor\top) \\ = \quad &\{3.2.6\} \\ &\top\rfloor((\top\rfloor a)\lfloor(\top\cdot\top)) \\ = \quad &\{3.2.7 \text{ und Idempotenz von } \top\} \\ &(\top\rfloor(\top\rfloor a))\lfloor\top \\ = \quad &\{3.2.6\} \\ &((\top\cdot\top)\rfloor a)\lfloor\top \\ = \quad &\{\text{Idempotenz von } \top\} \\ &(\top\rfloor a)\lfloor\top \\ = \quad &\{\text{Definition von } \diamondsuit a\} \\ &\diamondsuit a\end{aligned}$$

(iv) Analog zu (ii).

□

Lemma 4.2.3 (Distributivität)
Es gilt:

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

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

Beweis:

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

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

□

Lemma 4.2.4 (Konjunktivität)
Existiert neben dem $\sqcup$-Operator auch der $\sqcap$-Operator, so gilt:

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

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

Beweis:

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

(ii) Direkt aus 3.1.10.

□

Von besonderem Interesse bei Intervalloperatoren sind nicht nur ihre oben gezeigten fundamentalsten Eigenschaften, sondern auch, wie sie miteinander in Verbindung stehen. Auf Grund der Monotonie und der Distributivität bzw. der Konjunktivität liegt die Vermutung nahe, dass zwischen den Operatoren Galois-Verbindungen existieren. Denn Galois-Verbindungen haben allgemein die Eigenschaft, dass beide dazugehörigen Abbildungen monoton sind, die untere Adjungierte distributiert und die obere konjungiert. Und in der Tat gibt es einen solchen Zusammenhang.

Lemma 4.2.5
$\diamondsuit a \leq b \Leftrightarrow a \leq \boxplus b$ und $\diamondplus a \leq b \Leftrightarrow a \leq \boxminus b$ sind Galois-Verbindungen.

Beweis:

(i)

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

(ii)

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

□

Eine direkte Konsequenz aus den Galois-Verbindungen ist folgende Beziehung:

Lemma 4.2.6
Es gilt:

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

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

Beweis:

$$\begin{aligned}
& a \leq \overline{\diamondplus b} \\
\Leftrightarrow\ & \quad \{\text{Negation}\} \\
& \diamondplus b \leq \overline{a} \\
\Leftrightarrow\ & \quad \{\text{Galois-Verbindung (4.2.5)}\} \\
& b \leq \boxminus \overline{a}
\end{aligned}$$

$$
\begin{array}{ll}
\Leftrightarrow & \{\text{Definition von } \boxminus a\} \\
& b \leq \overline{\diamondminus \overline{a}} \\
\Leftrightarrow & \{\text{Negation}\} \\
& \diamondminus a \leq \overline{b}
\end{array}
$$

□

Nachdem der Zusammenhang der positiven und negativen Intervalloperatoren gezeigt wurde, stellt sich nun die Frage, ob man die positiven beziehungsweise die negativen Operatoren auch gegeneinander abschätzen kann. Die Galois-Verbindungen ergeben direkt eine mögliche Abschätzung, denn bei ihnen gelten immer die Kürzungsregeln. Weiter kann man aber auch die positiven und die negativen Intervalloperatoren mit sich selbst vergleichen. All dies führt zu folgenden Kern- und Hülleigenschaften dieser Operatoren.

Lemma 4.2.7 (Kern- und Hülleigenschaften von Intervalloperatoren)

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

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

(iii) $\diamondplus \boxminus a \leq a \leq \boxminus \diamondplus a$ (Kürzungsregel der Galois-Verbindung)

(iv) $\diamondminus \boxplus a \leq a \leq \boxplus \diamondminus a$ (Kürzungsregel der Galois-Verbindung)

Beweis:

(i)

$$
\begin{array}{ll}
& a \leq \diamondplus a \\
\Leftrightarrow & \{\text{Definition von } \diamondplus\} \\
& a \leq \top \cdot a \cdot \top \\
\Leftarrow & \{\text{Monotonie bzgl. der Multiplikation}\} \\
& \texttt{true}
\end{array}
$$

$$
\begin{array}{ll}
& \boxplus a \leq a \\
\Leftrightarrow & \{\text{Definition}\} \\
& \overline{\diamondplus \overline{a}} \leq a \\
\Leftrightarrow & \{\text{Negation}\} \\
& \overline{a} \leq \diamondplus \overline{a} \\
\Leftrightarrow & \{\text{erster Teil des Beweises}\} \\
& \texttt{true}
\end{array}
$$

(ii) Da $x\lfloor 1 = x = 1\rfloor x$, gilt:

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

$$
\begin{array}{ll}
 & \boxminus a \leq a \\
\Leftrightarrow & \quad \{\text{Definition von } \boxminus\} \\
 & \overline{\diamondminus \overline{a}} \leq a \\
\Leftrightarrow & \quad \{\text{Negation}\} \\
 & \overline{a} \leq \diamondminus \overline{a} \\
\Leftrightarrow & \quad \{\text{erster Teil des Beweises}\} \\
 & \texttt{true}
\end{array}
$$

(iii)

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

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

(iv) Analog zu (iii).

□

Zum Abschluss dieses Kapitels soll nun noch eine relativ kleine und leichte Eigenschaft des ersten positiven Intervalloperators gezeigt werden. Da diese jedoch im nächsten Kapitel benötigt wird, sei sie hier besonders herausgestellt.

Lemma 4.2.8

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

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

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

Beweis:

(i)

$$
\begin{array}{rcl}
x \cdot (\diamondminus a) & = & x \cdot (\top \cdot a \cdot \top) \\
 & \leq & \top \cdot \top \cdot a \cdot \top \\
 & = & \top \cdot a \cdot \top \\
 & = & \diamondminus a
\end{array}
$$

(ii) Analog zu (i).

(iii) Direkt aus (i) und (ii).

□

Kapitel 5

Ingenieurs-Induktion

In der Realität kommt es häufig vor, dass Maschinen oder Roboter sich ständig wiederholende Prozeduren bewerkstelligen. Soll die Korrektheit der von diesen geleisteten Arbeit bzw. des in den Maschinen verborgenen Computerprogramms gezeigt werden, beweist man in den meisten Fällen, dass im ersten und zweiten Durchlauf die Prozedur korrekt ist, und schließt daraus auf die globale Korrektheit. Im Allgemeinen kann diese Schlussfolgerung allerdings nicht als wahr angenommen werden und in der Tat ist sie auch in einigen Anwendungen falsch. Das bekannteste Gegenbeispiel für ein solches Phänomen ist wahrscheinlich die mathematische Beziehung $2^n \geq n^2$. Diese Gleichung ist für $n = 0, 1, 2$ korrekt, für $n = 3$ dagegen falsch. Im folgenden Abschnitt soll daher gezeigt werden, unter welchen Umständen es in Kleene-Algebren genügt, den Fall a und a^2 zu betrachten, um Eigenschaften auf dem kleinsten Fixpunkt a^* zu beweisen.

5.1 Lokale Linearität

Dabei stellt sich heraus, dass die lokale Linearität eine notwendige Voraussetzung ist, die man an eine solche Kleene-Algebra stellen muss. Da in der Literatur jedoch verschiedene Definitionen von lokaler Linearität zu finden sind, sei erwähnt, dass der hier eingeführte Begriff dem in [Kar00] von B. von Karger vorgestellten entspricht.

Definition 5.1.1 (Lokale Linearität)
Ein Halbring $(A, +, \cdot, 0, 1)$ mit Negation und Residuen heißt *lokal linear*, falls für alle $a, b, c \in A$ gilt:

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

Ein Beispiel für einen lokal linearen Halbring ist der der binären Relationen. Er wird folgendermaßen definiert: Sei $\mathcal{M}$ eine beliebige Grundmenge. Dann

ist $REL(\mathcal{M}) = (\mathcal{P}(\mathcal{M} \times \mathcal{M}), \cup, ;, \emptyset, Id)$ der idempotente Halbring der binären Relationen, wobei die Multiplikation elementweise und partiell definiert wird.

$$\begin{array}{rcl} (\mathcal{M} \times \mathcal{M}) \times (\mathcal{M} \times \mathcal{M}) & \rightarrow & \mathcal{M} \times \mathcal{M} \\ (a,b);(c,d) & \mapsto & \begin{cases} (a,d), \text{ falls } b = c \\ \text{undefiniert sonst.} \end{cases} \end{array}$$

Id stellt das neutrale Element der Multiplikation ; dar und ist somit $Id = \{(a,a) : a \in \mathcal{M}\}$. In dieser algebraischen Struktur gilt für $A, B \in \mathcal{P}(\mathcal{M} \times \mathcal{M})$:

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

wobei $A^{\smile} := \{(b,a) : (a,b) \in A\}$ ist. Daher folgt für alle $A, B, C \in \mathcal{P}(\mathcal{M} \times \mathcal{M})$:

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

und damit auch die lokale Linearität.

5.2 Ingenieurs-Induktion

Wie schon erwähnt, ist es begrenzt möglich, Eigenschaften von a^* in einer Kleene-Algebra zu beweisen, ohne diesen kleinsten Fixpunkt selbst betrachten zu müssen. Mit Definition 5.1.1 der lokalen Linearität lässt sich folgender "induktiver" Zusammenhang zwischen Eigenschaften von a^* und Eigenschaften von $1, a$ sowie a^2 herstellen.

Satz 5.2.1 (Ingenieurs-Induktion)
Sei $\mathcal{K}$ eine lokal lineare, boolesche Kleene-Algebra mit Residuen und sei weiter $b \leq \overline{\diamondsuit a}$.
Dann gilt

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

Anmerkung
Die Umkehrung $a^* \leq \overline{\diamondsuit b} \Rightarrow 1 + a + a \cdot a \leq \overline{\diamondsuit b}$ folgt ohne jegliche Voraussetzung direkt aus der Tatsache, dass $a^n \leq a^* \; \forall n \in \mathbb{N}$ ist.

Interessant hierbei ist mitunter, welche Eigenschaft der Ausdruck $\overline{\diamondsuit a}$ beschreibt. Betrachtet man diesen in den Beispielen $LAN(\Sigma)$ über einem Zeichenvorrat Σ und $REL(\mathcal{M})$ über einer Grundmenge $\mathcal{M}$, ergibt sich Folgendes:

(a) $\underline{LAN(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, \text{++}, \emptyset, \varepsilon)}$

Wie in Paragraph 3.1 gezeigt, beschreibt $\diamondsuit a$, $a \in \mathcal{P}(\Sigma^*)$ die Menge, welche alle Wörter enthält, die mindestens ein Teilwort, welches Element in a ist, besitzen. Demnach charakterisiert $\overline{\diamondsuit a}$ genau die Menge aller Wörter, die kein Teilwort besitzen, welches in a liegt. Mathematisch gesehen heißt dies:

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

Um die Ingenieurs-Induktion anwenden zu können, muss noch gezeigt werden, dass $LAN(\Sigma)$ lokal linear ist. Hierzu werden wieder einzelne Wörter betrachtet. Wie die Abtrennungsoperatoren auf $LAN(\Sigma)$ wirken, wurde bereits in Kapitel 3 erläutert.
Seien $a \in A, b \in B$ und $c \in C$ beliebige Wörter mit $A, B, C \in \mathcal{P}(\Sigma^*)$. Es sind drei Fälle zu unterscheiden.

(i) z.z.: $(A \text{++} B)\lfloor C \subseteq A \text{++} (B\lfloor C) \cup A\lfloor (C\lfloor B)$

- c ist Postfix von b, d.h. $\exists c_1 \in \Sigma^* \, : \, b = c_1 \text{++} c$
$$\begin{aligned}(a \text{++} b)\lfloor c &= (a \text{++} c_1 \text{++} c)\lfloor c \\ &= a \text{++} c_1 \\ &= a \text{++} ((c_1 \text{++} c)\lfloor c) \\ &= a \text{++} (b\lfloor c)\end{aligned}$$
- b ist Postfix von c, d.h. $\exists b_1 \in \Sigma^* \, : \, c = b_1 \text{++} b$
$$\begin{aligned}(a \text{++} b)\lfloor c &= (a \text{++} b)\lfloor (b_1 \text{++} b) \\ &= a\lfloor b_1 \\ &= a\lfloor ((b_1 \text{++} b)\lfloor b) \\ &= a\lfloor (c\lfloor b)\end{aligned}$$
- b ist kein Postfix von c und c keines von b
$(a \text{++} b)\lfloor c = \{\}$

(ii) z.z.: $A \text{++} (B\lfloor C) \subseteq (A \text{++} B)\lfloor C$

- c ist Postfix von b, d.h. $\exists c_1 \in \Sigma^* \, : \, b = c_1 \text{++} c$
$$a \text{++} (b\lfloor c) \overset{(i)}{=} (a \text{++} b)\lfloor c$$
- c ist kein Postfix von b
$$a \text{++} (b\lfloor c) = \{\}$$

(iii) z.z.: $A\lfloor (C\lfloor B) \subseteq (A \text{++} B)\lfloor C$

- b ist Postfix von c, d.h. $\exists b_1 \in \Sigma^* \, : \, c = b_1 \text{++} b$
$$a\lfloor (c\lfloor b) \overset{(i)}{=} (a \text{++} b)\lfloor c$$
- b ist kein Postfix von c
$a\lfloor (c\lfloor b) = \{\}$

Insgesamt ergibt sich also die lokale Linearität.

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

Da $LAN(\Sigma)$ eine boolesche Kleene-Algebra ist, auf der Residuen existieren, kann die Ingenieurs-Induktion angewendet werden. Diese beschreibt

allerdings weniger eine induktive Folgerung, als vielmehr eine Teilwörterbeziehung. Die Voraussetzung $b \leq \overline{\diamondsuit a}$ beschreibt, dass Elemente aus b keine Teilworte von Elementen aus a sind. $\varepsilon \cup a \cup a{+}{+}a \leq \overline{\diamondsuit b}$ bedeutet demnach, dass weder das leere Wort noch Elemente aus a noch Wörter aus $a{+}{+}a$ Teilworte von Elementen aus b sind. Wendet man Satz 5.2.1 an, so kann daraus geschlossen werden, dass keine Worte von a^* Teilworte in b sind.

(b) $\underline{REL(\mathcal{M}) = (\mathcal{P}(\mathcal{M} \times \mathcal{M}), \cup, ;, \emptyset, Id)}$
Zunächst sei erwähnt, dass $REL(\mathcal{M})$ ohne Probleme durch $A^* := \bigcup_{i=0}^{\infty} A^i$ $\forall A \subseteq \mathcal{M} \times \mathcal{M}$ zu einer Kleene-Algebra erweitert werden kann, welche ebenfalls mit $REL(\mathcal{M})$ bezeichnet wird. In dieser Kleene-Algebra der binären Relationen (und natürlich auch in dem entsprechenden Halbring) kann das größte Element in folgender Weise dargestellt werden:

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

Daher folgt für ein beliebiges Element $A \in \mathcal{P}(\mathcal{M} \times \mathcal{M})$ mit $A \neq \emptyset$ und $(a, b) \in A$ die sogenannte Tarski-Regel:

$$\diamondsuit A = \top; A; \top \geq \top; \{(a, b)\}; \top = \top.$$

Durch Negation dieser ergibt sich:

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

Aus diesem Grund kann man Satz 5.2.1 nur anwenden, falls $b = \emptyset$ oder $a = \emptyset$ ist. Im ersten Fall ist die Folgerung sehr einfach und nicht aussagekräftig, da $\overline{\diamondsuit b} = \overline{\diamondsuit \emptyset} = \overline{\emptyset} = \top$. Im anderen Fall gilt $a = \emptyset \Rightarrow a^* = Id$, so dass die Schlussweise der Ingenieurs-Induktion keine Folgerung mehr ist, da $Id \leq \overline{\diamondsuit b}$ vorausgesetzt wurde.

Dieses im zweiten Beispiel entstandene Phänomen kann allgemein zu folgender Bemerkung zusammengefasst werden.

Bemerkung 2
Sei $\mathcal{K}$ eine lokal lineare, boolesche Kleene-Algebra inklusive Residuen. Gilt hierbei

$$\diamondsuit x = \top \quad \forall x \in \mathcal{K}, x \neq 0,$$

so sind die Voraussetzungen der Ingenieurs-Induktion (5.2.1) nur für $a = 0$ oder $b = 0$ erfüllt. Für diese Fälle ist die Schlussweise trivial.

Bei der Betrachtung der Ingenieurs-Induktion für Elemente a mit $a \leq 1$ zeigt sich eine weitere Besonderheit. In diesem Fall wird weder die lokale Linearität noch die Eigenschaft $b \leq \overline{\diamondsuit a}$ als Voraussetzung benötigt. Auf Grund der Supremumseigenschaft der Addition ist dann $1 + a + a \cdot a = 1$ und es gilt nachstehendes Lemma:

Lemma 5.2.2
Ist $a \leq 1 \leq x$, so folgt $a^* \leq x$.

Beweis:

Mit der Horn-Regel ($*$-3) folgt:

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

Andererseits gilt nach ($*$-1), dass $1 \leq a^*$ ist.
Daraus folgt für alle $a \leq 1$: $a^* = 1$ und damit auch $a^* \leq x$.

□

Für $x = \overline{\diamondsuit b}$ ergibt sich eine sehr einfache Form der Ingenieurs-Induktion für Elemente kleiner gleich 1.
Um die allgemeine Ingenieurs-Induktion später übersichtlich und relativ kurz beweisen zu können, sind einige Vorüberlegungen nötig, die in folgenden zwei Sätzen mathematisch zusammengefasst sind.

Satz 5.2.3
In einer lokal linearen, booleschen Kleene-Algebra mit Residuen gilt:

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

Beweis:

(i)

$$\begin{array}{ll} & 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \leq & \quad \{\text{Lokale Linearität (5.1.1)}\} \\ & 1 \lfloor \top + (a^* \cdot a) \lfloor \top \\ = & \quad \{\text{Distributivität von } \lfloor \text{ (3.2.4)}\} \\ & (1 + a^* \cdot a) \lfloor \top \\ = & \quad \{a^* = 1 + a^* \cdot a \ (*\text{-}2)\} \\ & a^* \lfloor \top \end{array}$$

(ii)

$$\begin{array}{ll} & a^* \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{a^* = 1 + a^* \cdot a \ (*\text{-}2)\} \\ & (1 + a^* \cdot a) \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{\text{Distributivität von } \lfloor \text{ (3.2.4)}\} \\ & 1 \lfloor \top + (a^* \cdot a) \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{\text{Supremumseigenschaft}\} \\ & (a^* \cdot a) \lfloor \top \leq 1 \lfloor \top + a^* \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{\text{Fixpunkt-Definiton von } .^* \ (x^* = \mu_y : 1 + x \cdot y)\} \\ & ((\mu_y : 1 + a \cdot y) \cdot a) \lfloor \top \leq 1 \lfloor \top + (\mu_y : 1 + a \cdot y) \cdot (a \lfloor \top) \\ \Leftrightarrow & \quad \{2.2.1\} \\ & (\mu_y : a + a \cdot y) \lfloor \top \leq 1 \lfloor \top + (\mu_y : a \lfloor \top + a \cdot y) \end{array}$$

$$
\begin{array}{ll}
\Leftarrow & \{\mu\text{-Fusion}(2.2.3)\} \\
& \forall x : (a + a \cdot x)\lfloor\top \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftrightarrow & \{\text{Distributivität von } \lfloor\ (3.2.4)\} \\
& \forall x : a\lfloor\top + (a \cdot x)\lfloor\top \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftrightarrow & \{\text{Supremumseigenschaft}\} \\
& \forall x : (a \cdot x)\lfloor\top \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftrightarrow & \{\text{Lokale Linearität } (5.1.1)\} \\
& \forall x : a \cdot (x\lfloor\top) + a\lfloor(\top\lfloor x) \leq a\lfloor\top + a \cdot (x\lfloor\top) \\
\Leftarrow & \{\text{Monotonie bzgl. } +\} \\
& \forall x : a\lfloor(\top\lfloor x) \leq a\lfloor\top \\
\Leftrightarrow & \{3.2.9\} \\
& \texttt{true}
\end{array}
$$

In Teil (i) des Beweises fällt auf, dass die lokale Linearität nicht voll ausschöpft wird, d.h. es wird nur die Gleichung $a^* \cdot (a\lfloor\top) \leq (a^* \cdot a)\lfloor\top$, also die Euklidsche Ungleichung, benötigt. Daher ist die erste Abschätzung auch in algebraischen Strukturen gültig, in denen nur diese Euklidsche Ungleichung gilt, wie zum Beispiel in einer sequentiellen Algebra, die mit einem Kleene-Stern versehen ist.

□

Satz 5.2.4
In einer lokal linearen, booleschen Kleene-Algebra mit Residuen gilt:

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

Beweis:

$$
\begin{array}{ll}
& \diamondsuit a^* \\
= & \{\text{Definition von } \diamondsuit\} \\
& \top\rfloor(a^*\lfloor\top) \\
= & \{5.2.3\} \\
& \top\rfloor(1\lfloor\top + a^* \cdot (a\lfloor\top)) \\
= & \{\text{Distributivität von } \lfloor\ (3.2.4) \text{ und Definition von } \diamondsuit\} \\
& \diamondsuit 1 + \top\rfloor(a^* \cdot (a\lfloor\top)) \\
= & \{\text{Lokale Linearität } (5.1.1)\} \\
& \diamondsuit 1 + (a^*\rfloor\top)\rfloor(a\lfloor\top) + (\top\rfloor a^*) \cdot (a\lfloor\top) \\
= & \{3.2.9\} \\
& \diamondsuit 1 + \top\rfloor(a\lfloor\top) + (\top\rfloor a^*) \cdot (a\lfloor\top) \\
= & \{\text{Definition von } \diamondsuit \text{ und } 5.2.3\} \\
& \diamondsuit 1 + \diamondsuit a + (\top\rfloor 1 + (\top\rfloor a) \cdot a^*) \cdot (a\lfloor\top) \\
= & \{\text{Distributivität von } \lfloor\ (3.2.4)\} \\
& \diamondsuit 1 + \diamondsuit a + (\top\rfloor 1) \cdot (a\lfloor\top) + (\top\rfloor a) \cdot a^* \cdot (a\lfloor\top)
\end{array}
$$

$$
\begin{array}{ll}
= & \{\text{Anmerkung 5.2.5}\} \\
& \diamondsuit 1 + \diamondsuit a + (\top \rfloor a) \cdot a^* \cdot (a \lfloor \top) \\
\leq & \{a^* \leq 1 + \oplus a\} \\
& \diamondsuit 1 + \diamondsuit a + (\top \rfloor a) \cdot (1 + \oplus a) \cdot (a \lfloor \top) \\
= & \{\text{Distributivität von } \lfloor \text{ (3.2.4)}\} \\
& \diamondsuit 1 + \diamondsuit a + (\top \rfloor a) \cdot (a \lfloor \top) + (\top \rfloor a) \cdot \oplus a \cdot (a \lfloor \top) \\
\leq & \{4.2.8\} \\
& \diamondsuit 1 + \diamondsuit a + (\top \rfloor a) \cdot (a \lfloor \top) + \oplus a \\
\leq & \{\text{Lokale Linearität (5.1.1)}\} \\
& \diamondsuit 1 + \diamondsuit a + \top \rfloor (a \cdot a) \lfloor \top + \oplus a \\
= & \{\text{Definition von } \diamondsuit\} \\
& \diamondsuit 1 + \diamondsuit a + \diamondsuit (a \cdot a) + \oplus a \\
= & \{\text{Distributivität von } \diamondsuit \text{ (4.2.3)}\} \\
& \diamondsuit (1 + a + a \cdot a) + \oplus a
\end{array}
$$

□

Anmerkung 5.2.5

$$
\begin{array}{ll}
& (\top \rfloor 1) \cdot (a \lfloor \top) \\
\leq & \{\text{Lokale Linearität (5.1.1)}\} \\
& \top \rfloor (1 \cdot (a \lfloor \top)) \\
= & \{\text{Neutralität der 1}\} \\
& \top \rfloor (a \lfloor \top) \\
= & \{\text{Definition von } \diamondsuit\} \\
& \diamondsuit a
\end{array}
$$

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

Nachdem diese zwei Hilfssätze bewiesen wurden, kann der Beweis der Ingenieurs-Induktion, welche die Beziehung zwischen Eigenschaften von a^* und Eigenschaften auf $1, a$ und a^2 beschreibt, betrachtet werden.

Beweis von 5.2.1 (Ingenieurs-Induktion):

$$
\begin{array}{ll}
& 1 + a + a \cdot a \leq \overline{\oplus b} \text{ und } b \leq \overline{\oplus a} \\
\Leftrightarrow & \{\text{4.2.6 und Negation}\} \\
& \diamondsuit (1 + a + a \cdot a) \leq \overline{b} \text{ und } \oplus a \leq \overline{b} \\
\Leftrightarrow & \{\text{Supremumseigenschaft}\} \\
& \diamondsuit (1 + a + a \cdot a) + \oplus a \leq \overline{b} \\
\Rightarrow & \{5.2.4\} \\
& \diamondsuit a^* \leq \overline{b} \\
\Leftrightarrow & \{4.2.6\} \\
& a^* \leq \overline{\oplus b}
\end{array}
$$

□

Kapitel 6

Zeitdauer-Kalkül

Der Zeitdauer-Kalkül bietet die Möglichkeit, bei gegebenen Sicherheitsanforderungen an ein beliebiges System ein konkretes Design zu entwickeln und dessen Korrektheit zu beweisen. Zu diesem Zweck wird die im vorangegangenen Kapitel vorgestellte Ingenieurs-Induktion benötigt, so dass als Grundlage für die Entwicklung der Sicherheitsanforderungen und des Designs nur lokal lineare Kleene-Algebren in Frage kommen.
Doch bevor man sich dem Zeitdauer-Kalkül widmen kann, werden einige maßtheoretische Grundlagen benötigt, die zuvor vorgestellt werden.

6.1 Maße und Maßmengen

Um eine Sicherheitsanforderung an ein bestimmtes System stellen zu können, ist es unerlässlich, Eigenschaften dieses Systems in irgendeiner Art und Weise messen zu können. So sollte es zumindest möglich sein, die Zeitdauer oder aber auch andere Längeneigenschaften anzugeben. Eine Möglichkeit für eine solche Charakterisierung wird im Folgenden gegeben. Des Weiteren wird aufgezeigt, dass und wie Objekte mit denselben Eigenschaften zu sogenannten Maßmengen zusammengefasst werden können.

Definition 6.1.1
Seien X, Σ beliebige Mengen und $f : X \to \Sigma$ eine Funktion. Dann ist

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

die *Menge vom Maß σ unter f*.

Betrachtet man den Halbring $\mathcal{H}_X$ über der Menge X, dann ist $M^f_{=\sigma}$ ein Element aus diesem.
Anmerkung
Seien X, Σ, f wie in Definition 6.1.1. Ist f total definiert, so ist die Relation

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

eine Äquivalenzrelation und $M^f_{=\sigma}$, $\sigma \in \Sigma$ bilden die Äquivalenzklassen.

Beweis:

(i) Reflexivität

$$\begin{aligned} a \sim a &\Leftrightarrow f(a) = f(a) \\ &\Leftrightarrow \texttt{true} \end{aligned}$$

(ii) Symmetrie

$$\begin{aligned} a \sim b &\Leftrightarrow f(a) = f(b) \\ &\Leftrightarrow f(b) = f(a) \\ &\Leftrightarrow b \sim a \end{aligned}$$

(iii) Transitivität

$$\begin{aligned} a \sim b \wedge b \sim c &\Leftrightarrow f(a) = f(b) \wedge f(b) = f(c) \\ &\Rightarrow f(a) = f(c) \\ &\Leftrightarrow a \sim c \end{aligned}$$

(iv) $M^f_{=\sigma}$ sind die Äquivalenzklassen

$$\begin{aligned} a \sim b &\Leftrightarrow f(a) = f(b) \\ &\Rightarrow a, b \in M^f_{=f(a)} \\ a, b \in M^f_{=\sigma} &\Rightarrow f(a) = \sigma \wedge f(b) = \sigma \\ &\Rightarrow f(a) = f(b) \\ &\Leftrightarrow a \sim b \end{aligned}$$

□

Definition 6.1.2
Sei $(\Sigma, \leq)$ eine geordnete Menge, X eine Menge und $f : X \to \Sigma$ eine Funktion. Des Weiteren sei $\sigma \in \Sigma$ beliebig. Dann ist es möglich, weitere Maßmengen zu charakterisieren.

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

$M^f_{=\sigma}, M^f_{\leq\sigma}, M^f_{<\sigma}, M^f_{\geq\sigma}$ und $M^f_{>\sigma}$ werden als *Maßmengen unter f* bezeichnet. Eine direkte Konsequenz dieser Definitionen sind folgende Teilmengenbeziehungen:

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

Betrachtet man den Halbring $(\mathcal{P}(X), \cup, \cdot, \emptyset, 1)$ über einer Menge X, so sind die Maßmengen unter f Elemente aus diesem und lassen sich dementsprechend auch miteinander vereinigen und multiplizieren.

Beispiel 6 (Zeit-Halbringe)
In technischen Anwendungen wird häufig ein System über eine gewisse Zeit beobachtet. Um dies algebraisch mit Halbringen zu beschreiben, sind ein paar Überlegungen notwendig. Zeit kann man als linearen, eindimensionalen Raum auffassen, welcher in den meisten Anwendungen durch eine (Halb-)Gerade dargestellt wird. Daher kann dieser mit den reellen Zahlen $\mathbb{R}$ bzw. den positiven reellen Zahlen $\mathbb{R}^+$ identifiziert werden. Soll das System nur über einen bestimmten zusammenhängenden Zeitraum überwacht werden und fasst man die Zeit als $\mathbb{R}$ auf, so ist dieser Beobachtungszeitraum ein Intervall auf den reellen Zahlen. Daher bietet sich die Menge der Intervalle auf $\mathbb{R}$ als Grundmenge an, um hieraus dann später einen Halbring zu konstruieren. Sei also

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

In den meisten Anwendungen wird 0 als "Jetzt-Zeitpunkt" und werden die positiven Zahlen als Zeitpunkte in der Zukunft sowie die negativen als Punkte in der Vergangenheit interpretiert. Die Intervalle $[a, \infty] := [a, \infty)$ werden zu $\mathtt{Int}$ bzw. $\mathtt{Int}_0$ dazugenommen, da in technischen Anwendungen auch Beobachtungen eine Rolle spielen, die zu einem bestimmten Zeitpunkt a starten und kein Ende nehmen sollen. Sie sollen also bis zum Zeitpunkt "unendlich" fortgesetzt werden. Um einen Halbring über $\mathtt{Int}$ bzw. $\mathtt{Int}_0$ zu konstruieren, muss, wie oben beschrieben, eine Multiplikation auf diesen Grundmengen definiert werden. In diesem Fall bietet sich die Intervallkomposition an. Auf Grund der Tatsache, dass $\mathtt{Int}_0$ eine Teilmenge von $\mathtt{Int}$ ist, genügt es, die Komposition auf $\mathtt{Int}$ zu definieren. Im Weiteren wird meistens nur der Halbring über $\mathtt{Int}$ betrachtet, da der andere ein Teilhalbring von jenem über $\mathtt{Int}$ ist und daher durch diesen schon genau beschrieben wird.

$$\begin{aligned} ;: \mathtt{Int} \times \mathtt{Int} &\to \mathtt{Int} \\ [a,b];[c,d] &= \begin{cases} [a,d], \text{ falls } b = c \\ \text{undefiniert sonst.} \end{cases} \end{aligned}$$

Damit ergibt sich jeweils ein Halbring über $\mathtt{Int}$ und über $\mathtt{Int}_0$. Diese beiden werden im Folgenden auch als *Zeit-Halbringe* bezeichnet.

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

Hierbei ist $1_{\mathtt{Int}} = \{[a,a] : a \in \mathbb{R}_\infty\}$ bzw. $1_{\mathtt{Int}_0} = \{[a,a] : a \in \mathbb{R}_\infty, a \geq 0\}$ und bildet somit das neutrale Element bezüglich der Multiplikation. Zur Vervollständigung des Beispiels werden noch zwei typische Funktionen und Maßmengen über diesen angegeben:

(i) Die erste Funktion liefert die Länge eines beliebigen Intervalls.

$$\begin{aligned} L : \texttt{Int} &\to \mathbb{R}_\infty \\ [a,b] &\mapsto \begin{cases} b-a & \text{, falls } a,b \in \mathbb{R} \\ \infty & \text{, falls } a \in \mathbb{R}, b = \infty \\ 0 & \text{, falls } a = b = \infty. \end{cases} \end{aligned}$$

$M^L_{=30}$ beschreibt dann genau die Menge von Intervallen, welche die Länge 30 haben.

(ii) Im zweiten Beispiel sei eine beliebige Teilmenge N aus $\mathbb{R}_\infty$ gegeben.

$$\begin{aligned} \chi_N : \mathbb{R} &\to \{0,1\} \\ x &\mapsto \chi_N(x) = \begin{cases} 1 & \text{, falls } x \in N \\ 0 & \text{, falls } x \notin N, \end{cases} \\ F : \texttt{Int} &\to \mathbb{R}_\infty \\ [a,b] &\mapsto \int_a^b \chi_N(t)\,dt. \end{aligned}$$

Hierbei bedeutet $\int$ das normale Lebesgue-Integral. $M^F_{<4}$ beschreibt die Menge von Intervallen $[a,b]$ mit $\int_a^b \chi_N(t)\,dt < 4$.

Soweit es die Eindeutigkeit zulässt, werden im Folgenden die oberen Indizes bei Maßmengen, welche die Funktionen näher beschreiben, einfach weggelassen. Des Weiteren seien, sofern nicht anders angegeben, X, Σ Mengen, X mit einer Multiplikation versehen, $\mathcal{H}_X$ der Halbring über X und $f : X \to \Sigma$ eine Funktion. Der Rest dieses Paragraphen beschäftigt sich mit Eigenschaften von Maßmengen über f.

Satz 6.1.3
Sei $(\Sigma, +, 0_\sigma)$ ein partielles Monoid, $(\Sigma, \leq)$ eine geordnete Menge und $f : X \to \Sigma$ ein Homomorphismus, d.h. $f(a \cdot b) = f(a) + f(b)\ \forall a, b \in X$, sofern $a \cdot b$ definiert ist. Dann gilt für $x, y \in \Sigma$:

(i) Ist f surjektiv, so folgt $1 \in M_{=0_\sigma}$.

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

(iii) Ist $+$ monoton, d.h. $a \leq b \Rightarrow a + c \leq b + c$ und $a \leq b \Rightarrow c + a \leq c + b$, $\forall a, b, c \in \Sigma$, so gilt auch

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

für einen beliebigen Vergleichsoperator $op \in \{\leq, <, \geq, >\}$.

Beweis:

(i) Sei $a \in X$.

$$\begin{aligned} & f(a) = f(1 \cdot a) = f(1) + f(a) \\ \Rightarrow \quad & f(1) = 0_\sigma, \text{ falls } f \text{ surjektiv} \\ \Rightarrow \quad & 1 \in M_{=0_\sigma} = \{x \,:\, x \in X, f(x) = 0_\sigma\} \end{aligned}$$

(ii)

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

(iii)

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

Für die anderen Vergleichsoperatoren erfolgen die Beweise analog.

□

Definition 6.1.4
Sind die Maßmengen unter zwei Funktionen $f, g : X \to \Sigma$ gegeben und sind $op, \widetilde{op} \in \{=, \leq, <, \geq, >\}$ zwei Vergleichsoperatoren. Dann ist

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

eine *Maßmenge unter f und g.*
Offensichtlich gilt:

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

Beispiel 7
Seien die Funktionen $L, F : \texttt{Int} \to \mathbb{R}_\infty$ und $\chi_N : \mathbb{R} \to \{0, 1\}$ wie in Beispiel 6 gegeben.

$$M^L_{\leq 30} \cap M^F_{>4} = \{[a, b] \,:\, [a, b] \in \texttt{Int}, L([a, b]) \leq 30, F([a, b]) > 4\}$$

beschreibt genau die Intervalle, deren Länge kleiner gleich 30 und deren Lebesgue Integral über χ_N echt größer 4 ist.

Lemma 6.1.5
Ist $(\Sigma, \leq)$ eine geordnete Menge, so gilt:

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

Beweis:

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

□

Lemma 6.1.6
Ist $(\Sigma, \leq)$ eine total geordnete Menge, d.h. $\forall x, y \in \Sigma : x \leq y \vee y \leq x$, so sind gewisse Maßmengen zueinander komplementär.

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

Beweis:

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

Die zweite Gleichung lässt sich analog beweisen.

□

Lemma 6.1.7
Ist $(\Sigma, \leq)$ eine geordnete Menge und besitzt Σ ein kleinstes Element $\perp$, dann gilt

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

Also ist $M_{\geq \perp}$ das größte Element in $\mathcal{P}(X)$ bezüglich der Teilmengenrelation.

Beweis:

Da $\perp$ das kleinste Element in Σ ist, gilt $f(a) \geq \perp \quad \forall a \in X$.

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

□

Korollar 6.1.8
Dual zu 6.1.7 gilt

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

falls $(\Sigma, \leq)$ eine geordnete Menge mit größtem Element $\top$ ist.

Korollar 6.1.9
Falls f ein Homomorphismus ist und Σ eine geordnete Menge mit kleinstem Element 0, folgt aus 6.1.5 und 6.1.7 unmittelbar

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

und damit auch

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

Beweis:

(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)

$$\begin{aligned} & \diamondsuit M_{<x} \\ = \quad & \overline{X \backslash \overline{M_{<x}}/X} \\ \overset{6.1.6}{=} \quad & \overline{X \backslash M_{\geq x}/X} \\ \overset{(i)}{\subseteq} \quad & \overline{M_{\geq x}} \\ \overset{6.1.6}{=} \quad & M_{<x} \end{aligned}$$

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

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

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

□

Anmerkung
Da $\mathbb{R}^+$ total geordnet ist und auch ein kleinstes Element besitzt, gilt für alle Maßmengen unter $f : X \to \mathbb{R}^+$ das soeben vorgestellte Korollar, also insbesondere auch für die Maßmengen unter den im Beispiel 6 eingeführten Funktionen L und F.

6.2 Die Gasleitung - Zeitdauer-Kalkül anhand eines Beispiels

Ein in der Literatur viel beschriebenes, praktisches Beispiel für den Zeitdauer-Kalkül ist die Beobachtung einer Gasleitung (im Englischen häufig mit "gas burner" bezeichnet). So beschreiben Z. Chaochen, C.A.R. Hoare und A.P. Ravn in [CHR91] dieses Gasleitungsbeispiel. B. von Karger bringt es in [Kar00] mit Beobachtungsräumen in Verbindung. Im Folgenden wird dieses wohl bekannteste Beispiel vorgestellt und an ihm der Zeitdauer-Kalkül gezeigt.

6.2.1 Das Gasleitungs-Problem

In der Praxis kommt es vor, dass an Ventilen und am Ende einer Gasleitung Gas austritt, welches nicht verbrannt wird. Dies ist zwar unerwünscht, lässt sich aber in der Realität nicht vermeiden. Wünschenswert wäre es daher, ein System zu entwickeln, welches die Gasleitung über eine gewisse Zeit überwacht und bei Bedarf, also zum Beispiel, wenn zu viel Gas austritt, die Gaszufuhr unterbricht. Ein Ingenieur sollte daher in der Lage sein, für ein solches System Sicherheitsanforderungen zu formulieren. Im Gasleitungsbeispiel könnte das zum Beispiel die in [CHR91] vorgestellte Bedingung sein.

> "In jedem beobachteten Zeitintervall, das länger als eine Minute ist, sollte an der Gasleitung in nicht mehr als einem Zwanzigstel der Zeit Gas austreten." (Req1)

Dies ist zwar sicherlich eine mögliche Anforderung, aber unter Umständen etwas unglaubwürdig, da man folgende falsche Argumentation führen kann.
Man betrachte ein Zeitintervall, welches 20 Stunden andauert. In diesem könnte es passieren, dass eine Stunde lang ununterbrochen Gas austritt, ohne dass das Sicherheitssystem Alarm schlagen würde.
Der Fehler dieser Argumentation liegt selbstverständlich daran, dass man auch die Teilintervalle des 20-Stunden-Intervalls betrachten muss.
Gäbe es ein 60-Minuten-Intervall, in dem, wie oben angenommen, ununterbrochen Gas ausströmt, so würde die Sicherheitsanforderung (Req1) verletzt sein, da nicht nur in einem Zwanzigstel der Zeit (3 Minuten), sondern immer (60 Minuten) Gas austritt. Entsprechend müssen sämtliche Teilintervalle des "Oberintervalls", welche länger als 60 Sekunden sind, betrachtet werden.
Um solche Probleme von Anfang an zu umgehen, bietet sich die von B. von

Karger ([Kar00]) vorgestellte Sicherheitsanforderung an, die nicht Intervalle einer Mindestlänge als Objekte verwenden, sondern solche mit einer maximalen Dauer.

> "Ein Gasleitungssystem ist genau dann sicher, falls in jedem Beobachtungsintervall $[a, b]$, welches kürzer als 30 Sekunden ist, maximal 4 Sekunden lang Gas austritt." (Req2)

Diese Bedingung wird im Folgenden näher betrachtet und algebraisch beschrieben.

6.2.2 Algebraische Charakterisierung

(Req2) zeigt, dass diese Sicherheitsanforderung eng mit den Zeit-Halbringen in Verbindung steht. Für die mathematische Beschreibung werden zwei Funktionen benötigt. Die eine, welche Längen von Intervallen berechnet, wurde in Beispiel 6 bereits vorgestellt. Die andere, welche die austretende Menge Gas misst, muss noch definiert werden. Wählt man allerdings $N \subseteq \mathbb{R}_\infty$ als diejenige Menge von Zeitpunkten, zu denen Gas austritt, so kann man eine Funktion $Leak$ analog zu der oben vorgestellten Funktion F definieren.

$$\begin{aligned} Leak : \texttt{Int} &\to \mathbb{R} \\ [a, b] &\mapsto \int_a^b \chi_N(t)\, dt. \end{aligned}$$

Hieraus ergibt sich folgende zu (Req2) äquivalente algebraische Sicherheitsanforderung:

$$\begin{aligned} & \text{Das Gasleitungssystem ist sicher} \\ \Leftrightarrow \quad & \nexists b \in \texttt{Int} : L(b) < 30 \wedge Leak(b) > 4 \qquad \text{(Req)} \\ \Leftrightarrow \quad & \forall a \in \texttt{Int} : L(a) \geq 30 \vee Leak(a) \leq 4. \end{aligned}$$

6.2.3 Der Zeitdauer-Kalkül anhand des Beispiels

Die Intervalloperatoren über $\mathcal{H}_{\texttt{Int}}$ bzw. $\mathcal{H}_{\texttt{Int}_0}$ zeigen, dass $\boxplus M$ für eine Maßmenge M genau jene Intervalle beschreibt, welche in M liegen und deren Teilintervalle ebenfalls in M enthalten sind. Daher ist es möglich, die Bedingung (Req) mit Intervalloperatoren in $\mathcal{H}_{\texttt{Int}}$ auszudrücken. Eine mögliche Spezifikation des Sicherheitssystems ist demnach

$$\mathtt{g}as\_spec = \boxplus \overline{b}, \quad \text{wobei } b := M^L_{<30} \cap M^{Leak}_{>4}.$$

Will man ein konkretes Sicherheitssystem aufbauen, sollte dessen Verhalten eine Teilmenge von $\mathtt{g}as\_spec$ sein. Da Intervalle, die "in der Vergangenheit liegen", uninteressant sind, kann man sich im Folgenden auf $\texttt{Int}_0$ beschränken.

Interessant wird ein solches System genau dann, wenn es eine bestimmte Routine immer wieder ausführen kann. Um diese Wiederholung zu charakterisieren, kann zu einer Kleene-Algebra übergegangen werden (vgl. Kapitel 2). Im Folgenden wird also anstelle von $\mathcal{H}_{\mathtt{Int}_0}$ die Kleene-Algebra $\mathcal{H}_{\mathtt{Int}_0} = (\mathcal{P}(\mathtt{Int}_0), \cup, ;, \emptyset, 1, ^*)$ betrachtet, wobei folgende Beziehung für $a \in \mathcal{P}(\mathtt{Int}_0)$ gegeben ist:

$$\begin{aligned} a^0 &= 1, \\ a^{i+1} &= a^i; a, \\ a^* &= \bigcup_{i \geq 0} a^i. \end{aligned}$$

Sei ein konkretes Design des Kontrollsystems in folgender Weise gegeben:

$$\mathtt{gas\_}design = a^*, \quad \text{wobei } a := M^L_{=30} \cap M^{Leak}_{<2}.$$

Dieses Design ist von besonderem Interesse, da es sich im Gegensatz zu gas_spec nur mit Intervallen einer exakten Länge beschäftigt. Daher wäre es leicht möglich, ein automatisches System aufzubauen, welches ständig Intervalle von exakt 30 Sekunden Länge beobachtet. Um zu zeigen, dass es sich bei gas_design um ein sinnvolles, korrektes Design handelt, müssen folgende zwei Punkte bewiesen werden.

(i) $\mathtt{gas\_}design \subseteq \mathtt{gas\_}spec$.

(ii) Das System läuft ab einem Startpunkt x im Falle keiner Sicherheitsverletzung auf unbestimmte Zeit, d.h.: $\forall x \in \mathbb{R}_\infty, x \geq 0 : [x, \infty] \in \lim_{n \to \infty} (M^L_{=30})^n$.

Beweis:

(i) (a) z.z.: $\mathcal{H}_{\mathtt{Int}_0}$ ist lokal linear.
Betrachtet man die Abtrennungsoperatoren in $\mathtt{Int}_0$, so ergibt sich für $[a,b], [c,d] \in \mathtt{Int}_0$ folgende Beziehung:

$$[a,b] \lfloor [c,d] = \begin{cases} [a,c] & \text{, falls } a \leq c \text{ und } b = d \\ \{\} & \text{, sonst.} \end{cases}$$

Also haben die Abtrennungsoperatoren ähnlich wie bei der Kleene-Algebra der formalen Sprachen (vgl. Kapitel 5) eine abschneidende Eigenschaft. Demzufolge kann der lokale Linearitätsbeweis von $\mathcal{H}_{\mathtt{Int}_0}$ äquivalent zu dem von $LAN(\Sigma)$ geführt werden.

(b) Da $\mathcal{H}_{\mathtt{Int}_0}$ lokal linear ist, genügt es entsprechend der Ingenieurs-Induktion Folgendes für Elemente $a, b \in \mathcal{P}(\mathtt{Int}_0)$ zu zeigen:

(1) $1 \cup a \cup a; a \subseteq \overline{\diamondsuit b} \overset{4,2,6}{\Leftrightarrow} \diamondsuit(1 \cup a \cup a; a) \subseteq \overline{b}$

(2) $b \subseteq \overline{\diamondsuit a}$

zu (1):

$$
\begin{array}{ll}
 & \diamondsuit(1 \cup a \cup a; a) \\
= & \quad \{\text{Definition von } a\} \\
 & \diamondsuit(1 \cup (M^L_{=30} \cap M^{Leak}_{<2}) \\
 & \cup (M^L_{=30} \cap M^{Leak}_{<2}); (M^L_{=30} \cap M^{Leak}_{<2})) \\
\subseteq & \quad \{\text{Teilmengenbeziehung}\} \\
 & \diamondsuit(1 \cup M^{Leak}_{<2} \cup M^{Leak}_{<2}; M^{Leak}_{<2}) \\
\subseteq & \quad \{\text{Monotonie, 6.1.3}\} \\
 & \diamondsuit(M^{Leak}_{=0} \cup M^{Leak}_{<2} \cup M^{Leak}_{<2}; M^{Leak}_{<2}) \\
\subseteq & \quad \{6.1.3\} \\
 & \diamondsuit(M^{Leak}_{=0} \cup M^{Leak}_{<2} \cup M^{Leak}_{<(2+2)}) \\
\subseteq & \quad \{\text{Teilmengenbeziehung (6.1.5)}\} \\
 & \diamondsuit M^{Leak}_{<4} \\
= & \quad \{6.1.9\} \\
 & M^{Leak}_{<4} \\
\subseteq & \quad \{\text{Teilmengenbeziehung}\} \\
 & M^{Leak}_{\leq 4} \\
= & \quad \{\text{Negation (6.1.6)}\} \\
 & \overline{M^{Leak}_{>4}} \\
\subseteq & \quad \{\text{Teilmengenbeziehung}\} \\
 & \overline{M^L_{<30} \cap M^{Leak}_{>4}} \\
= & \quad \{\text{Definition von b}\} \\
 & \overline{b}
\end{array}
$$

zu (2):

$$
\begin{array}{ll}
 & \diamondsuit a \\
= & \quad \{\text{Definition von } a\} \\
 & \diamondsuit(M^L_{=30} \cap M^{Leak}_{<2}) \\
\subseteq & \quad \{\text{Monotonie und Teilmengenbeziehung}\} \\
 & \diamondsuit M^L_{=30} \\
= & \quad \{\text{Definition von } \diamondsuit\} \\
 & \mathtt{Int}_0; M^L_{=30}; \mathtt{Int}_0 \\
= & \quad \{6.1.7\} \\
 & M^L_{\geq 0}; M^L_{=30}; M^L_{\geq 0} \\
\subseteq & \quad \{6.1.3\} \\
 & M^L_{\geq 30} \\
= & \quad \{\text{Negation (6.1.6)}\} \\
 & \overline{M^L_{<30}} \\
\subseteq & \quad \{\text{Teilmengenbeziehung}\} \\
 & \overline{M^L_{<30} \cap M^{Leak}_{>4}} \\
= & \quad \{\text{Definition von } b\} \\
 & \overline{b}
\end{array}
$$

(ii) $\forall x \in \mathbb{R}_\infty$ mit $x \geq 0$ gilt:

$$\begin{aligned}[x,\infty] &= [x,x+30];[x+30,\infty] \\ &= [x,x+30];[x+30,x+60];[x+60,\infty] \\ &= \ldots\end{aligned}$$

Also lässt sich $[x,\infty]$ in ein Produkt umformen.

$$\forall x \in \mathbb{R}_\infty, x \geq 0 \,:\, [x,\infty] = \prod_{i \in \{k \cdot 30 \,:\, k \in \mathbb{N}_\infty\}} [x+i, x+i+30]$$

Da jedoch für alle Intervalle dieser Form $L([x+i,x+i+30]) = 30$ gilt, folgt, dass $[x+i,x+i+30] \in M^L_{=30}$ und damit

$$[x,\infty] \in \lim_{n\to\infty} (M^L_{=30})^n \quad \forall x \in \mathbb{R}_\infty, x \geq 0.$$

□

6.3 Zeitdauer-Kalkül

Zum Schluss dieses Kapitels wird noch die vorige Korrektheitsaussage in einer sehr allgemeinen Version dargestellt.

Satz 6.3.1 (Zeitdauer-Kalkül)
Sei $\mathcal{H}_X = (\mathcal{P}(X), \cup, \cdot, 0, 1, ^*)$ eine lokal lineare Kleene-Algebra über einer Menge X, Σ_1 eine total geordnete Menge, $(\Sigma_2, +, 0)$ ein Monoid mit kleinstem Element 0, $f_i : X \to \Sigma_i$ Homomorphismen mit $i \in \{1,2\}$, f_2 surjektiv und $A_j, B_k \subseteq X$, $j \in J$, $k \in K$ beliebige Elemente aus $\mathcal{P}(X)$. Ist $x \in \Sigma_1$ und $y \in \Sigma_2$, so gilt mit $a := M^{f_1}_{=x} \cap M^{f_2}_{<y} \cap A_j$ und $b := M^{f_1}_{<x} \cap M^{f_2}_{>(y+y)} \cap B_k$:

$$a^* \leq \overline{\diamondsuit b} = \boxplus \overline{b}.$$

Beweis:

Obwohl der Beweis fast identisch zu demjenigen im vorhergehenden Abschnitt ist, soll er hier nochmal gezeigt werden.
Da $\mathcal{H}_X$ lokal linear ist, reicht es entsprechend der Ingenieurs-Induktion zu zeigen, dass Folgendes gilt:

(1) $1 + a + a \cdot a \leq \overline{\diamondsuit b} \overset{4.2.6}{\Leftrightarrow} \diamondsuit(1 + a + a \cdot a) \leq \overline{b}$

(2) $b \leq \overline{\diamondsuit a}$

zu (1):

$$\begin{aligned} & \diamondsuit(1 + a + a \cdot a) \\ = \quad & \{\text{Definition von } a\} \\ & \diamondsuit(1 + (M^{f_1}_{=x} \cap M^{f_2}_{<y} \cap A_j) \\ & +(M^{f_1}_{=x} \cap M^{f_2}_{<y} \cap A_j) \cdot (M^{f_1}_{=x} \cap M^{f_2}_{<y} \cap A_j)) \\ \leq \quad & \{\text{Teilmengenbeziehung}\} \\ & \diamondsuit(1 + M^{f_2}_{<y} + M^{f_2}_{<y} \cdot M^{f_2}_{<y}) \end{aligned}$$

$$
\begin{array}{lll}
\leq & & \{\text{Monotonie, 6.1.3}\} \\
 & \diamondsuit(M^{f_2}_{=0} + M^{f_2}_{<y} + M^{f_2}_{<y} \cdot M^{f_2}_{<y}) & \\
\leq & & \{6.1.3\} \\
 & \diamondsuit(M^{f_2}_{=0} + M^{f_2}_{<y} + M^{f_2}_{<(y+y)}) & \\
\leq & & \{\text{Teilmengenbeziehung (6.1.5)}\} \\
 & \diamondsuit M^{f_2}_{<(y+y)} & \\
= & & \{6.1.9\} \\
 & M^{f_2}_{<(y+y)} & \\
\leq & & \{\text{Teilmengenbeziehung}\} \\
 & M^{f_2}_{\leq(y+y)} & \\
= & & \{\text{Negation (6.1.6)}\} \\
 & \overline{M^{f_2}_{>(y+y)}} & \\
\leq & & \{\text{Teilmengenbeziehung}\} \\
 & \overline{M^{f_1}_{<x} \cap M^{f_2}_{>(y+y)} \cap B_k} & \\
= & & \{\text{Definition von b}\} \\
 & \overline{b} &
\end{array}
$$

zu (2):

$$
\begin{array}{lll}
 & \diamondsuit a & \\
= & & \{\text{Definition von } a\} \\
 & \diamondsuit M^{f_1}_{=x} \cap M^{f_2}_{<y} \cap A_j & \\
\leq & & \{\text{Monotonie und Teilmengenbeziehung}\} \\
 & \diamondsuit M^{f_1}_{=x} & \\
= & & \{\text{Definition von } \diamondsuit\} \\
 & X \cdot M^{f_1}_{=x} \cdot X & \\
= & & \{6.1.7\} \\
 & M^{f_1}_{\geq 0} \cdot M^{f_1}_{=x} \cdot M^{f_1}_{\geq 0} & \\
\leq & & \{6.1.3\} \\
 & M^{f_1}_{\geq x} & \\
= & & \{\text{Negation (6.1.6)}\} \\
 & \overline{M^{f_1}_{<x}} & \\
\leq & & \{\text{Teilmengenbeziehung}\} \\
 & \overline{M^{f_1}_{<x} \cap M^{f_2}_{>(y+y)} \cap B_k} & \\
= & & \{\text{Definition von } b\} \\
 & \overline{b} &
\end{array}
$$

Hierbei ist die Wahl der Mengen A_j, B_k absolut unerheblich, d.h. man kann sowohl Maßmengen über beliebigen Funktionen als auch jede andere beliebige Teilmenge von $\mathcal{P}(X)$ wählen.

□

6.4 Weitere Anwendungen für den Zeitdauer-Kalkül

Der Zeitdauer-Kalkül kann für die unterschiedlichsten Anwendung verwendet werden. Aus diesem Grund soll an dieser Stelle ein kurzer Überblick über einige weitere Beispiele gegeben werden.

(i) Identisch zu dem ausführlich vorgestellten Beispiel der Gasleitung können auch Sicherheitsanforderungen an Bahnschranken oder Aufzüge gestellt werden. So sollte zum Beispiel eine Bahnschranke mindestens 60 Sekunden vor dem Eintreffen eines Zugs an dem Übergang geschlossen sein. Eine Anforderung an Lifts, wäre zum Beispiel folgende:

> "Ein Aufzug sollte Personen, die ihn benutzen wollen, nie länger als 5 Minuten warten lassen."

(ii) Ein anderes Beispiel kann über der Pfad-Kleene-Algebra $PAT(V) = (\mathcal{P}(V^*), \cup, \bowtie, \emptyset, V^{\leq 1}, \rightsquigarrow)$ (vgl. Beispiel 3) konstruiert werden. Sind den Kanten auch noch Gewichte zugeordnet, d.h. es existiert eine Funktion $w : E \to \mathbb{N}$, wobei $E \subseteq V^2$ die Kantenmenge des Graphen ist, so ist es möglich, zwei weitere Funktionen zu charakterisieren.
Seien $u, v \in V, t \in V^*$

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

Hierbei beschreibt die Funktion l die Länge eines Kantenzuges und $weight$ ordnet jedem ein spezifisches Gewicht zu.
Der für den Zeitdauer-Kalkül benötigte Intervalloperator $\overline{\diamondsuit P}$, wobei P eine Menge von Pfaden ist, beschreibt genau jene Menge von Wegen, die keine Teilpfade besitzen, die in P liegen.
$a := M^l_{=x} \cap M^{weight}_{<y}$ definiert jene Menge, welche die Kantenzüge enthält, die genau aus x Knoten bestehen und deren spezifisches Gewicht kleiner y ist. Dementsprechend beschreibt $b := M^l_{<x} \cap M^{weight}_{>(y+y)}$ die Menge aller Pfade mit weniger als x Knoten und einem Gewicht größer als $2y$.
Der Zeitdauerkalkül besagt, dass $a^* = \bigcup_{i \in \mathbb{N}} a^i$, also der kleinste Fixpunkt von a, Teilmenge von $\overline{\diamondsuit b}$ ist, also von jener Teilmenge aller Pfade, deren Teilpfade nicht zugleich eine Länge von weniger als x Knoten und ein Gewicht von mehr als $2y$ besitzen.

Kapitel 7

Resümee und Ausblick

Ziel dieser Arbeit ist es gewesen, den Zeitdauer-Kalkül für Kleene-Algebren herzuleiten. Dazu war die Analyse und die Definition von speziellen Operatoren wie den Residuen, den Abtrennungs- und den Intervalloperatoren notwendig. Aus diesem Grund hat sich ein Großteil dieser Arbeit den Beweisen von Eigenschaften dieser Operatoren gewidmet.
Anschließend wurde durch die Ingenieurs-Induktion gezeigt, dass es unter Umständen nicht erforderlich ist, Eigenschaften für den kleinsten Fixpunkt von a zu beweisen. Dies ist der Fall, wenn a über die Intervalloperatoren mit den zu betrachtenden Eigenschaften in Verbindung steht. In einer solchen Situation genügt es, einzelne Objekte wie das Einselement, a und a^2 zu betrachten. Auf diese Weise ist es möglich, sich die oft komplizierte Berechnung des Fixpunktes zu ersparen. Ein weiterer Vorteil der Ingenieurs-Induktion wird deutlich, wenn man mengenartige Kleene-Algebren betrachtet. Bei diesen sind häufig die Fixpunktmengen von a weitaus mächtiger und unübersichtlicher als a selbst, das Einselement und die anderen betrachteten Mengen. Die Ingenieurs-Induktion ermöglicht in vielen Fällen das Rechnen auf kleineren Mengen.
Auf der Ingenieurs-Induktion aufbauend, konnte der Zeitdauer-Kalkül eingeführt werden. Hierzu war es zunächst nötig, Halbringe über Intervallen reeller Zahlen zu konstruieren. Dadurch war es möglich, den Faktor Zeit in die Begriffe der Halbringe und Kleene-Algebren einzubetten. Später wurden mit dieser Grundlage bei gegebenen Sicherheitsanforderungen spezielle Designs entworfen. Die Korrektheit dieser wurde anschließend über den Zeitdauer-Kalkül bewiesen. Zur Veranschaulichung des Zeitdauer-Kalküls diente das Beispiel einer Gasleitung, an welcher unkontrolliert Gas ausströmen und die somit zu einem Sicherheitsrisiko werden kann.

Weiterführend wäre von Interesse, ob die Ingenieurs-Induktion auch für nicht lokal lineare Kleene-Algebren bewiesen werden kann oder ob eine nicht lokal lineare, boolesche Kleene-Algebra konstruiert werden kann, welche die Folgerung der Ingenieurs-Induktion nicht erfüllt. Einfache Beispiele, wie die in dieser Arbeit vorgestellten und kleine atomare, aber auch kompliziertere Kleene-

Algebren, wie etwa die von K. Iwano und K. Steiglitz vorgestellte Polygon-Kleene-Algebra ([IS90]), sind entweder lokal linear, erfüllen die Ingenieurs-Induktion, obwohl sie nicht lokal linear sind, oder besitzen keine Negationsfunktion. Sollte es sich als richtig erweisen, dass die Ingenieurs-Induktion auch für nicht lokal lineare Kleene-Algebren gültig ist, kann aufbauend auf dieser Erkenntnis ohne weitere Probleme der Zeitdauer-Kalkül auf die Klasse aller booleschen Kleene-Algebren, welche Residuen besitzen, erweitert werden. Denn im Beweis des Zeitdauer-Kalküls wurde die lokale Linearität nur für die Ingenieurs-Induktion benötigt.

Anhang A

Kleene-Algebren mit Residuen

Satz A.1
Kleene-Algebren sind unter homomorphen Abbildungen nicht abgeschlossen.

Beweis:

Sei $LAN(\Sigma) = (\mathcal{P}(\Sigma^*), \cup, \mathbin{+\!\!+}, \emptyset, \{\varepsilon\})$ die Kleene-Algebra der formalen Sprachen über Σ. Sei $A = \{0, e, a, 1\}$ und h ein Homomorphismus mit

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

Durch diese Abbildung wird A zum homomorphen Bild von $\mathcal{P}(\Sigma^*)$. Allgemein gilt für beliebige Mengen M und N aus $\mathcal{P}(\Sigma^*)$ die Dreiecksungleichung:

$$|M \mathbin{+\!\!+} N| \leq |M| \cdot |N| .$$

Daher gilt für endliche Mengen X und Y mit $X, Y \subseteq \Sigma^*$ und $X, Y \neq \emptyset, \{\varepsilon\}$, dass $X \mathbin{+\!\!+} Y$ wiederum endlich ist. Aus diesem Grund folgt

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

Wäre A wieder eine Kleene-Algebra, so müsste entspechend ($*$-3) folgende Beziehung gelten:

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

Es gilt jedoch:

$$\begin{aligned} & X^* = \bigcup_{i \geq 0} X^i \\ \Rightarrow \quad & |X^*| = \infty \\ \Rightarrow \quad & h(X^*) = 1. \end{aligned}$$

$$\Rightarrow a^* \cdot a = h(X^{*}\text{++}X) = 1$$

Der letzte Schritt gilt, da $|X^{*}\text{++}X| \geq |X^*| = \infty$. Dies ist jedoch ein Widerspruch zu (A.1).

□

Satz A.2
Eine Kleene-Algebra $(A, +, \cdot, 0, 1, ^*)$ mit Residuen ist eine Varietät, welche durch einen Halbring mit Residuen und folgende Gleichungen eindeutig definiert ist. Sei $a \in A$.

$$1 + a + a \cdot a^* \leq a^*, \tag{A.2}$$
$$1 + a + a^* \cdot a \leq a^*, \tag{A.3}$$
$$(a/a)^* \leq (a/a), \tag{A.4}$$
$$(a\backslash a)^* \leq (a\backslash a). \tag{A.5}$$

Dies bedeutet explizit, dass Kleene-Algebren mit Residuen unter homomorphen Bildern abgeschlossen sind.

Beweis:

z.z.: $(*\text{-}3) \Leftrightarrow ((x/x)^* \leq (x/x))$

"$\Rightarrow$"

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

"$\Leftarrow$" Sei $(x/x)^* \leq (x/x)$. Dann gilt:

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

Aus dieser Umformung kann ($*$-3) gefolgert werden.

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

Analog hierzu kann natürlich auch die Äquivalenz zwischen ($*$-4) und $(x\backslash x)^* \leq (x\backslash x)$ gezeigt werden.

□

Lemma A.3
In Kleene-Algebren mit Residuen sind die beiden Horn-Regeln ($*$-3) und ($*$-4) äquivalent, d.h.:

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

Beweis:

"⇒" (i) z.z.: $1 \leq x\backslash x$

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

(ii) z.z.: $(x\backslash x) \cdot (x\backslash x) \leq (x\backslash x)$

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

(iii) z.z.: $(b+a\cdot x \leq x \Rightarrow a^*\cdot b \leq x) \Rightarrow (1+a+x\cdot x \leq x \Rightarrow a^* \leq x)$

$$\begin{array}{ll} & a \leq x \\ \Rightarrow & \quad \{\text{Monotonie bzgl. der Multiplikation}\} \\ & a \cdot x \leq x \cdot x \\ \Rightarrow & \quad \{\text{Voraussetzung: } x \cdot x \leq x\} \\ & a \cdot x \leq x \\ \Rightarrow & \quad \{x \leq x \text{ und Supremumseigenschaft}\} \\ & x + a \cdot x \leq x \\ \Rightarrow & \quad \{\text{Voraussetzung}\} \\ & a^* \cdot x \leq x \\ \Rightarrow & \quad \{\text{Voraussetzung: } 1 \leq x\} \\ & a^* \cdot 1 \leq x \\ \Leftrightarrow & a^* \leq x \end{array}$$

(iv) z.z.: $b + x \cdot a \leq x \Rightarrow b \cdot a^* \leq x$

$$
\begin{aligned}
& b + x \cdot a \leq x \\
\Leftrightarrow \quad & \{\text{Supremumseigenschaft}\} \\
& b \leq x \wedge x \cdot a \leq x \\
\Leftrightarrow \quad & \{\text{Definition von } \backslash\} \\
& b \leq x \wedge a \leq x \backslash x \\
\Leftrightarrow \quad & \{\text{(i) und (ii)}\} \\
& b \leq x \wedge a \leq x \backslash x \wedge 1 \leq x \backslash x \wedge (x \backslash x) \cdot (x \backslash x) \leq (x \backslash x) \\
\Leftrightarrow \quad & \{\text{Supremumseigenschaft}\} \\
& b \leq x \wedge 1 + a + (x \backslash x) \cdot (x \backslash x) \leq x \backslash x \\
\Rightarrow \quad & \{\text{(iii)}\} \\
& b \leq x \wedge a^* \leq x \backslash x \\
\Leftrightarrow \quad & \{\text{Definition vom } \backslash\} \\
& b \leq x \wedge x \cdot a^* \leq x \\
\Rightarrow \quad & \{\text{Monotonie der Multiplikation}\} \\
& b \cdot a^* \leq x
\end{aligned}
$$

"$\Leftarrow$"

Analog zu "$\Rightarrow$".

□

Literaturverzeichnis

[Beh98] Ralf Behnke. *Transformationelle Programmentwicklung im Rahmen relationaler und sequentieller Algebren*. 1998.

[BJ72] T.S. Blyth und M.F. Janowitz. *Residuation theory*, Band 102 der Reihe *Pure and applied mathematics*. Pergamon Press, 1972.

[CHR91] Zhou Chaochen, C.A.R Hoare und Anders P. Ravn. *A calculus of durations*. Band 40 der Reihe *Information Processing Letters*, Seiten 269–276, 1991.

[Dim00] Cătălin Dima. *Real-time automata and the Kleene algebra of sets of real numbers*. In: *Proceedings of STACS'2000*, Seiten 279–289, 2000.

[DMS03] Jules Desharnais, Bernhard Möller und Georg Struth. *Kleene Algebra with Domain*. Technischer Bericht Universität Augsburg, 2003. http://www.informatik.uni-augsburg.de/forschung/techBerichte/reports/2003-7.pdf.

[Dut95a] B. Dutertre. *Complete Proof Systems for First Order Interval Temporal Logic*. In: IEEE PRess (Herausgeber): *Tenth Annual IEEE Symb. on Logic in Computer Science*, Seiten 36–43, 1995.

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

[HC97] Michael R. Hansen und Zhou Chaochen. *Duration Calculus: Logical foundations*. Band 9 der Reihe *Formal Aspects of Computing*, Seiten 283–330, 1997.

[Heh98] Eric C.R. Hehner. *Formalization of Time and Space*. Band 10 der Reihe *Formal Aspects of Computing*, Seiten 290–306, 1998.

[HW93] Udo Hebisch und Hanns Joachim Weinert. *Halbringe. Algebraische Theorie und Anwendungen in der Informatik*. Teubner-Studienbücher: Mathematik. Teubner, 1993.

[IS90] Kazuo Iwano und Kenneth Steiglitz. *A Semiring on Convex Polygons and Zero-Sum Cycle Problems.* Band 19(5) der Reihe *SIAM Journal on Computing*, Seiten 883–901, 1990.

[Jip02] Peter 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] Burghard von Karger. *Temporal Algebra.* Math. Structures in Computer Science, 1996.

[Kar00] Burghard von Karger. *A calculational approach to reactive systems.* Band 37 der Reihe *Science of Computer Programming*, Seiten 139–161, 2000.

[Kar01] Burghard von Karger. *Temporal Algebra.* In: Roland Backhouse, Roy Crole und Jeremy Gibbons (Herausgeber): *Algebraic and Coalgebraic Methods in the Mathematics of Program Construction*, Band 2297 der Reihe *Lecture Notes in Computer Science*, Seiten 309–385. Springer, 2001.

[Koz90] Dexter Kozen. *On Kleene algebras and closed semirings.* In: Rovan (Herausgeber): *Mathematical Foundation in Compututer Science 1990*, Band 452 der Reihe *Lecture Notes in Computer Science*, Seiten 26–47. Springer, 1990. http://www.cs.cornell.edu/kozen/papers/kacs.ps.

[Koz94] Dexter Kozen. *A completeness theorem for Kleene algebras and the algebra of regular events.* Band 110(2) der Reihe *Information and Computation*, Seiten 366–390, 1994.

[LRL98] Zhiming Liu, Anders P. Ravn und Xiaoshan Li. *Unifying Proof Methodologies of DC and LTL.* In: *Duration Calculus Workshop, ESSLLI'98*, Seiten 99–109, 1998.

[Möl] Bernhard Möller. *Residuals and Detachments.* Unveröffentlichtes Manuskript.

[Pra91] Vaughan Pratt. *Action Logic and Pure Induktion, Logics in AI.* In: *European Workshop JELIA '90, ed J. van Eijck*, Band 478 der Reihe *Lectures in Computer Science*, Seiten 97–120, 1991. http://boole.stanford.edu/pub/jelia.ps.gz.