Modal Design Algebra

Walter Guttmann[1] and Bernhard Möller[2]

[1] Abteilung Programmiermethodik und Compilerbau, Fakultät für Informatik, Universität Ulm, D-89069 Ulm, Germany
walter.guttmann@uni-ulm.de
[2] Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany
moeller@informatik.uni-augsburg.de

Abstract. We give an algebraic model of the designs of UTP based on a variant of modal semirings, hence generalising the original relational model. This is intended to exhibit more clearly the algebraic principles behind UTP and to provide deeper insight into the general properties of designs, the program and specification operators, and refinement. Moreover, we set up a formal connection with general and total correctness of programs as discussed by a number of authors. Finally we show that the designs form a left semiring and even a Kleene and omega algebra. This is used to calculate closed expressions for the least and greatest fixed-point semantics of the demonic while loop that are simpler than the ones obtained from standard UTP theory and previous algebraic approaches.

1 Introduction

The Unifying Theories of Programming (UTP), developed in [13], model the termination behaviour of programs using two special variables ok and ok' that express whether a program has been started and has terminated, respectively. Specifications and programs are identified with predicates relating the initial values v of variables to their final values v'; moreover, ok and ok' may occur freely in predicates. Using these variables, Hoare and He introduce a special class of predicates that reflect an assumption/commitment style of specification. These *designs* have the form

$$P \vdash Q \;\stackrel{\text{def}}{\Leftrightarrow}\; ok \;\wedge\; P \;\Rightarrow\; ok' \;\wedge\; Q \;,$$

with ok and ok' not occurring in P or Q. The informal meaning is: if a computation allowed by the design has started in a state that satisfies the precondition P it will eventually terminate in a state that satisfies the postcondition Q.

In the general case, UTP allows the precondition P to involve both initial and final values of the program variables. A subclass that is interesting for a number of reasons is that of *normal* designs in which P is a *condition*, i.e., is only allowed to depend on input values of variables. Originally [13] these were called *(H3)* designs and characterised by a healthiness condition; the term "normal" is due to [10]. A yet smaller subclass, the *feasible* or *(H4)* designs models programs that cannot "recover" from nontermination.

The aims and results of the present paper are the following:

1. We model normal designs in a more general class of algebras than pure relation algebra. This is intended to exhibit more clearly the algebraic principles behind UTP and to provide deeper insight into the general properties of designs, the program and specification operators, and refinement.
2. We set up a formal connection between UTP and the theories of general (e.g. [2, 3, 9, 19, 21]) and total (e.g. [1, 5, 6, 8, 20]) correctness of programs (the latter also being known as demonic semantics).
3. We show that the designs form a left semiring and even a Kleene and omega algebra. This is used to calculate closed expressions for the least and greatest fixed-point semantics of the demonic while loop that are simpler than the ones obtained from standard UTP theory and previous algebraic approaches.

To achieve this we model normal designs as pairs (a, t) where a corresponds to a state transition relation and condition t characterises the input states from which termination is guaranteed. The structure from which a and t are taken is that of an idempotent semiring which is an algebraic abstraction of the basic operations of choice and sequential composition, as detailed in the next section.

2 The Basis: Choice and Composition

A *semiring* is a structure $(S, +, 0, \cdot, 1)$ such that

- $(S, +, 0)$ is a commutative monoid,
- $(S, \cdot, 1)$ is a monoid,
- operation $\cdot$ distributes over $+$ in both arguments
- and 0 is a left and right annihilator, i.e., $0 \cdot x = 0 = x \cdot 0$.

A semiring is *idempotent* if $+$ is, i.e., if $x + x = x$. Then $+$ can be interpreted as (angelic) choice, with 0 modelling the most partial program with no transition possibilities at all, and $\cdot$ as sequential composition, where 1 models the program skip. In this case, the relation $x \leq y \Leftrightarrow x + y = y$ is a partial order, called the *natural order* on S. It has 0 as its least element. Moreover, $+$ and $\cdot$ are isotone w.r.t. $\leq$ and $x + y$ is the least upper bound or join of x and y w.r.t. $\leq$.

An idempotent semiring is *Boolean* if it also has a greatest lower-bound or meet operation $\wedge$, such that $+$ and $\wedge$ distribute over each other, and an operation $\bar{}$ that satisfies de Morgan's laws as well as $x \wedge \overline{x} = 0$ and $x + \overline{x} = \top$, where $\top = \overline{0}$ is the greatest element. In other words, a Boolean semiring is a Boolean algebra with a sequential composition operation. To save parentheses we use the convention that $\wedge$ binds tighter than $+$ but less tight than $\cdot$ does. We use $\wedge$ rather than $\sqcap$ for the meet to avoid a clash of notation between semiring theory and the theory of UTP. To disambiguate the formulas we use a larger $\bigwedge$ for meta-logical conjunction.

An important, even Boolean, semiring is $\mathrm{REL}(M) = \mathcal{P}(M \times M)$, the algebra of binary relations under union and composition over a set M, of which the predicates of UTP form a special instance. The greatest element is $\top = M \times M$. Next to that, we have the Boolean semiring $\mathrm{TRC}(A)$ of sets of traces (i.e., finite strings) over alphabet A under union as $+$ and trace concatenation (i.e., fusion

product) as the $\cdot$ operation. TRC(A) is isomorphic to the path algebra described in detail in [7]; in the present paper it will mainly be used for counterexamples to properties that hold in REL(M) but not necessarily in general semirings.

3 Modelling Conditions

Elements of REL(M), denoted by predicates relating pre- and post-states, can be used to describe the input/output behaviour of programs. To keep the framework uniform one wants to encode also assertions about the program variables, i.e., to characterise subsets $N \subseteq M$ of states, as special predicates or relations. There are three basic methods to do this:

1. Use predicates that do not depend on the output values of variables, corresponding to *right-universal* relations $N \times M$. In a semiring with $\top$ they are abstractly characterised as *right ideals*, i.e., as elements a with $a \cdot \top = a$.
2. Use predicates that do not depend on the input values of variables, corresponding to *left-universal* relations $M \times N$. In a semiring with $\top$ they are abstractly characterised as *left ideals*, i.e., as elements a with $\top \cdot a = a$.
3. Use sub-predicates of skip corresponding to *partial identity* relations of the form $\{(s, s) : s \in N\}$. In an idempotent semiring they are abstractly characterised as elements a with $a \leq 1$.

Each of these approaches has its advantages and disadvantages. Classical UTP uses variant 1, while variant 3 is used in test and modal semirings. Since we are going to import some results from the first framework, we will show some connections between variants 1 and 3 (we do not need variant 2 in the present paper, but the treatment for it would be symmetrical).

1. A *test semiring* [15] is a pair $(S, \mathsf{test}(S))$, where S is an idempotent semiring and $\mathsf{test}(S) \subseteq [0, 1]$ is a Boolean subalgebra of the interval $[0, 1]$ of S such that $0, 1 \in \mathsf{test}(S)$ and join and meet in $\mathsf{test}(S)$ coincide with $+$ and $\cdot$. This fits well with the notation in switching and lattice theory and is the reason why $+$ is used for general choice in semiring notation. In general, $\mathsf{test}(S)$ may be a proper subset of the elements below 1 in S. The negation of test p, i.e., its complement relative to 1 in $\mathsf{test}(S)$, is denoted by $\neg p$. We have the correspondences *false* $\leftrightarrow 0$ and *true* $\leftrightarrow 1$. In a test semiring, for $p \in \mathsf{test}(S)$ and $a \in S$, the products $p \cdot a$ and $a \cdot p$ are the *input* and *output restrictions* of a to those pre-/post-states that satisfy p. An important example is REL(M) with the partial identities as tests.
2. A *(right) pre-condition-semiring* is a pair $(S, \mathsf{cond}(S))$, where S is an idempotent semiring with a greatest element $\top$ and $\mathsf{cond}(S) \subseteq S$ is a Boolean subalgebra of S with $0, \top \in \mathsf{cond}(S)$ and such that the join operation in $\mathsf{cond}(S)$ coincides with $+$ and for every element $a \in S$ and every condition $t \in \mathsf{cond}(S)$ the meet $t \wedge a$, called the *input restriction of a by t*, exists and satisfies $(t + u) \wedge a = (t \wedge a) + (u \wedge a)$ as well as $t \wedge (a + b) = t \wedge a + t \wedge b$. We have the correspondences *false* $\leftrightarrow 0$ and *true* $\leftrightarrow \top$. The negation of t, i.e.,

its complement relative to $\top$ in $\mathsf{cond}(S)$, is denoted by $\overline{t}$. Finally, S is called a *(right) condition semiring* if all elements of $\mathsf{cond}(S)$ are right ideals. An example is again $\mathrm{REL}(M)$, with the right-universal relations as conditions.

We will use the letters $a, b, c, \ldots$ for semiring elements, $p, q, r, \ldots$ for tests and $s, t, u, \ldots$ for conditions. It should be noted that 0 and $\top$ are always right (and left) ideals. For 0 this follows from its left annihilation property, while for $\top$ we get, using neutrality of 1 and isotony, $\top = \top{\cdot}1 \leq \top{\cdot}\top \leq \top$, which, together with antisymmetry of $\leq$ shows the claim.

In a pre-condition-semiring there is no reasonable definition of output restriction. However, as we will see below, for condition semirings there is.

Using input restriction we can define conditionals by setting, respectively,

$$a \lhd p \rhd b \stackrel{\text{def}}{=} p \cdot a + \neg p \cdot b \;, \qquad a \lhd v \rhd b \stackrel{\text{def}}{=} v \wedge a + \overline{v} \wedge b \;.$$

Moreover, we have the following correspondence for input restriction:

Lemma 3.1. *[16] In every test semiring S with greatest element $\top$, for all $p \in \mathsf{test}(S)$ and $a \in S$ the meet $p \cdot \top \wedge a$ exists and $p \cdot a = p \cdot \top \wedge a$.*

By associativity of $\cdot$ and $(p \cdot \top) \cdot \top = p \cdot (\top \cdot \top) = p \cdot \top$ the element $p \cdot \top$ is indeed a right ideal. In fact it is easy to show that the right ideals in a semiring S with $\top$ are exactly the products $a \cdot \top$ for $a \in S$.

Now we look at condition semirings. We obtain the representation

$$t = (t \wedge 1) \cdot \top \;, \tag{crep}$$

and $t \wedge a = (t \wedge 1) \cdot a$, the analogue of Lemma 3.1, by specialising the

Lemma 3.2. *$(t \wedge a) \cdot b = t \wedge (a \cdot b)$ for a condition t.*

Proof. ($\leq$) By isotony, $(t \wedge a) \cdot b \leq a \cdot b$ and $(t \wedge a) \cdot b \leq t \cdot b \leq t \cdot \top = t$ since, as a condition, t is a right ideal.
($\geq$) By Boolean algebra and the first inequality, $t \wedge (a \cdot b) = t \wedge ((t \wedge a) \cdot b + (\overline{t} \wedge a) \cdot b) \leq t \wedge ((t \wedge a) \cdot b + \overline{t} \wedge (a \cdot b)) = t \wedge ((t \wedge a) \cdot b) \leq (t \wedge a) \cdot b$. □

Corollary 3.3. *In a condition semiring, $t \wedge 1 \leq u \wedge 1 \Leftrightarrow t \leq u$.*

Proof. ($\Leftarrow$) follows by isotony of meet.
($\Rightarrow$) $t \underset{\text{(crep)}}{=} (t \wedge 1) \cdot \top \underset{\text{(assump., isot.)}}{\leq} (u \wedge 1) \cdot \top \underset{\text{(crep)}}{=} u$. □

So $\mathsf{cond}(S)$ and the set $\mathrm{CS}(S) \stackrel{\text{def}}{=} \{t \wedge 1 : t \in \mathsf{cond}(S)\}$ of *condition subidentities* are order-isomorphic. Hence also $\mathrm{CS}(S)$ is a Boolean algebra with

$$\begin{aligned} t \wedge 1 + u \wedge 1 &= (t + u) \wedge 1 \;, \\ (t \wedge 1) \wedge (u \wedge 1) &= (t \wedge 1) \cdot (u \wedge 1) \;, \\ \neg(t \wedge 1) &= \overline{t} \wedge 1 \;. \end{aligned}$$

Altogether we have the

Corollary 3.4. *Every condition semiring S can be made into a test semiring by setting* $\mathsf{test}(S) \stackrel{\text{def}}{=} \mathrm{CS}(S)$ *and choosing the operations as above.*

By these results, in a condition semiring we can define the *output restriction of a by t* as $a \cdot (t \wedge 1)$.

4 Domain and Modal Operators

The domain of a semiring element a is intended to characterise the set of possible input states of a, i.e., the states from which corresponding output states may be reached under a. Again, such sets can be modelled by tests or by conditions.

A simple equational axiomatisation for the case of test semirings has been presented in [7]. We give a corresponding axiomatisation for the case of pre-condition-semirings here. Both cases are compared side-by-side in [12].

The domain operation $\mathrel{⌜} : S \to \mathsf{cond}(S)$ has the axioms

$$\begin{aligned} a &\leq \mathrel{⌜}a \wedge a && \text{(cd1)}\\ \mathrel{⌜}(t \wedge a) &\leq t && \text{(cd2)}\\ \mathrel{⌜}(a \cdot (\mathrel{⌜}b \wedge 1)) &\leq \mathrel{⌜}(a \cdot b) && \text{(cd3)} \end{aligned}$$

Actually, (cd1) and (cd3) can be strengthened to equations (see Lemma 4.1 below). By reasoning as in [7] we obtain that (cd1) $\wedge$ (cd2) is equivalent to

$$\mathrel{⌜}a \leq t \;\Leftrightarrow\; a \leq t \wedge a \;\Leftrightarrow\; a \leq t\ . \qquad \text{(GCc)}$$

This property has the form of a Galois connection that corresponds to the one for test semirings with $\top$ (see [7] for details). Moreover, by shunting, (cd1) $\wedge$ (cd2) is equivalent to $\mathrel{⌜}a \leq t \;\Leftrightarrow\; \overline{t} \wedge a \leq 0$. By the Galois connection, the domain operation is unique if it exists. Moreover, one obtains the following consequences.

Lemma 4.1.

1. $\mathrel{⌜}a \leq 0 \;\Leftrightarrow\; a \leq 0$,
2. $\mathrel{⌜}(a + b) \;=\; \mathrel{⌜}a + \mathrel{⌜}b$,
3. $a \leq b \;\Rightarrow\; \mathrel{⌜}a \leq \mathrel{⌜}b$,
4. $\mathrel{⌜}t \;=\; t$,
5. $\mathrel{⌜}(\mathrel{⌜}a) \;=\; \mathrel{⌜}a$,
6. $a \;=\; \mathrel{⌜}a \wedge a$,
7. $\mathrel{⌜}(t \wedge a) \;=\; t \wedge \mathrel{⌜}a$,
8. $\mathrel{⌜}(a \cdot b) \;\leq\; \mathrel{⌜}(a \cdot \mathrel{⌜}b)$,
9. $\mathrel{⌜}(a \cdot \top) = \mathrel{⌜}a \;\Leftrightarrow\; \mathrel{⌜}b = \mathrel{⌜}b \cdot \top$,
10. $\mathrel{⌜}(a \cdot b) \leq \mathrel{⌜}a \;\Leftrightarrow\; \mathrel{⌜}c = \mathrel{⌜}c \cdot \top$.

Of these, properties 9. and 10. again show the special importance of using condition semirings rather than pre-condition-semirings. See [12] for the proofs.

By 9. and (crep), in a condition semiring the third axiom simplifies to

$$\mathrel{⌜}(a \cdot \mathrel{⌜}b) \leq \mathrel{⌜}(a \cdot b)\ . \qquad \text{(cd3)}$$

Moreover, we have $\mathrel{⌜}1 \underset{9.}{=} \mathrel{⌜}(1 \cdot \top) \;=\; \mathrel{⌜}\top \underset{4.}{=} \top$.

Now we make the connection with the relational case more explicit. Call a semiring S with $\top$ *ideal-closed*, briefly *id-closed*, if its set $\mathrm{RI}(S)$ of right ideals is a Boolean algebra. The relation semiring $\mathrm{REL}(M)$ is id-closed whereas the trace semiring $\mathrm{TRC}(A)$ is not.

Lemma 4.2.

1. *Consider an id-closed semiring S. Then the pair $(S, \mathrm{RI}(S))$ can uniquely be made into a domain semiring by setting $\ulcorner a \stackrel{\text{def}}{=} a \cdot \top$.*
2. *In this case we have $\ulcorner a \cdot \top = a \cdot \top$.*

Proof. 1. We show that $\ulcorner$ satisfies the domain axioms.
(cd1) $\ulcorner a \wedge a = a$, since $a = a \cdot 1 \leq a \cdot \top$.
(cd2) $\ulcorner(t \wedge a) \underset{\text{(def.)}}{=} (t \wedge a) \cdot \top \underset{\text{(Lemma 3.2)}}{=} t \wedge a \cdot \top \leq t$.
(cd3) $\ulcorner(a \cdot \ulcorner b) \underset{\text{(def., assoc.)}}{=} a \cdot b \cdot \top \cdot \top = a \cdot b \cdot \top \underset{\text{(def.)}}{=} \ulcorner(a \cdot b)$.
2. $\ulcorner a \cdot \top = a \cdot \top \cdot \top = a \cdot \top$. □

Based on domain we can define forward modal operators by

$$\langle\!\langle a \rangle\!\rangle t \stackrel{\text{def}}{=} \ulcorner(a \cdot t) \;, \qquad [\![a]\!] t \stackrel{\text{def}}{=} \overline{\langle\!\langle a \rangle\!\rangle \bar{t}} \;.$$

Thus $\langle\!\langle a \rangle\!\rangle t$ and $[\![a]\!] t$ characterise those states for which *some* and *all* a-successor states satisfy t, respectively; $[\![a]\!] t$ is the abstract counterpart of the wlp operator [19]. The special case corresponding to $\mathrm{REL}(M)$ is immediate from Lemma 4.2:

Corollary 4.3. *Over an id-closed semiring $\langle\!\langle a \rangle\!\rangle t = a \cdot t$ and $[\![a]\!] t = \overline{a \cdot \bar{t}}$.*

From the general definitions it straightforward to prove the following properties.

$$\begin{array}{cc}
\langle\!\langle a \rangle\!\rangle 0 = 0 \;, & [\![a]\!] \top = \top \;, \\
\langle\!\langle 0 \rangle\!\rangle t = 0 \;, & [\![0]\!] t = \top \;, \\
\langle\!\langle a \rangle\!\rangle (t + u) = \langle\!\langle a \rangle\!\rangle t + \langle\!\langle a \rangle\!\rangle u \;, & [\![a]\!](t \wedge u) = [\![a]\!] t \wedge [\![a]\!] u \;, \\
\langle\!\langle a + b \rangle\!\rangle t = \langle\!\langle a \rangle\!\rangle t + \langle\!\langle b \rangle\!\rangle t \;, & [\![a + b]\!] t = [\![a]\!] t \wedge [\![b]\!] t \;, \\
\langle\!\langle t \wedge a \rangle\!\rangle u = t \wedge \langle\!\langle a \rangle\!\rangle u \;, & [\![t \wedge a]\!] u = \bar{t} + [\![a]\!] u \;, \\
\langle\!\langle 1 \rangle\!\rangle t = t \;, & [\![1]\!] t = t \;, \\
\langle\!\langle a \cdot b \rangle\!\rangle t = \langle\!\langle a \rangle\!\rangle \langle\!\langle b \rangle\!\rangle t \;, & [\![a \cdot b]\!] t = [\![a]\!] [\![b]\!] t \;.
\end{array}$$

Hence $\langle\!\langle a \rangle\!\rangle$ and $[\![a]\!]$ are isotone. Moreover, the diamond is isotone and the box is antitone in its first argument, respectively.

Because of the importance of modal operators, we call a test or condition semiring with domain *modal*.

5 Designs, Commands and Correctness

To stay in line with the treatment in [13], we now restrict ourselves to modelling sets of states by conditions rather than tests. Assume a modal condition semiring S. As mentioned in the introduction, then the set of *commands* [19, 18] over S is $\mathrm{COM}(S) \stackrel{\text{def}}{=} S \times \mathsf{cond}(S)$. In a command (a, t) the element $a \in S$ describes the state transition behaviour and $t \in \mathsf{cond}(S)$ characterises the states with guaranteed termination; all states characterised by $\bar{t}$ have the "result" of looping besides any proper states that may be reached from them under a. The command

(a,t) is synonymous both for the normal designs $t \vdash a$ of [13] and the normal prescriptions $t \Vdash a$ of Dunne [10]. The difference is reflected in the refinement relations on commands that will be detailed below. The following definitions and properties are adaptations of the corresponding ones in [18].

In the command view the weakest (liberal) precondition can be defined as

$$\mathsf{wlp}.(a,t).u \stackrel{\text{def}}{=} [\![a]\!]u \;, \qquad \mathsf{wp}.(a,t).u \stackrel{\text{def}}{=} t \wedge \mathsf{wlp}.(a,t).u \;.$$

This implies Nelson's *pairing condition* for commands k:

$$\mathsf{wp}.k.u \;=\; \mathsf{wp}.k.\top \wedge \mathsf{wlp}.k.u \;.$$

An important auxiliary concept is the *guard* of a command:

$$\mathsf{grd}.(a,t) \stackrel{\text{def}}{=} \overline{\mathsf{wp}.(a,t).0} \;=\; \bar{t} + \Gamma a \;.$$

It characterises the set of states that, if non-diverging, allow a transition under a. A command is called *total* if its guard equals top. The above formula links Parnas's condition [21] on termination constraints with totality:

$$\mathsf{grd}.(a,t) \;=\; \top \;\Leftrightarrow\; t \leq \Gamma a \;.$$

We will shortly see that this condition characterises exactly the feasible normal designs. Nelson remarks that totality of command k is also equivalent to Dijkstra's law $\mathsf{wp}.k.0 = 0$ of the excluded miracle.

The basic non-iterative commands are defined as

$$\mathsf{fail} \stackrel{\text{def}}{=} (0,\top) \;, \qquad \mathsf{skip} \stackrel{\text{def}}{=} (1,\top) \;, \qquad \mathsf{loop} \stackrel{\text{def}}{=} (0,0) \;,$$
$$(a,t) \,[]\, (b,u) \stackrel{\text{def}}{=} (a+b,\, t \wedge u) \;, \qquad (a,t)\,;(b,u) \stackrel{\text{def}}{=} (a \cdot b,\, t \wedge [\![a]\!]u) \;.$$

Here $t \wedge [\![a]\!]u$ characterises those states for which a is guaranteed to terminate and which under a only lead to guaranteed termination states of b.

The commands form a *left semiring*, i.e., satisfy all semiring laws except for the right annihilation law for the zero element fail.

Theorem 5.1. *The structure* $\mathrm{COM}(S) \stackrel{\text{def}}{=} (\mathrm{COM}(S), [], \mathsf{fail}, ;, \mathsf{skip})$ *is an idempotent left semiring. The associated natural order on* $\mathrm{COM}(S)$ *is*

$$(a,t) \leq (b,u) \;\Leftrightarrow\; a \leq b \;\wedge\; t \geq u \;.$$

The proof, which is a mere transliteration of the corresponding one in [18] for the test semiring case, can be found in [12]. It is essential that semiring S be a semiring and not only a left semiring. The natural order between commands is used in [10]. Its drawback is that it cannot be used as the approximation order for fixpoint semantics; for details see again [18].

By standard order theory, if S is a complete lattice with $\mathsf{cond}(S)$ as a complete sublattice then $\mathrm{COM}(S)$ is again a complete lattice with, for arbitrary I,

$$\sqcup\,\{(a_i,p_i) : i \in I\} \;=\; (\sqcup\,\{a_i : i \in I\}, \sqcap\,\{a_i : i \in I\}).$$

Likewise, $\mathsf{chaos} \stackrel{\text{def}}{=} (\top, 0)$ is the greatest element of $\mathrm{COM}(S)$, whereas $\mathsf{havoc} \stackrel{\text{def}}{=} (\top, \top)$ represents the most nondeterministic everywhere terminating program.

As in [13] we say that command k is *(H4)* or *feasible* iff $k\,;\mathsf{loop} = \mathsf{loop}$. One calculates, using $[\![a]\!]0 = \overline{\ulcorner a}$ and semiring properties,

$$(a,t)\,;\mathsf{loop} = (a \cdot 0,\, t \wedge [\![a]\!]0) = (0,\, t \wedge \overline{\ulcorner a}) \;.$$

Corollary 5.2. *Command (a,t) is feasible iff $t \leq \ulcorner a$.*

Therefore loop, skip, havoc and chaos are feasible, whereas fail is not. Moreover, $[]$ and ; preserve feasibility.

6 Refinement

Let us now look more closely at the natural order induced on the commands by the left semiring structure. By antitony of box we obtain for commands k, l

$$k \leq l \;\;\Rightarrow\;\; \mathsf{wlp}.k \geq \mathsf{wlp}.l \;\;\wedge\;\; \mathsf{wp}.k \geq \mathsf{wp}.l \;,$$

where on the right hand side $\geq$ is the pointwise order between condition transformers. The second conjunct is the converse of the usual refinement relation. For it we calculate

$$\begin{array}{ll}
& \mathsf{wp}.(a,t).v \geq \mathsf{wp}.(b,u).v \\
\Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\
& t \wedge [\![a]\!]v \geq u \wedge [\![b]\!]v \\
\Leftrightarrow & \quad \{\![\text{ universal property of meet }]\!\} \\
& t \geq u \wedge [\![b]\!]v \;\wedge\; [\![a]\!]v \geq u \wedge [\![b]\!]v \\
\Leftrightarrow & \quad \{\![\text{ shunting in right conjunct }]\!\} \\
& t \geq u \wedge [\![b]\!]v \;\wedge\; \langle\!\langle b \rangle\!\rangle \overline{v} \geq u \wedge \langle\!\langle a \rangle\!\rangle \overline{v} \\
\Leftrightarrow & \quad \{\![\text{ diamond law }]\!\} \\
& t \geq u \wedge [\![b]\!]v \;\wedge\; \langle\!\langle b \rangle\!\rangle \overline{v} \geq \langle\!\langle u \wedge a \rangle\!\rangle \overline{v} \\
\Leftarrow & \quad \{\![\text{ isotony }]\!\} \\
& t \geq u \;\wedge\; b \geq u \wedge a \;.
\end{array}$$

We use the latter formula as the refinement relation between commands:

$$(a,t) \sqsubseteq (b,u) \stackrel{\text{def}}{\Leftrightarrow} u \leq t \;\wedge\; u \wedge a \leq b \;.$$

Due to our generalised setting we only have $k \sqsubseteq l \;\Rightarrow\; \mathsf{wp}.k \geq \mathsf{wp}.l$. Equivalence holds if the underlying modal condition semiring S is *extensional*, i.e, if $\langle\!\langle a \rangle\!\rangle \leq \langle\!\langle b \rangle\!\rangle \;\Rightarrow\; a \leq b$ (the converse implication holds by isotony). For instance, $\mathrm{REL}(M)$ is extensional, whereas $\mathrm{TRC}(A)$ is not.

Unlike $\leq$ the relation $\sqsubseteq$ is only a preorder with associated equivalence relation

$$k \equiv l \stackrel{\text{def}}{\Leftrightarrow} k \sqsubseteq l \;\wedge\; l \sqsubseteq k \;.$$

Componentwise, this works out as $(a,t) \equiv (b,u) \;\Leftrightarrow\; t = u \;\wedge\; t \wedge a \leq b \;\wedge\; t \wedge b \leq a$, which further simplifies to

$$(a,t) \equiv (b,u) \;\Leftrightarrow\; t = u \;\wedge\; t \wedge a = t \wedge b \;. \tag{eqc}$$

This agrees with the behaviour of designs described in [13]. For instance,

$$(t \wedge a, t) \equiv (a,t) \equiv (\overline{t} + a, t) \;.$$

Our relations between commands are put into perspective by

Lemma 6.1.

1. $k \leq l \;\Rightarrow\; k \sqsubseteq l \;\Rightarrow\; \mathsf{wp}.k \geq \mathsf{wp}.l.$
2. $k \sqsubseteq l \;\Leftrightarrow\; k \,[]\, l \equiv l.$

Proof. 1. $(a,t) \leq (b,u) \;\Leftrightarrow\; u \leq t \;\wedge\; a \leq b \;\Rightarrow\; u \leq t \;\wedge\; u \wedge a \leq b \;\Leftrightarrow\; (a,t) \sqsubseteq (b,u)$.
The second implication has been shown above.

2. By (eqc) and lattice algebra, $(a,t) \,[]\, (b,u) \equiv (b,u) \;\Leftrightarrow\; (a+b, t \wedge u) \equiv (b,u) \;\Leftrightarrow\; t \wedge u = u \;\wedge\; u \wedge (a+b) = u \wedge b \;\Leftrightarrow\; u \leq t \;\wedge\; u \wedge a + u \wedge b = u \wedge b \;\Leftrightarrow\; u \leq t \;\wedge\; u \wedge a \leq u \wedge b \;\Leftrightarrow\; u \leq t \;\wedge\; u \wedge a \leq b \;\Leftrightarrow\; (a,t) \sqsubseteq (b,u)$. □

This lemma explains our choice for the direction of the $\sqsubseteq$ relation; in many texts on refinement it is used the other way around.

For calculations to work smoothly the following property is important:

Lemma 6.2.

1. *The operations* $[]$ *and* ; *on commands are* $\sqsubseteq$*-isotone.*
2. *The equivalence* $\equiv$ *is a congruence w.r.t.* $[]$ *and* ;.

Proof.

1. Assume $(a,t) \sqsubseteq (b,u)$, i.e., $u \leq t \;\wedge\; u \wedge a \leq b$.
For $[]$ we obtain from the definitions and the universal property of meet

$$\begin{aligned}&(a,t) \,[]\, (c,v) \sqsubseteq (b,u) \,[]\, (c,v) \;\Leftrightarrow\\ &\qquad u \wedge v \leq t \wedge v \;\;\wedge\;\; u \wedge v \wedge a \leq b + c \;\;\wedge\;\; u \wedge v \wedge c \leq b + c \;,\end{aligned}$$

and by isotony all three conjuncts are implied by the assumption. Commutativity of $[]$ shows $\sqsubseteq$-isotony in its second argument.
For the first argument of ; we obtain from the definitions and the universal property of meet

$$\begin{aligned}&(a,t) \,;\, (c,v) \sqsubseteq (b,u) \,;\, (c,v) \;\Leftrightarrow\\ &\qquad u \wedge [\![b]\!]v \leq t \;\;\wedge\;\; u \wedge [\![b]\!]v \leq [\![a]\!]v \;\;\wedge\;\; u \wedge [\![b]\!]v \wedge a \cdot c \leq b \cdot c \;.\end{aligned}$$

The first conjunct is implied by the assumption $u \leq t$. The second one transforms by shunting into $[\![b]\!]v \leq \overline{u} + [\![a]\!]v = [\![u \wedge a]\!]v$, which follows from

the assumption $u \wedge a \leq b$ and antitony of box. The third one transforms by Lemma 3.2 into $[\![b]\!]v \wedge (u \wedge a) \cdot c \leq b \cdot c$, which follows again from $u \wedge a \leq b$ and isotony of composition.
For the second argument of ; we obtain from the definitions

$$(c, v)\,;(a, t) \sqsubseteq (c, v)\,;(b, u) \;\Leftrightarrow\; v \wedge [\![c]\!]u \leq v \wedge [\![c]\!]t \;\wedge\; v \wedge [\![c]\!]u \wedge c \cdot a \leq c \cdot b\ .$$

The first conjunct is implied by the assumption $u \leq t$ and isotony of $[\![c]\!]$. The second one follows by shunting from $c \cdot a \leq c \cdot b + \overline{\overline{c \cdot \overline{u}}}$ which follows from the assumption $a \leq b + \overline{u}$ and isotony of composition and domain.

2. Immediate from 1. □

Finally we look at the lattice structure of commands under $\sqsubseteq$. Note that join and meet can also be defined for preorders; they enjoy all the usual properties except that they are unique only up to the associated equivalence relation.

Lemma 6.3.

1. *The join of commands (a, t) and (b, u) w.r.t. $\sqsubseteq$ is*

$$(a, t) \sqcup (b, u) \;=\; (a + b, t \wedge u) \;=\; (a, t)\,[\!]\,(b, u)\ .$$

2. *If the meet $a \wedge b$ exists then so does the meet of (a, t) and (b, u) w.r.t. $\sqsubseteq$, viz.*

$$(a, t) \wedge (b, u) \;=\; (a \wedge b + \overline{t} \wedge b + \overline{u} \wedge a + \overline{t} \wedge \overline{u}, t + u)\ .$$

Proof.

1. We use indirect equality. For all (c, v) we have

$$\begin{array}{ll} & (a, t) \sqsubseteq (c, v) \;\wedge\; (b, u) \sqsubseteq (c, v) \\ \Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\ & v \leq t \;\wedge\; v \wedge a \leq c \;\wedge\; v \leq u \;\wedge\; v \wedge b \leq c \\ \Leftrightarrow & \quad \{\![\text{ lattice algebra }]\!\} \\ & v \leq t \wedge u \;\wedge\; v \wedge a + v \wedge b \leq c \\ \Leftrightarrow & \quad \{\![\text{ distributivity }]\!\} \\ & v \leq t \wedge u \;\wedge\; v \wedge (a + b) \leq c \\ \Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\ & (a + b, t \wedge u) \sqsubseteq (c, v)\ . \end{array}$$

2. $$\begin{array}{ll} & (c, v) \sqsubseteq (a, t) \;\wedge\; (c, v) \sqsubseteq (b, u) \\ \Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\ & t \leq v \;\wedge\; t \wedge c \leq a \;\wedge\; u \leq v \;\wedge\; u \wedge c \leq b \\ \Leftrightarrow & \quad \{\![\text{ lattice algebra, shunting }]\!\} \\ & t + u \leq v \;\wedge\; c \leq \overline{t} + a \;\wedge\; c \leq \overline{u} + b \\ \Leftrightarrow & \quad \{\![\text{ lattice algebra }]\!\} \\ & t + u \leq v \;\wedge\; c \leq (\overline{t} + a) \wedge (\overline{u} + b)\ , \end{array}$$

so that $(a, t) \wedge (b, u) \;=\; ((\overline{t} + a) \wedge (\overline{u} + b), t + u)$. The form of the expression given in the statement of the lemma results by Boolean algebra. □

In the remainder we will work with the quotient set $\mathrm{C}(S) = \mathrm{COM}(S)/\!\equiv$ most of the time, but still abbreviate the classes $[(a, t)]_{\equiv}$ by their representatives (a, t).

7 Conditionals

To round off the picture, we define a number of conditional commands in terms of the basic ones:

$$t \longrightarrow k \stackrel{\text{def}}{=} (t \wedge 1, \top)\,;k\ , \qquad k \lhd t \rhd l \stackrel{\text{def}}{=} (t \longrightarrow k)\,[\!]\,(\overline{t} \longrightarrow l)\ ,$$
$$\mathsf{assert}\,t \stackrel{\text{def}}{=} \mathsf{skip} \lhd t \rhd \mathsf{loop}\ , \qquad \mathsf{assume}\,t \stackrel{\text{def}}{=} \mathsf{skip} \lhd t \rhd \mathsf{chaos}\ .$$

In particular, these commands are again $\sqsubseteq$-isotone so that $\equiv$ is a congruence w.r.t. them as well. Componentwise, the first two definitions work out to

$$t \longrightarrow (b,u) = (t \wedge b, \overline{t} + u)\ ,$$
$$(b,u) \lhd t \rhd (c,v) = (b \lhd t \rhd c, u \lhd t \rhd v)\ .$$

For the latter one calculates by Boolean algebra

$$\begin{aligned}(\overline{t}+u)\wedge(t+v) \;&=\; \overline{t}\wedge v + t\wedge u + u\wedge v \;=\; \overline{t}\wedge v + t\wedge u + t\wedge u\wedge v + \overline{t}\wedge u\wedge v\\ &=\; t\wedge u + \overline{t}\wedge v \;=\; u \lhd t \rhd v\ .\end{aligned}$$

Let us prove two laws for the two-sided conditional. As an abbreviation, let $p \stackrel{\text{def}}{=} (t \wedge 1, \top), q \stackrel{\text{def}}{=} (\overline{t} \wedge 1, \top)$ and observe that $p\,[\!]\,q = \mathsf{skip}$. Then, first,

$$k \lhd t \rhd k \underset{\text{(defs.)}}{=} p\,;k\,[\!]\,q\,;k \underset{\text{(dist.)}}{=} (p\,[\!]\,q)\,;k \underset{\text{(above)}}{=} \mathsf{skip}\,;k \underset{\text{(neut.)}}{=} k\ .$$

Second,

$$(k \lhd t \rhd l)\,;m \underset{\text{(defs.)}}{=} (p;k\,[\!]\,q;l)\,;m \underset{\text{(dist.)}}{=} p;k;m\,[\!]\,q;l;m \underset{\text{(defs.)}}{=} (k\,;m) \lhd t \rhd (l\,;m)\ .$$

From these two laws it follows that $k \lhd t \rhd l$ preserves feasibility, whereas $t \longrightarrow k$ does this only in the uninteresting case $t = \top$. Therefore also $\mathsf{assert}\,t$ and $\mathsf{assume}\,t$ are feasible.

Finally, we prove a more specialised property that we will need later on.

Lemma 7.1. $(a,t)\,;(b,u) \lhd z \rhd (c,\top) = (z \wedge a, t \lhd z \rhd \top)\,;(b,u)\,[\!]\,(\overline{z} \wedge c, \top)$.

Proof.
$$\begin{aligned}&((a,t)\,;(b,u)) \lhd z \rhd (c,\top)\\ =\;& \quad \{\![\text{ command composition }]\!\}\\ &(a \cdot b, t \wedge [\![a]\!]u) \lhd z \rhd (c,\top)\\ =\;& \quad \{\![\text{ command conditional }]\!\}\\ &(a \cdot b \lhd z \rhd c, t \wedge [\![a]\!]u \lhd z \rhd \top)\\ =\;& \quad \{\![\text{ definition of conditional }]\!\}\\ &(z \wedge (a \cdot b) + \overline{z} \wedge c, z \wedge t \wedge [\![a]\!]u + \overline{z})\\ =\;& \quad \{\![\text{ Lemma 3.2 and Boolean algebra }]\!\}\\ &((z \wedge a) \cdot b + \overline{z} \wedge c, (z \wedge t + \overline{z}) \wedge ([\![a]\!]u + \overline{z}))\\ =\;& \quad \{\![\text{ definition of conditional and box property }]\!\}\\ &((z \wedge a) \cdot b + \overline{z} \wedge c, (t \lhd z \rhd \top) \wedge [\![z \wedge a]\!]u)\end{aligned}$$

$$
\begin{array}{ll}
= & \{\![\text{ command disjunction }]\!\} \\
& ((z \wedge a) \cdot b, (t \lhd z \rhd \top) \wedge [\![z \wedge a]\!] u) \mathbin{[]} (\overline{z} \wedge c, \top) \\
= & \{\![\text{ command composition }]\!\} \\
& (z \wedge a, t \lhd z \rhd \top) \,;\, (b, u) \mathbin{[]} (\overline{z} \wedge c, \top).
\end{array}
$$

□

8 Feasible Normal Designs and Demonic Semantics

We have already seen that command (a, t) is feasible if and only if $t \leq \ulcorner a$ and thus define the set of feasible commands as $\mathrm{F}(S) = \{(a, t) | (a, t) \in \mathrm{C}(S) \ \wedge \ t \leq \ulcorner a\}$. The aim of the present section is to establish a correspondence between feasible commands and elements of the underlying semiring S. It will be used to define the demonic operators on S and is an abstract version of the mappings $\mathcal{I}_d$ and $\mathcal{H}_d$ on relations defined in [11], and given by

$$
\begin{array}{ll}
E : \mathrm{F}(S) \ \to \ S \ , & D : S \ \to \ \mathrm{F}(S) \ , \\
E((a, t)) \stackrel{\text{def}}{=} \ t \wedge a \ , & D(a) \stackrel{\text{def}}{=} \ (a, \ulcorner a) \ .
\end{array}
$$

We will abbreviate $E((a, t))$ to $E(a, t)$. This function, which would make sense even for arbitrary pairs, describes the demonic view of (a, t) that discards all input states of a for which both termination and nontermination may occur, i.e., all those characterised by $\overline{t} \wedge \ulcorner a$. For the resulting semiring element, no extra termination information is needed; this is reflected in the definition of D.

Lemma 8.1. *E and D are inverse to each other, in one case up to $\equiv$.*

Proof. By Lemma 4.1(7), feasibility, and refinement ordering,

$$D(E(a, t)) = D(t \wedge a) = (t \wedge a, \ulcorner(t \wedge a)) = (t \wedge a, t \wedge \ulcorner a) = (t \wedge a, t) \equiv (a, t).$$

Conversely, by (cd1) we have $E(D(a)) = E(a, \ulcorner a) = \ulcorner a \wedge a = a$. □

We will give a demonic ordering and demonic operations on S for modelling total correctness. In contrast to [8], where such an ordering and operations are introduced by new definitions, we can derive these using the correspondence from Lemma 8.1. The demonic refinement ordering is

$$a \sqsubseteq\!\!\!\!\sqsubseteq b \stackrel{\text{def}}{=} D(a) \sqsubseteq D(b) \ \Leftrightarrow \ (a, \ulcorner a) \sqsubseteq (b, \ulcorner b) \ \Leftrightarrow \ \ulcorner b \leq \ulcorner a \ \wedge \ \ulcorner b \wedge a \leq b.$$

By (eqc) and (cd1) $\sqsubseteq\!\!\!\!\sqsubseteq$ is antisymmetric, i.e., a partial order. Thus, by Lemma 8.1, the mappings E and D are order isomorphisms between $(\mathrm{F}(S), \sqsubseteq)$ and $(S, \sqsubseteq\!\!\!\!\sqsubseteq)$. Since chaos is the greatest element of $\mathrm{COM}(S)$, and therefore also of $\mathrm{F}(S)$, the $\sqsubseteq\!\!\!\!\sqsubseteq$-greatest element of S is $E(\mathsf{chaos}) = E(\top, 0) = 0$. In general, however, there is no $\sqsubseteq\!\!\!\!\sqsubseteq$-smallest element, since the corresponding least element fail of $\mathrm{COM}(S)$ is not feasible.

The demonic composition is

$$\begin{aligned} a \mathbin{\square} b &\stackrel{\text{def}}{=} E(D(a)\,;D(b)) = E((a,{\ulcorner}a)\,;(b,{\ulcorner}b)) = E(a\cdot b, {\ulcorner}a \wedge [\![a]\!]{\ulcorner}b) \\ &= {\ulcorner}a \wedge [\![a]\!]{\ulcorner}b \wedge a\cdot b = [\![a]\!]{\ulcorner}b \wedge a\cdot b, \end{aligned}$$

since $a\cdot b \le {\ulcorner}(a\cdot b) \le {\ulcorner}a$ by (cd1) and Lemma 4.1(10). The unit skip of $\mathrm{COM}(S)$ is feasible, thus $E(\mathsf{skip}) = E(1,\top) = 1$ is also the unit of demonic composition.

The demonic choice (which coincides with the $\sqsubseteq$-join) is

$$\begin{aligned} a \sqcup b &\stackrel{\text{def}}{=} E(D(a) \mathbin{[]} D(b)) = E((a,{\ulcorner}a) \mathbin{[]} (b,{\ulcorner}b)) = E(a+b, {\ulcorner}a \wedge {\ulcorner}b) \\ &= {\ulcorner}a \wedge {\ulcorner}b \wedge (a+b). \end{aligned}$$

The demonic meet, whenever it exists, is, by Lemma 6.3.2,

$$\begin{aligned} a \sqcap b &\stackrel{\text{def}}{=} E(D(a)\wedge D(b)) = E((a,{\ulcorner}a)\wedge(b,{\ulcorner}b)) \\ &= E(a\wedge b + \overline{{\ulcorner}a}\wedge b + \overline{{\ulcorner}b}\wedge a, {\ulcorner}a + {\ulcorner}b) \\ &= ({\ulcorner}a + {\ulcorner}b)\wedge(a\wedge b + \overline{{\ulcorner}a}\wedge b + \overline{{\ulcorner}b}\wedge a) \\ &= a\wedge b + \overline{{\ulcorner}a}\wedge b + \overline{{\ulcorner}b}\wedge a, \end{aligned}$$

since $a\wedge b + \overline{{\ulcorner}a}\wedge b + \overline{{\ulcorner}b}\wedge a \le a+b+a = a+b \le {\ulcorner}a + {\ulcorner}b$ by (cd1). The necessary and sufficient condition for its existence is the feasibility of $D(a)\wedge D(b)$, hence,

$$\begin{aligned} & D(a)\wedge D(b) \in \mathrm{F}(S) \\ \Leftrightarrow\quad & \{\![\text{ above calculation, feasibility }]\!\} \\ & {\ulcorner}a + {\ulcorner}b \le {\ulcorner}(a\wedge b + \overline{{\ulcorner}a}\wedge b + \overline{{\ulcorner}b}\wedge a) \\ \Leftrightarrow\quad & \{\![\text{ Lemma 4.1(2,7) }]\!\} \\ & {\ulcorner}a + {\ulcorner}b \le {\ulcorner}(a\wedge b) + \overline{{\ulcorner}a}\wedge{\ulcorner}b + \overline{{\ulcorner}b}\wedge{\ulcorner}a \\ \Leftrightarrow\quad & \{\![\text{ shunting and de Morgan }]\!\} \\ & ({\ulcorner}a + {\ulcorner}b)\wedge({\ulcorner}a + \overline{{\ulcorner}b})\wedge({\ulcorner}b + \overline{{\ulcorner}a}) \le {\ulcorner}(a\wedge b) \\ \Leftrightarrow\quad & \{\![\text{ Boolean algebra }]\!\} \\ & {\ulcorner}a\wedge{\ulcorner}b \le {\ulcorner}(a\wedge b), \end{aligned}$$

which is equivalent to ${\ulcorner}(a\wedge b) = {\ulcorner}a\wedge{\ulcorner}b$.

Finally, the demonic conditional is

$$\begin{aligned} E(D(a) \lhd t \rhd D(b)) &= E((a,{\ulcorner}a) \lhd t \rhd (b,{\ulcorner}b)) = E(a \lhd t \rhd b, {\ulcorner}a \lhd t \rhd {\ulcorner}b) \\ &= ({\ulcorner}a \lhd t \rhd {\ulcorner}b)\wedge(a \lhd t \rhd b) = ({\ulcorner}a\wedge a) \lhd t \rhd ({\ulcorner}b \wedge b) \\ &= a \lhd t \rhd b \end{aligned}$$

by Boolean algebra and (cd1). Hence we do not introduce a new notation for it.

The solutions to demonic recursions are also derived according to the order isomorphism and the following general lemma.

Lemma 8.2. *1. Let $(A,\le)$ and $(B,\sqsubseteq)$ be partial orders, $h : A \to B$ an order isomorphism, $f : A \to A$, and $g : B \to B$ such that $h\circ f = g\circ h$.*
Then f is order preserving if and only if g is order preserving.

2. *Furthermore, let f be order preserving and f° a fixed point of f. Then $h(f^\circ)$ is a fixed point of g.*
3. *Furthermore, let $f^\bot$ be the least fixed point of f, and $f^\top$ the greatest. Then $h(f^\bot)$ is the least fixed point of g, and $h(f^\top)$ the greatest.*

Proof. 1. Assume $x \leq y$. Then

$$f(x) \leq f(y) \;\Leftrightarrow\; h(f(x)) \sqsubseteq h(f(y)) \;\Leftrightarrow\; g(h(x)) \sqsubseteq g(h(y)) \;,$$

which, together with surjectivity of h shows the claim.
2. $g(h(f^\circ)) = h(f(f^\circ)) = h(f^\circ)$.
3. $h(f^\bot)$ and $h(f^\top)$ are fixed points of g by 2. Let g° be a fixed point of g. Swapping the partial orders, 2. states that $h^{-1}(g^\circ)$ is a fixed point of f. Hence, $f^\bot \leq h^{-1}(g^\circ) \leq f^\top$. By order isomorphism, $h(f^\bot) \sqsubseteq g^\circ \sqsubseteq h(f^\top)$.

□

Corollary 8.3. *Let $f : S \to S$ be $\mathbb{\sqsubseteq}$-preserving. Then the least fixed point of f with respect to $\mathbb{\sqsubseteq}$ is $\mu_{\mathbb{\sqsubseteq}}(f) = E(\mu_{\sqsubseteq}(D \circ f \circ E))$. Analogously, the greatest fixed point is $\nu_{\mathbb{\sqsubseteq}}(f) = E(\nu_{\sqsubseteq}(D \circ f \circ E))$.*

9 The Kleene Algebra of Commands

A *Kleene algebra* is a structure $(K, ^*)$ such that K is an idempotent semiring and the star * satisfies the unfold and induction laws

$$\begin{array}{rcl@{\qquad\qquad}rcl} 1 + a \cdot a^* & \leq & a^* & 1 + a^* \cdot a & \leq & a^* \\ b + a \cdot c \leq c & \Rightarrow & a^* \cdot b \leq c & b + c \cdot a \leq c & \Rightarrow & b \cdot a^* \leq c \end{array}$$

for $a, b, c \in K$ [14]. Hence $a^* \cdot b$ is the least fixed point of the mapping $\lambda x.a \cdot x + b$.

The following Lemma proves a generalisation to condition semirings of the left induction law from Kleene algebra.

Lemma 9.1. $v \wedge (b + c \cdot a) \leq c \;\Rightarrow\; v \wedge b \cdot a^* \leq c$.

Proof. By Boolean algebra and Lemma 3.2, $v \wedge (b + c \cdot a) = v \wedge b + v \wedge (c \cdot a) = v \wedge b + (v \wedge c) \cdot a = v \wedge b + (v \wedge (c + \overline{v})) \cdot a = v \wedge b + v \wedge ((c + \overline{v}) \cdot a) = v \wedge (b + (c + \overline{v}) \cdot a)$. Hence, by the above calculation, shunting, Kleene star induction and shunting again,

$$\begin{array}{c} v \wedge (b + c \cdot a) \leq c \;\Leftrightarrow\; v \wedge (b + (c + \overline{v}) \cdot a) \leq c \;\Leftrightarrow\; b + (c + \overline{v}) \cdot a \leq c + \overline{v} \\ \Leftrightarrow\; b \cdot a^* \leq c + \overline{v} \;\Leftrightarrow\; v \wedge b \cdot a^* \leq c \;. \end{array}$$

□

Lemma 9.2. *1. $v \leq [\![a]\!] v \;\Leftrightarrow\; a \cdot \overline{v} \leq \overline{v}$.*
2. $v \leq t \wedge [\![a]\!] v \;\Rightarrow\; v \leq [\![a^*]\!] t$.

Proof. 1. By the definition of box, Boolean algebra, and (GCc),

$$v \leq [\![a]\!] v \;\Leftrightarrow\; v \leq \overline{\Box(a \cdot \overline{v})} \;\Leftrightarrow\; \Box(a \cdot \overline{v}) \leq \overline{v} \;\Leftrightarrow\; a \cdot \overline{v} \leq \overline{v}.$$

2.
$$
\begin{array}{ll}
 & v \le t \wedge [\![a]\!] v \\
\Leftrightarrow & \quad \{\![\text{ Boolean algebra }]\!\} \\
 & v \le t \ \wedge \ v \le [\![a]\!] v \\
\Leftrightarrow & \quad \{\![\text{ Boolean algebra and 1. }]\!\} \\
 & \overline{t} \le \overline{v} \ \wedge \ a \cdot \overline{v} \le \overline{v} \\
\Leftrightarrow & \quad \{\![\text{ Boolean algebra }]\!\} \\
 & \overline{t} + a \cdot \overline{v} \le \overline{v} \\
\Rightarrow & \quad \{\![\text{ Kleene star induction }]\!\} \\
 & a^* \cdot \overline{t} \le \overline{v} \\
\Leftrightarrow & \quad \{\![\text{ (GCc) }]\!\} \\
 & \overline{\lceil}(a^* \cdot \overline{t}) \le \overline{v} \\
\Leftrightarrow & \quad \{\![\text{ Boolean algebra and definition of box }]\!\} \\
 & v \le \overline{\lceil}(a^* \cdot \overline{t}) = [\![a^*]\!] t.
\end{array}
$$

□

We will now lift the Kleene star from the underlying semiring S to the quotient command semiring $\mathrm{C}(S)$. This is needed to calculate the least fixed point of loops. Since the right annihilation law fails to hold in $\mathrm{C}(S)$ the resulting structure is called a *weak Kleene algebra* [18].

Theorem 9.3. $(a,t)^* = (a^*, [\![a^*]\!] t)$.

Proof. By uniqueness of star it suffices to show the star axioms for $(a^*, [\![a^*]\!] t)$.

1. By command operations, properties of box, and the Kleene unfold axiom,

$$
\begin{aligned}
\mathsf{skip} \,[]\, (a,t) \,;\, (a^*, [\![a^*]\!] t) &= (1, \top) \,[]\, (a \cdot a^*, t \wedge [\![a]\!] [\![a^*]\!] t) \\
&= (1 + a \cdot a^*, [\![1]\!] t \wedge [\![a \cdot a^*]\!] t) = (a^*, [\![1 + a \cdot a^*]\!] t) = (a^*, [\![a^*]\!] t).
\end{aligned}
$$

2. For similar reasons,

$$
\begin{aligned}
\mathsf{skip} \,[]\, (a^*, [\![a^*]\!] t) \,;\, (a,t) &= (1, \top) \,[]\, (a^* \cdot a, [\![a^*]\!] t \wedge [\![a^*]\!] t) \\
&= (1 + a^* \cdot a, [\![a^*]\!] t) = (a^*, [\![a^*]\!] t).
\end{aligned}
$$

3. By command operations and ordering,

$$
\begin{aligned}
(b,u) \,[]\, (a,t) \,;\, (c,v) \sqsubseteq (c,v) &\Leftrightarrow (b,u) \,[]\, (a \cdot c, t \wedge [\![a]\!] v) \sqsubseteq (c,v) \\
&\Leftrightarrow (b + a \cdot c, u \wedge t \wedge [\![a]\!] v) \sqsubseteq (c,v) \\
&\Leftrightarrow v \le t \wedge u \wedge [\![a]\!] v \ \wedge \ v \wedge (b + a \cdot c) \le c.
\end{aligned}
$$

By Lemma 9.2.1, $a \cdot \overline{v} \le \overline{v}$, hence $b + a \cdot (c + \overline{v}) = b + a \cdot c + a \cdot \overline{v} \le c + \overline{v}$. By Kleene star induction, $a^* \cdot b \le c + \overline{v}$, thus $v \wedge a^* \cdot b \le c$ by shunting. Moreover, $v \le [\![a^*]\!](t \wedge u)$ by Lemma 9.2.2.
By command operations, properties of box, and the last two facts,

$$
(a^*, [\![a^*]\!] t) \,;\, (b,u) = (a^* \cdot b, [\![a^*]\!] t \wedge [\![a^*]\!] u) = (a^* \cdot b, [\![a^*]\!](t \wedge u)) \sqsubseteq (c,v).
$$

4. By command operations and ordering,

$$\begin{aligned}(b,u)\,[]\,(c,v)\,;(a,t)\sqsubseteq(c,v) &\Leftrightarrow (b,u)\,[]\,(c\cdot a, v\wedge[\![c]\!]t)\sqsubseteq(c,v)\\ &\Leftrightarrow (b+c\cdot a, u\wedge v\wedge[\![c]\!]t)\sqsubseteq(c,v)\\ &\Leftrightarrow v\leq u\ \wedge\ v\leq[\![c]\!]t\ \wedge\ v\wedge(b+c\cdot a)\leq c.\end{aligned}$$

By Lemma 9.1, $v\wedge b\cdot a^*\leq c$. Moreover, $v\leq[\![c]\!]t\leq[\![v\wedge b\cdot a^*]\!]t=\overline{v}+[\![b\cdot a^*]\!]t$ by box properties. By $v\leq u$ and shunting, $v\leq u\wedge[\![b\cdot a^*]\!]t$.
Together, by command operations, and properties of box,

$$(b,u)\,;(a^*,[\![a^*]\!]t)=(b\cdot a^*,u\wedge[\![b]\!][\![a^*]\!]t)=(b\cdot a^*,u\wedge[\![b\cdot a^*]\!]t)\sqsubseteq(c,v).$$

□

10 The Omega Algebra of Commands

A *weak omega algebra* is a structure $(K,{}^\omega)$ such that K is a weak Kleene algebra and the omega ${}^\omega$ satisfies the unfold and co-induction laws

$$a^\omega=a\cdot a^\omega$$
$$c\leq a\cdot c+b\ \Rightarrow\ c\leq a^\omega+a^*\cdot b$$

for $a,b,c\in K$ [16]. It follows that $a^\omega+a^*\cdot b$ is the greatest fixed point of the mapping $\lambda x.a\cdot x+b$.

In contrast to this definition, an *omega algebra* requires K to be a Kleene algebra but weakens the unfold axiom to $a^\omega\leq a\cdot a^\omega$ [4]. The reverse inequality need not hold in absence of the right annihilation law [16].

For the greatest fixed point of loops, we will now lift the omega operator from the underlying semiring S to the quotient command semiring $\mathrm{C}(S)$. To calculate the weak omega operator we need the analogue of the convergence algebra defined in [18]. The convergence operation $\triangle : S\ \rightarrow\ \mathsf{cond}(S)$ satisfies the unfold and co-induction laws

$$[\![a]\!](\triangle a)\leq\triangle a$$
$$t\wedge[\![a]\!]u\leq u\ \Rightarrow\ \triangle a\wedge[\![a^*]\!]t\leq u$$

The condition $\triangle a$ characterises the states from which no infinite transition paths emerge. The following lemma states a few properties of convergence.

Lemma 10.1. *1. $\triangle a\wedge[\![a^*]\!]t$ is the least (pre-)fixed point of $\lambda u.t\wedge[\![a]\!]u$.*
In particular, $\triangle a$ is the least (pre-)fixed point of $[\![a]\!]$.
2. $\overline{\top a}\leq\triangle a\leq\overline{\top a^\omega}$ and hence $\triangle a\wedge a^\omega=0$.
3. $\triangle$ is antitone.
4. $[\![a^*]\!](\triangle a)=[\![a\cdot a^*]\!](\triangle a)=[\![a]\!](\triangle a)=\triangle a$.

Proof. 1. By box properties, and the Kleene star and convergence unfold laws, $t\wedge[\![a]\!](\triangle a\wedge[\![a^*]\!]t)=t\wedge[\![a]\!](\triangle a)\wedge[\![a]\!][\![a^*]\!]t\leq\triangle a\wedge[\![1+a\cdot a^*]\!]t=\triangle a\wedge[\![a^*]\!]t$.
Hence, by the co-induction axiom, $\triangle a\wedge[\![a^*]\!]t$ is the least pre-fixed point of $\lambda u.t\wedge[\![a]\!]u$. Then, it is also the least fixed point [8].
Choose $t=\top$ for the special case, using $[\![a^*]\!]\top=\top$.

2. By condition semiring properties, the definition of box, and the unfold law,

$$\overline{\Gamma a} = \overline{\Gamma(a \cdot \top)} \leq \overline{\Gamma(a \cdot \overline{\triangle a})} = [\![a]\!](\triangle a) = \triangle a.$$

   By definition of box, Lemma 4.1(8), and the omega axioms,

$$[\![a]\!]\overline{\Gamma a^\omega} = \overline{\Gamma(a \cdot \Gamma a^\omega)} \leq \overline{\Gamma(a \cdot a^\omega)} = \overline{\Gamma a^\omega}.$$

   Hence, $\overline{\Gamma a^\omega}$ is a fixed point of $[\![a]\!]$, and $\triangle a \leq \overline{\Gamma a^\omega}$ by 1.
3. By antitony of box and 1, $a \leq b \Rightarrow [\![b]\!] \leq [\![a]\!] \Rightarrow \triangle b \leq \triangle a$.
4. By box properties and 1, $[\![1]\!](\triangle a) = \triangle a = [\![a]\!](\triangle a)$. Moreover, by star and box properties,

$$[\![a]\!][\![a^*]\!](\triangle a) = [\![a \cdot a^*]\!](\triangle a) = [\![a^* \cdot a]\!](\triangle a) = [\![a^*]\!][\![a]\!](\triangle a) = [\![a^*]\!](\triangle a) \ ,$$

   so that $[\![a^*]\!](\triangle a)$ is a fixed point of $[\![a]\!]$. The remaining inequalities follow by antitony of the box operator. □

In the special case of REL(M), $\triangle a = \overline{a^\omega}$ can be proved by Corollary 4.3.

Theorem 10.2. $(a,t)^\omega = (a^\omega, \triangle a \wedge [\![a^*]\!]t) \equiv (0, \triangle a \wedge [\![a^*]\!]t)$.

Proof. We prove that $(a^\omega, \triangle a \wedge [\![a^*]\!]t)$ satisfies the weak omega axioms. The claimed $\equiv$-relation then follows by Lemma 10.1.2.

1. By command operations, the fixed-point property of a^ω and Lemma 10.1.1,

$$(a,t)\,;(a^\omega, \triangle a \wedge [\![a^*]\!]t) \;=\; (a \cdot a^\omega, t \wedge [\![a]\!](\triangle a \wedge [\![a^*]\!]t)) \;=\; (a^\omega, \triangle a \wedge [\![a^*]\!]t) \ .$$

2. Assume

$$(c,v) \sqsubseteq (a,t)\,;(c,v) \,[]\, (b,u) = (a \cdot c, t \wedge [\![a]\!]v) \,[]\, (b,u) = (a \cdot c + b, t \wedge [\![a]\!]v \wedge u),$$

   which is equivalent to $w \leq v \;\wedge\; w \wedge c \leq a \cdot c + b$, where $w \stackrel{\text{def}}{=} t \wedge u \wedge [\![a]\!]v$. We have to show

$$\begin{aligned}(c,v) &\sqsubseteq (a^\omega, \triangle a \wedge [\![a^*]\!]t) \,[]\, (a^*, [\![a^*]\!]t)\,;(b,u)\\ &= (a^\omega + a^* \cdot b, \triangle a \wedge [\![a^*]\!]t \wedge [\![a^*]\!]t \wedge [\![a^*]\!]u)\\ &= (a^\omega + a^* \cdot b, \triangle a \wedge [\![a^*]\!](t \wedge u)) \ ,\end{aligned}$$

   which by definitions and shunting is equivalent to $x \leq v \;\wedge\; c \leq a^\omega + a^* \cdot b + \overline{x}$, where $x \stackrel{\text{def}}{=} \triangle a \wedge [\![a^*]\!](t \wedge u)$.
   The first conjunct follows from the first assumption by convergence co-induction. For the second one transforms the second assumption by shunting into $c \leq a \cdot c + b + \overline{w}$. By omega co-induction $c \leq a^\omega + a^* \cdot b + a^* \cdot \overline{w}$, so we are done if we can show $a^* \cdot \overline{w} \leq \overline{x}$.
   We have $a^* \cdot \overline{w} \leq \Gamma(a^* \cdot \overline{w}) = \overline{[\![a^*]\!]w}$, so that it suffices to show $\overline{[\![a^*]\!]w} \leq \overline{x}$, equivalently $x \leq [\![a^*]\!]w$. Now, by box and star properties,

$$\begin{aligned}x \leq [\![a^*]\!]w \;&\Leftrightarrow\; x \leq [\![a^*]\!](t \wedge u) \wedge [\![a^*]\!][\![a]\!]v\\ &\Leftrightarrow\; x \leq [\![a^*]\!](t \wedge u) \;\wedge\; x \leq [\![a^*]\!]v \ .\end{aligned}$$

The first conjunct holds by definition of x. For the second one, since $x \leq v$ as shown above, it suffices by isotony of $[\![a^*]\!]$ to show $x \leq [\![a^*]\!]x$. Now, by disjunctivity of $[\![a^*]\!]$, Lemma 10.1.4 and star properties,

$$\begin{aligned}[\![a^*]\!]x \;&=\; [\![a^*]\!](\triangle a \wedge [\![a^*]\!](t \wedge u)) \;=\; [\![a^*]\!](\triangle a) \wedge [\![a^*]\!][\![a^*]\!](t \wedge u) \\ &=\; \triangle a \wedge [\![a^*]\!][\![a^*]\!](t \wedge u) \;=\; \triangle a \wedge [\![a^*]\!](t \wedge u) \;=\; x \;.\end{aligned}$$

□

11 The Demonic While Loop

The Kleene and omega algebraic properties of commands finally enable the calculation of the least and greatest fixed points of the function that describes the demonic while loop.

Theorem 11.1.

1. $\mu_{\sqsubseteq}(\lambda x.a \circ x \lhd t \rhd 1) = [\![(t \wedge a)^*]\!](\overline{t} + \ulcorner a) \wedge (t \wedge a)^* \cdot (\overline{t} \wedge 1)$.
2. $\nu_{\sqsubseteq}(\lambda x.a \circ x \lhd t \rhd 1) = \triangle(t \wedge a) \wedge \mu_{\sqsubseteq}(\lambda x.a \circ x \lhd t \rhd 1)$.

Proof. We calculate the fixed points according to Corollary 8.3.

1. For the least fixed point,

$$\begin{aligned}
& \mu_{\sqsubseteq}(\lambda x.a \circ x \lhd t \rhd 1) \\
= \quad & \{\![\text{ Corollary 8.3 }]\!\} \\
& E(\mu_{\sqsubseteq}(\lambda(b,u).D(a \circ E(b,u) \lhd t \rhd 1))) \\
= \quad & \{\![\text{ demonic conditional: } D(a \lhd t \rhd b) = D(a) \lhd t \rhd D(b) \text{ }]\!\} \\
& E(\mu_{\sqsubseteq}(\lambda(b,u).D(a \circ E(b,u)) \lhd t \rhd D(1))) \\
= \quad & \{\![\text{ demonic composition: } D(a \circ b) = D(a) \,;\, D(b) \text{ }]\!\} \\
& E(\mu_{\sqsubseteq}(\lambda(b,u).D(a) \,;\, D(E(b,u)) \lhd t \rhd D(E(\mathsf{skip})))) \\
= \quad & \{\![\text{ Lemma 8.1 }]\!\} \\
& E(\mu_{\sqsubseteq}(\lambda(b,u).(a, \ulcorner a) \,;\, (b,u) \lhd t \rhd (1, \top))) \\
= \quad & \{\![\text{ Lemma 7.1 }]\!\} \\
& E(\mu_{\sqsubseteq}(\lambda(b,u).(t \wedge a, \ulcorner a \lhd t \rhd \top) \,;\, (b,u) \mathbin{[\!]} (\overline{t} \wedge 1, \top))) \\
= \quad & \{\![\text{ definition of conditional and Boolean algebra }]\!\} \\
& E(\mu_{\sqsubseteq}(\lambda(b,u).(t \wedge a, \overline{t} + \ulcorner a) \,;\, (b,u) \mathbin{[\!]} (\overline{t} \wedge 1, \top))) \\
= \quad & \{\![\text{ } a^* \cdot b \text{ is the least fixed point of } (\lambda x.a \cdot x + b) \text{ }]\!\} \\
& E((t \wedge a, \overline{t} + \ulcorner a)^* \,;\, (\overline{t} \wedge 1, \top)) \\
= \quad & \{\![\text{ Theorem 9.3 }]\!\} \\
& E(((t \wedge a)^*, [\![(t \wedge a)^*]\!](\overline{t} + \ulcorner a)) \,;\, (\overline{t} \wedge 1, \top)) \\
= \quad & \{\![\text{ command composition }]\!\} \\
& E((t \wedge a)^* \cdot (\overline{t} \wedge 1), [\![(t \wedge a)^*]\!](\overline{t} + \ulcorner a) \wedge [\![(t \wedge a)^*]\!]\top) \\
= \quad & \{\![\text{ box properties and definition of } E \text{ }]\!\} \\
& [\![(t \wedge a)^*]\!](\overline{t} + \ulcorner a) \wedge (t \wedge a)^* \cdot (\overline{t} \wedge 1).
\end{aligned}$$

2. For the greatest fixed point,

$$
\begin{array}{ll}
 & \nu_{\sqsubseteq}(\lambda x.a \,\square\, x \lhd t \rhd 1) \\
= & \quad \{\![\text{ calculation as in 1. }]\!\} \\
 & E(\nu_{\sqsubseteq}(\lambda(b,u).(t \wedge a, \overline{t} + \ulcorner a) \,;\, (b,u) \,[]\, (\overline{t} \wedge 1, \top))) \\
= & \quad \{\![\; a^* \cdot b + a^\omega \text{ is the greatest fixed point of } (\lambda x.a \cdot x + b) \;]\!\} \\
 & E((t \wedge a, \overline{t} + \ulcorner a)^* \,;\, (\overline{t} \wedge 1, \top) \,[]\, (t \wedge a, \overline{t} + \ulcorner a)^\omega) \\
= & \quad \{\![\text{ Theorem 10.2 and calculation as in 1. }]\!\} \\
 & E(((t \wedge a)^* \cdot (\overline{t} \wedge 1), [\![(t \wedge a)^*]\!](\overline{t} + \ulcorner a)) \,[] \\
 & \quad (0, \triangle(t \wedge a) \wedge [\![(t \wedge a)^*]\!](\overline{t} + \ulcorner a))) \\
= & \quad \{\![\text{ command disjunction }]\!\} \\
 & E((t \wedge a)^* \cdot (\overline{t} \wedge 1), \triangle(t \wedge a) \wedge [\![(t \wedge a)^*]\!](\overline{t} + \ulcorner a)) \\
= & \quad \{\![\text{ 1. }]\!\} \\
 & \triangle(t \wedge a) \wedge \mu_{\sqsubseteq}(\lambda x.a \,\square\, x \lhd t \rhd 1).
\end{array}
$$

□

12 Conclusion

The treatment has shown that almost all of the standard theory of normal designs carries over to the general case. One can even prove a generalisation of the fixed point theorem 3.1.6 of [13] that allows an alternative derivation of the omega operator for commands. It should be noted that the operations of complement and meet are not required for all semiring elements but only on the conditions.

By defining refinement as in Section 6 we committed ourselves to total correctness. The branch of general correctness, exemplified by the normal prescriptions of [10], can be explored by taking the natural order of commands given in Theorem 5.1 instead. Since then, however, the connection starting with Lemma 8.1 no longer holds, the loop semantics cannot be calculated in the same way. An alternative treatment using the Egli-Milner order is given in [18]. The treatment of conditions as right ideals has been an interesting exercise but is not as smooth as using tests, not least because of its lack of symmetry.

Finally, we would like to mention that the command semiring can actually be made into a modal semiring itself, so that the general soundness and completeness proof for the associated Hoare logic can directly be applied to commands (see [17] for details).

It is to be hoped that the generalised results will be of use for handling trace semantics and other semantical models by taking algebras like TRC(A) and their properties into account, thus dealing with healthiness conditions such as (R1)–(R3) of UTP in a purely algebraic fashion. The presented method could also serve as a model for the extension by parameters that describe further observations as proposed in [13].

Acknowledgement: We are grateful to P. Höfner, Kim Solin and the anonymous referees for helpful discussions and remarks.

References

1. R. C. Backhouse, J. van der Woude: Demonic operators and monotype factors. Mathematical Structures in Computer Science 3, 417–433 (1993)
2. R. Berghammer, H. Zierer: Relational algebraic semantics of deterministic and non-deterministic programs. Theoretical Computer Science 43, 123–147 (1986)
3. M. Broy, R. Gnatz, M. Wirsing: Semantics of nondeterministic and non-continuous constructs. In F.L. Bauer, M. Broy (eds.): Program construction. Lecture Notes in Computer Science 69. Springer 1979, 553–592
4. E. Cohen: Separation and reduction. In R. Backhouse, J. Oliveira (eds.): Mathematics of Program Construction. Lecture Notes in Computer Science 1837, Springer 2000, 45–59
5. J. Desharnais, N. Belkhiter, S.B.M. Sghaier, F. Tchier, A. Jaoua, A. Mili, and N. Zaguia: Embedding a demonic semilattice in a relation algebra. Theoretical Computer Science 149, 333–360 (1995)
6. J. Desharnais, A. Mili, T.T. Nguyen: Refinement and demonic semantics. In C. Brink, W. Kahl, G. Schmidt (eds): Relational methods in computer science, Chapter 11. Springer 1997, 166–183
7. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. ACM TOCL (to appear)
8. J. Desharnais, B. Möller, F. Tchier: Kleene under a modal demonic star. Journal on Logic and Algebraic Programming, Special Issue on Relation Algebra and Kleene Algebra, 2006 (to appear)
9. H. Doornbos: A relational model of programs without the restriction to Egli-Milner-monotone constructs. In E.-R. Olderog (ed.): Programming concepts, methods and calculi. North-Holland 1994, 363–382
10. S. Dunne: Recasting Hoare and He's unifying theory of programs in the context of general correctness. In Butterfield, A., Strong, G., Pahl, C., eds.: 5th Irish Workshop on Formal Methods. EWiC, The British Computer Society, 2001
11. W. Guttmann: Non-termination in Unifying Theories of Programming. In Düntsch, I., Winter, M., eds.: 8th International Conference on Relational Methods in Computer Science (RelMiCS 8/AKA 3), Computer Science Department, Brock University, St. Catharines, Ontario, Canada 2005, 87–94
12. W. Guttmann, B. Möller: Modal design algebra. Institut für Informatik, Universität Augsburg, Report 2005-15
13. C.A.R. Hoare, J. He: Unifying theories of programming. Prentice Hall 1998
14. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation 110, 366–390 (1994)
15. D. Kozen: Kleene algebra with tests. ACM TOPLAS 19:427–443 (1997)
16. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. Lecture Notes in Computer Science 3125. Springer 2004, 252–273
17. B. Möller, G. Struth: Modal Kleene algebra and partial correctness. In C. Rattray, S. Maharaj, C. Shankland (eds.): Algebraic methodology and software technology. Lecture Notes in Computer Science 3116. Springer 2004, 379–393
18. B. Möller, G. Struth: wp is wlp. Institut für Informatik, Universität Augsburg, Report 2004-14
19. G. Nelson: A generalization of Dijkstra's calculus. ACM TOPLAS 11, 517–561 (1989)
20. T.T. Nguyen: A relational model of nondeterministic programs. International J. Foundations Comp. Sci. 2, 101–131 (1991)
21. D. Parnas: A generalized control structure and its formal definition. Commun. ACM 26, 572–581 (1983)