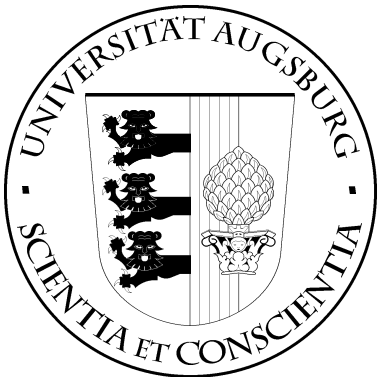
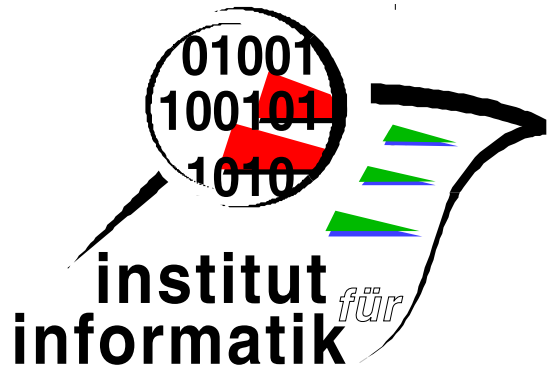
Universität Augsburg



Modal Design Algebra

Walter Guttmann **Bernhard Möller**

Report 2005-15 September 2005



Institut für Informatik
D-86135 Augsburg

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 (H3) designs based on a variant of modal semirings, hence generalising the original relational model. This makes the theory applicable to a wider class of settings, e.g., to algebras of sets of traces. Moreover, we set up the connection with the weakly and strongly demonic semantics of programs as discussed by a number of authors. This is done using commands (a, t) where a corresponds to the transition relation of a program and the condition t characterises the input states from which termination is guaranteed. The commands form not only a semiring but 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.

1 Introduction

The Unifying Theories of Programming (UTP) developed in [12] 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. Programs are identified with predicates relating the initial values v of variables with their final values v'; moreover, ok and ok' may occur freely in predicates.

However, the set of all such predicates is too general for a number of reasons not to be discussed here. Therefore, Hoare and He introduce a special class of predicates, called *designs*, of the form

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

where ok and ok' are not allowed to occur in P or Q. The informal meaning is: if the design has been started and satisfies the precondition P it will eventually terminate and satisfy the postcondition Q.

In the general case, the precondition P may 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 mention input values of variables. Originally [12] 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 aim of the present paper is twofold:

1. to present an algebraic view of normal designs in a more general class of algebras than pure relation algebra, thus making its results applicable to a broader variety of settings;
2. to set up the connection with the weakly (e.g. [2, 3, 9, 16, 18]) and strongly demonic (e.g. [1, 5, 6, 8, 17]) semantics of programs.

Essentially, we model normal designs as pairs (a, t) consisting of an element a that corresponds to the transition relation of a program and a condition t that 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 the 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 idempotent, i.e., $x + x = x$. 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. $\leq$.

In an idempotent semiring, $+$ 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 that does not change the state in any way).

An idempotent semiring is *Boolean* if it also has a greatest lower-bound or meet operation $\sqcap$, such that $+$ and $\sqcap$ distribute over each other, and an operation $\overline{\ }$ that satisfies de Morgan's laws as well as $x \sqcap \overline{x} = 0$ 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 $\sqcap$ binds tighter than $+$ but less tight than $\cdot$ does.

An important, even Boolean, semiring is $\mathrm{REL}(M)$, the algebra of binary relations under union and composition over a set M, of which the predicates of UTP form a special instance. 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. $\mathrm{TRC}(A)$ 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 but not necessarily in general semirings.

3 Modelling Conditions

Predicates or elements of REL(M) can be used to describe the input/output behaviour of programs. However, in programming logic one also needs to express assertions about the program variables or, equivalently, to characterise subsets $N \subseteq M$ of states. To keep the framework uniform one wants to encode these 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. As 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 a number of results from the latter two frameworks 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* 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 $\cdot$. In particular, $p \leq 1$ for all $p \in \mathsf{test}(S)$. But in general, $\mathsf{test}(S)$ is only a subalgebra of the subalgebra of all elements below 1 in S. We have the correspondences $\mathsf{false} \leftrightarrow 0$ and $\mathsf{true} \leftrightarrow 1$. The negation of test p, i.e., its complement relative to 1 in $\mathsf{test}(S)$, is denoted by $\neg p$. In a test semiring, the *input* and *output restrictions of $a \in S$ by $p \in \mathsf{test}(S)$* are $p \cdot a$ and $a \cdot p$, respectively.
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 $t \sqcap a$, called the *input restriction of a by t*, exists and satisfies $(t+u) \sqcap a = (t \sqcap a) + (u \sqcap a)$ as well as $t \sqcap (a+b) = t \sqcap a + t \sqcap b$. We have the correspondences $\mathsf{false} \leftrightarrow 0$ and $\mathsf{true} \leftrightarrow \top$. The negation of t, i.e., its complement relative to $\top$ in $\mathsf{cond}(S)$, is denoted by $\bar{t}$. Finally, S is called a *(right) condition semiring* if all elements of $\mathsf{cond}(S)$ are right ideals.

There is an unfortunate clash of notation between semiring theory and the theory of designs in that the algebraic representation of choice is denoted by $+$ in the first case and by $\sqcap$ in the second case (and indeed is the meet there since the converse of the natural ordering is used). Nevertheless, to keep with

the semiring tradition, we have decided to use $+$ for choice (which is the join w.r.t. $\leq$) and $\sqcap$ for the greatest lower bound w.r.t. $\leq$. To avoid confusion, one may, most of the time, simply read the $\sqcap$ symbol as restriction without thinking of its order-theoretic interpretation.

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 ideals. For 0 this follows from its left annihilation property, while for $\top$ we get, using neutrality of 1 and isotonicity,

$$\top = \top \cdot 1 \leq \top \cdot \top \leq \top \ ,$$

which, together with antisymmetry of $\leq$ shows the claim.

In a pre-condition-semiring there is no reasonable definition of output restriction of $a \in S$ by $t \in \mathsf{cond}(S)$; however, as we will see below, for condition semirings there is.

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

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

Moreover, we have the following correspondence for input restriction:

Lemma 3.1. *(See [14].) In every test semiring S with $\top$, for all $p \in \mathsf{test}(S)$ and $a \in S$ the meet $p \cdot \top \sqcap a$ exists and*

$$p \cdot a \ = \ p \cdot \top \sqcap a \ . \tag{tir}$$

And 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 $a \in S$.

From (tir) we obtain, by specialising a to 1, the representation

$$p \ = \ p \cdot \top \sqcap 1 \ . \tag{trep}$$

This entails

Lemma 3.2. *In a test semiring with $\top$,*

$$p \leq q \ \Leftrightarrow \ p \cdot \top \leq q \cdot \top \ .$$

Proof. ($\Rightarrow$) follows by neutrality of 1 and isotonicity of composition.
($\Leftarrow$) $p \underset{\text{(trep)}}{=} p \cdot \top \sqcap 1 \underset{\text{(assump., isot.)}}{\leq} q \cdot \top \sqcap 1 \underset{\text{(trep)}}{=} q.$ □

So $\mathsf{test}(S)$ and the set $\mathrm{TI}(S) \stackrel{\text{def}}{=} \{p \cdot \top : p \in \mathsf{test}(S)\}$ of *test ideals* are order-isomorphic. Hence also $\mathrm{TI}(S)$ is a Boolean algebra with

$$\begin{aligned} p \cdot \top + q \cdot \top \ &= \ (p + q) \cdot \top \ , \\ p \cdot \top \sqcap q \cdot \top \ &= \ (p \cdot q) \cdot \top \ , \\ \overline{p \cdot \top} \ &= \ \neg p \cdot \top \ , \end{aligned}$$

so that we get the

Corollary 3.3. *Every test semiring S with $\top$ can be made into a condition semiring by setting* $\mathsf{cond}(S) \stackrel{\text{def}}{=} \mathrm{TI}(S)$ *and choosing the operations as above.*

Now we look at the converse direction, going from a condition semiring to a test semiring. The analogue of (tir) is

Lemma 3.4. *For a condition t,*

$$t \sqcap a \;=\; (t \sqcap 1) \cdot a \;. \tag{cir}$$

Proof. $(\geq)$ First, $(t \sqcap 1) \cdot a \underset{\text{(isot.)}}{\leq} t \cdot a \underset{\text{(isot.)}}{\leq} t \cdot \top = t$, since t is a right ideal.
Second, $(t \sqcap 1) \cdot a \leq a$ by isotonicity, since $t \sqcap 1 \leq 1$.
$(\leq)$ $t \sqcap a \leq (t \sqcap 1) \cdot a \underset{\text{(shunting)}}{\Leftrightarrow} a \leq \overline{t} + (t \sqcap 1) \cdot a \underset{\text{(Bool. alg.)}}{\Leftrightarrow} (\overline{t} \sqcap 1) \cdot a + (t \sqcap 1) \cdot a \leq \overline{t} + (t \sqcap 1) \cdot a \underset{\text{(isot.)}}{\Leftarrow} (\overline{t} \sqcap 1) \cdot a \leq \overline{t} \underset{(\overline{t}\text{ ideal})}{\Leftrightarrow} (\overline{t} \sqcap 1) \cdot a \leq \overline{t} \cdot \top \underset{\text{(isot.)}}{\Leftrightarrow} \text{TRUE}.$ □

Corollary 3.5. $t \sqcap a \cdot b = (t \sqcap a) \cdot b$.

Proof. By (cir) twice and associativity we have

$$t \sqcap a \cdot b \;=\; (t \sqcap 1) \cdot (a \cdot b) \;=\; ((t \sqcap 1) \cdot a) \cdot b \;=\; (t \sqcap a) \cdot b \;.$$

□

Specialising a to 1 and b to $\top$ we obtain the representation

$$t \;=\; (t \sqcap 1) \cdot \top \;. \tag{crep}$$

This entails

Lemma 3.6. *In a condition semiring,*

$$t \sqcap 1 \leq u \sqcap 1 \;\Leftrightarrow\; t \leq u \;.$$

Proof. $(\Leftarrow)$ is just isotonicity of meet.
$(\Rightarrow)$ $t \underset{\text{(crep)}}{=} (t \sqcap 1) \cdot \top \underset{\text{(assump., isot.)}}{\leq} (u \sqcap 1) \cdot \top \underset{\text{(crep)}}{=} u.$ □

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

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

For the second equation we calculate

$$(t \sqcap 1) \sqcap (u \sqcap 1) \underset{\text{(Bool.alg.)}}{=} t \sqcap u \sqcap 1 \underset{\text{(cir)}}{=} (t \sqcap 1) \cdot (u \sqcap 1) \;;$$

the third one follows from the first and second. Altogether we have the

Corollary 3.7. *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 $a \cdot (t \sqcap 1)$.

4 Domain

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 will be modelled by tests and conditions, respectively.

A simple equational axiomatisation for the case of test semirings has been presented in [7] and subsequent papers. We repeat it and give a corresponding axiomatisation for the case of pre-condition-semirings in parallel.

The domain operations are

$$\ulcorner : S \to \mathsf{test}(S) \qquad \urcorner : S \to \mathsf{cond}(S)$$

with the respective axioms

$$\begin{array}{rlrl} a \leq \ulcorner a \cdot a & \text{(td1)} & a \leq \urcorner a \sqcap a & \text{(cd1)} \\ \ulcorner(p \cdot a) \leq p & \text{(td2)} & \urcorner(t \sqcap a) \leq t & \text{(cd2)} \\ \ulcorner(a \cdot \ulcorner b) \leq \ulcorner(a \cdot b) & \text{(td3)} & \urcorner(a \cdot (\urcorner b \sqcap 1)) \leq \urcorner(a \cdot b) & \text{(cd3)} \end{array}$$

According to [7] (td1) $\wedge$ (td2) is equivalent to

$$\ulcorner a \leq p \;\Leftrightarrow\; a \leq p \cdot a$$

which, in turn is equivalent to

$$\ulcorner a \leq p \;\Leftrightarrow\; \neg p \cdot a \leq 0 \;.$$

By analogous reasoning we obtain that (cd1) $\wedge$ (cd2) is equivalent to

$$\urcorner a \leq t \;\Leftrightarrow\; a \leq t \sqcap a \;\Leftrightarrow\; a \leq t \;. \qquad \text{(GCc)}$$

This property has the form of a Galois connection which corresponds to the one for the case of a test semiring with $\top$ (see again [7]):

$$\ulcorner a \leq p \;\Leftrightarrow\; a \leq p \cdot \top \;. \qquad \text{(GCt)}$$

Moreover, now by simple shunting, (cd1) $\wedge$ (cd2) is equivalent to

$$\urcorner a \leq t \;\Leftrightarrow\; \bar{t} \sqcap a \leq 0 \;.$$

By the Galois connections, the domain operations are unique if they exist. Moreover, one obtains the following consequences.

Lemma 4.1.

$$\begin{array}{rlll} 1. & \ulcorner a \leq 0 \;\Leftrightarrow\; a \leq 0 \;, & \urcorner a \leq 0 \;\Leftrightarrow\; a \leq 0 \;. \\ 2. & \ulcorner(a + b) \;=\; \ulcorner a + \ulcorner b \;, & \urcorner(a + b) \;=\; \urcorner a + \urcorner b \;. \\ 3. & a \leq b \;\Rightarrow\; \ulcorner a \leq \ulcorner b \;, & a \leq b \;\Rightarrow\; \urcorner a \leq \urcorner b \;. \\ 4. & \ulcorner p \;=\; p \;, & \urcorner t \;=\; t \;. \\ 5. & \ulcorner(\ulcorner a) \;=\; \ulcorner a \;, & \urcorner(\urcorner a) \;=\; \urcorner a \;. \\ 6. & a \;=\; \ulcorner a \cdot a \;, & a \;=\; \urcorner a \sqcap a \;. \\ 7. & \ulcorner(p \cdot a) \;=\; p \cdot \ulcorner a \;, & \urcorner(t \sqcap a) \;=\; t \sqcap \urcorner a \;. \\ 8. & \ulcorner(a \cdot b) \;\leq\; \ulcorner(a \cdot \ulcorner b) \;, & \urcorner(a \cdot b) \;\leq\; \urcorner(a \cdot \urcorner b) \;. \\ 9. & \ulcorner(a \cdot \top) \;=\; \ulcorner a \;, & \urcorner(a \cdot \top) = \urcorner a \;\Leftrightarrow\; \urcorner b = \urcorner b \cdot \top \;. \\ 10. & \ulcorner(a \cdot b) \;\leq\; \ulcorner a \;, & \urcorner(a \cdot b) \leq \urcorner a \;\Leftrightarrow\; \urcorner c = \urcorner c \cdot \top \;. \end{array}$$

Of these, properties 9. and 10. again show the special importance of using condition semirings rather than pre-condition-semirings.

Proof. We only prove the properties for $\urcorner$.

1. Immediate from (GCc).
2. By (GCc) $\urcorner$ is the lower adjoint of a Galois connection and hence preserves all existing joins.
3. Immediate from 2.
4. $t \leq \urcorner t \sqcap t \leq \urcorner t$ follows immediately from (cd1). The converse inequation follows by $\urcorner t = \urcorner(t \sqcap \top) \leq t$ immediately from (cd2).
5. Immediate from 4.
6. Immediate from the definitions.
7. By Boolean algebra and 2. we have $\urcorner a = \urcorner(t \sqcap a) + \urcorner(\bar{t} \sqcap a)$. Now

$$t \sqcap \urcorner a = (t \sqcap \urcorner(t \sqcap a)) + (t \sqcap \urcorner(\bar{t} \sqcap a)) = \urcorner(t \sqcap a),$$

   since $\urcorner(t \sqcap a) \leq t$ and $\urcorner(\bar{t} \sqcap a) \leq \bar{t}$ by (cd2).
8. Immediate from (GCc) and isotonicity.
9. ($\Rightarrow$) Specialise a to $\urcorner b$ and use the $\leq$ half of the assumption. Then

$$\urcorner(\urcorner b \cdot \top) \leq \urcorner(\urcorner b) \underset{4.}{\Leftrightarrow} \urcorner(\urcorner b \cdot \top) \leq \urcorner b \underset{\text{(GCc)}}{\Leftrightarrow} \urcorner b \cdot \top \leq \urcorner b \ .$$

   ($\Leftarrow$) Specialise b to a. Then

$$\urcorner(a \cdot \top) \leq \urcorner a \underset{\text{(GCc)}}{\Leftrightarrow} a \cdot \top \leq \urcorner a \underset{\text{(assump.)}}{\Leftarrow} a \cdot \top \leq \urcorner a \cdot \top \underset{\text{(isot.)}}{\Leftarrow} a \leq \urcorner a \underset{\text{(GCc)}}{\Leftrightarrow} \text{TRUE} \ .$$

10. ($\Rightarrow$) Specialise b to $\top$ and use 9.
    ($\Leftarrow$) The proof proceeds as for 9. with b instead of $\top$. □

By 9. and (crep), in a condition semiring the axiom (cd3) can be simplified to

$$\urcorner(a \cdot \urcorner b) \leq \urcorner(a \cdot b) \ , \qquad \text{(cd3)} \ .$$

Moreover, we have

Lemma 4.2. *In a condition semiring with domain,* $\urcorner 1 = \top$.

Proof. $\urcorner 1 \underset{\text{lhs of 9.}}{=} \urcorner(1 \cdot \top) = \urcorner\top \underset{4.}{=} \top$. □

Next we establish a connection between the two versions of the domain operation.

Lemma 4.3.

1. *Consider a test semiring S with $\top$ and test-based domain $\ulcorner$ and extend it to a condition semiring according to Corollary 3.3. Then $\urcorner a \stackrel{\text{def}}{=} \ulcorner a \cdot \top$ defines a condition-based domain operation.*

2. *Consider a condition semiring S with condition-based domain π and extend it to a test semiring according to Corollary 3.7. Then $\lceil a \stackrel{\text{def}}{=} \pi a \sqcap 1$ defines a test-based domain operation.*

Proof. We have to show that the operations satisfy the respective axioms.

1. (cd1) $\pi a \sqcap a \underset{\text{(def.)}}{=} \lceil a \cdot \top \sqcap a \underset{\text{(tir)}}{=} \lceil a \cdot a \underset{\text{(td1)}}{\geq} a$.
   (cd2) $\pi(p \cdot \top \sqcap a) \underset{\text{(tir)}}{=} \pi(p \cdot a) \underset{\text{(def.)}}{=} \lceil(p \cdot a) \cdot \top \underset{\text{(td2)}}{\leq} p \cdot \top$.
   (cd3) $\pi(a \cdot (\pi b \sqcap 1)) \underset{\text{(def.)}}{=} \lceil(a \cdot (\lceil b \cdot \top \sqcap 1)) \cdot \top \underset{\text{(tir)}}{=} \lceil(a \cdot \lceil b) \cdot \top \underset{\text{(td3)}}{\leq} \lceil(a \cdot b) \cdot \top \underset{\text{(def.)}}{=} \pi(a \cdot b)$.
2. (td1) $\lceil a \cdot a \underset{\text{(def.)}}{=} (\pi a \sqcap 1) \cdot a \underset{\text{(cir)}}{=} \pi a \sqcap a \underset{\text{(cd1)}}{\geq} a$.
   (td2) $\lceil((t \sqcap 1) \cdot a) \underset{\text{(cir)}}{=} \lceil(t \sqcap a) \underset{\text{(def.)}}{=} \pi(t \sqcap a) \sqcap 1 \underset{\text{(cd2)}}{\leq} t \sqcap 1$.
   (td3) $\lceil(a \cdot \lceil b) \underset{\text{(def.)}}{=} \pi(a \cdot (\pi b \sqcap 1)) \sqcap 1 \underset{\text{(cd3)}}{\leq} \pi(a \cdot b) \sqcap 1 \underset{\text{(def.)}}{=} \lceil(a \cdot b)$. □

Finally we make the connection with the relational case more explicit. Call a semiring S with $\top$ *full* if its set $\mathrm{RI}(S)$ of right ideals is a Boolean algebra. The relation semiring REL is full whereas the trace semiring TRC is not.

Lemma 4.4.

1. *Consider a full semiring S. Then the pair $(S, \mathrm{RI}(S))$ can uniquely be made into a domain semiring by setting $\pi a \stackrel{\text{def}}{=} a \cdot \top$.*
2. *In this case we have $\pi a \cdot \top = a \cdot \top$.*
3. *If we pass to the associated test semiring according to Lemma 4.3.2 then*

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

Proof. 1. We show that π satisfies the domain axioms.
(cd1) $\pi a \sqcap a = a$, since $a = a \cdot 1 \leq a \cdot \top$.
(cd2) $\pi(t \sqcap a) \underset{\text{(def.)}}{=} (t \sqcap a) \cdot \top \underset{\text{(Cor. 3.5)}}{=} t \sqcap a \cdot \top \leq t$.
(cd3) $\pi(a \cdot \pi b) \underset{\text{(def., assoc.)}}{=} a \cdot b \cdot \top \cdot \top = a \cdot b \cdot \top \underset{\text{(def.)}}{=} \pi(a \cdot b)$.
2. $\pi a \cdot \top = a \cdot \top \cdot \top = a \cdot \top$.
3. The first equation is immediate from $\lceil a = \pi a \sqcap 1$. This also implies

$$\lceil a \cdot \top = (\pi a \sqcap 1) \cdot \top \underset{\text{(cir)}}{=} \pi a \sqcap \top = \pi a = a \cdot \top \ .$$

□

5 Modal Operators

Based on domain we can define forward modal operators by

$$\langle a \rangle p \stackrel{\text{def}}{=} \lceil(a \cdot p) \ , \qquad \langle\!\langle a \rangle\!\rangle t \stackrel{\text{def}}{=} \pi(a \cdot t) \ ,$$
$$[a] p \stackrel{\text{def}}{=} \neg\langle a \rangle \neg p \ , \qquad [\![a]\!] t \stackrel{\text{def}}{=} \overline{\langle\!\langle a \rangle\!\rangle \overline{t}} \ .$$

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. Again, we give the special case corresponding to REL, which is immediate from Lemma 4.4:

Corollary 5.1. *Over a full semiring*

$$\langle\!\langle a \rangle\!\rangle t \;=\; a \cdot t \;, \qquad [\![a]\!]t \;=\; \overline{a \cdot \overline{t}} \;.$$

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

$$\begin{array}{cc}
\langle a\rangle 0 = 0 \;, & \langle\!\langle a \rangle\!\rangle 0 = 0 \;, \\
\langle 0\rangle p = 0 \;, & \langle\!\langle 0 \rangle\!\rangle t = 0 \;, \\
\langle a\rangle(p+q) = \langle a\rangle p + \langle a\rangle q \;, & \langle\!\langle a \rangle\!\rangle(t+u) = \langle\!\langle a \rangle\!\rangle t + \langle\!\langle a \rangle\!\rangle u \;, \\
\langle a+b\rangle p = \langle a\rangle p + \langle b\rangle p \;, & \langle\!\langle a+b \rangle\!\rangle t = \langle\!\langle a \rangle\!\rangle t + \langle\!\langle b \rangle\!\rangle t \;, \\
\langle p \cdot a\rangle q = p \cdot \langle a\rangle q \;, & \langle\!\langle t \sqcap a \rangle\!\rangle u = t \sqcap \langle\!\langle a \rangle\!\rangle u \;, \\
\langle 1\rangle p = p \;, & \langle\!\langle 1 \rangle\!\rangle t = t \;, \\
\langle a \cdot b\rangle p = \langle a\rangle\langle b\rangle p \;, & \langle\!\langle a \cdot b \rangle\!\rangle t = \langle\!\langle a \rangle\!\rangle\langle\!\langle b \rangle\!\rangle t \;.
\end{array}$$

Hence $\langle a\rangle$ and $\langle\!\langle a \rangle\!\rangle$ are isotone. Moreover, both diamonds are isotone in their first arguments.

$$\begin{array}{cc}
[a]1 = 1 \;, & [\![a]\!]\top = \top \;, \\
[0]p = 1 \;, & [\![0]\!]t = \top \;, \\
[a](p \cdot q) = [a]p \cdot [a]q \;, & [\![a]\!](t \sqcap u) = [\![a]\!]t \sqcap [\![a]\!]u \;, \\
[a+b]p = [a]p \cdot [b]p \;, & [\![a+b]\!]t = [\![a]\!]t \sqcap [\![b]\!]t \;, \\
[p \cdot a]q = \neg p + [a]q \;, & [\![t \sqcap a]\!]u = \overline{t} + [\![a]\!]u \;, \\
[1]p = p \;, & [\![1]\!]t = t \;, \\
[a \cdot b]p = [a][b]p \;, & [\![a \cdot b]\!]t = [\![a]\!][\![b]\!]t \;.
\end{array}$$

Hence $[a]$ and $[\![a]\!]$ are isotone. Moreover, both boxes are antitone in their first arguments. Finally, box allows us to transport a condition over the first factor of a composition:

Lemma 5.2. $[a]p \cdot a \cdot b \;=\; [a]p \cdot a \cdot p \cdot b \qquad [\![a]\!]t \sqcap a \cdot b \;=\; [\![a]\!]t \sqcap a \cdot (t \sqcap b).$

Proof. We only prove the case of $[\![a]\!]$. By Boolean algebra and distributivity

$$[\![a]\!]t \sqcap a \cdot b \;=\; [\![a]\!]t \sqcap a \cdot (t \sqcap b) + [\![a]\!]t \sqcap a \cdot (\overline{t} \sqcap b) \;.$$

Now,

$$[\![a]\!]t \sqcap a \cdot (\overline{t} \sqcap b) \leq [\![a]\!]t \sqcap a \cdot \overline{t} \;=\; \overline{{}^{\sqcap}(a \cdot \overline{t})} \sqcap a \cdot \overline{t} \leq 0 \;,$$

since $a \cdot \overline{t} \leq {}^{\sqcap}(a \cdot \overline{t})$. □

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

6 Designs, Commands and Correctness

To stay in line with the treatment in [12], we restrict ourselves now 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* [16, 15] 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 looping "outcome" besides any proper states that may be reached from them under a. The command (a, t) is synonymous for the normal design $t \vdash a$ as defined in [12]. The following definitions and properties are adaptations of the corresponding ones in [15].

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

$$\mathsf{wlp}.(a,t).u \stackrel{\text{def}}{=} [\![a]\!]u \;, \qquad \mathsf{wp}.(a,t).u \stackrel{\text{def}}{=} t \sqcap \mathsf{wlp}.(a,t).u \;. \tag{1}$$

Then $t = \mathsf{wp}.(a,t).\top$, so that, for command k,

$$\mathsf{wp}.k.u = \mathsf{wp}.k.\top \sqcap \mathsf{wlp}.k.u \;. \tag{2}$$

This *pairing condition* is at the centre of Nelson's approach [16].

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

$$\mathsf{grd}.(a,t) \stackrel{\text{def}}{=} \overline{\mathsf{wp}.(a,t).0} = \bar{t} + {}^{\sqcap}a \;. \tag{3}$$

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 [18] on termination constraints with totality:

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

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 of the excluded miracle $\mathsf{wp}.k.0 = 0$.

We now define the basic non-iterative commands.

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

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

We now show that the commands form a *left semiring*, i.e., satisfy all semiring laws except for the right annihilation law for the zero element fail. Note that it is essential that the underlying semiring S is a semiring and not only a left semiring.

Theorem 6.1. *The structure* $\mathrm{COM}(S) \stackrel{\text{def}}{=} (\mathrm{COM}(S), \sqcap, \mathsf{fail}, ;, \mathsf{skip})$ *is an idempotent left semiring. The associated natural order on* $\mathrm{COM}(S)$ *is*

$$(a,t) \leq (b,u) \;\Leftrightarrow\; a \leq b \wedge t \geq u \;. \tag{4}$$

Proof. Commutativity, associativity and idempotence of $\sqcap$ as well as neutrality of fail w.r.t. $\sqcap$ are immediate from the properties of the underlying test semiring.

Next we show associativity of ;.

$$\begin{array}{ll} & (a,t)\,;\,((b,u)\,;\,(c,v)) \\ = & \quad \{\![\text{ definition }]\!\} \\ & (a,t)\,;\,(b\cdot c, u \sqcap [\![b]\!]v) \\ = & \quad \{\![\text{ definition }]\!\} \\ & (a\cdot(b\cdot c), t \sqcap [\![a]\!](u \sqcap [\![b]\!]v)) \\ = & \quad \{\![\text{ associativity of } \cdot\text{, conjunctivity of } [\![a]\!] \text{ }]\!\} \\ & ((a\cdot b)\cdot c, t \sqcap [\![a]\!]u \sqcap [\![a]\!][\![b]\!]v) \\ = & \quad \{\![\text{ modal law }]\!\} \\ & ((a\cdot b)\cdot c, t \sqcap [\![a]\!]u \sqcap [\![a\cdot b]\!]v) \\ = & \quad \{\![\text{ definition }]\!\} \\ & ((a,t)\,;\,(b,u))\,;\,(c,v) \end{array}$$

Neutrality of skip is obvious. Now we show left-distributivity of ; over $\sqcap$.

$$\begin{array}{ll} & ((a,t) \sqcap (b,u))\,;\,(c,v) \\ = & \quad \{\![\text{ definition }]\!\} \\ & (a+b, t \sqcap u)\,;\,(c,v) \\ = & \quad \{\![\text{ definition }]\!\} \\ & ((a+b)\cdot c, t \sqcap u \sqcap [\![a+b]\!]v) \\ = & \quad \{\![\text{ distributivity of } \cdot\text{, antidisjunctivity of } [\![\text{-}]\!] \text{ }]\!\} \\ & (a\cdot c + b\cdot c, t \sqcap u \sqcap [\![a]\!]v \sqcap [\![b]\!]v) \\ = & \quad \{\![\text{ associativity and commutativity of } \cdot \text{ on tests, definition }]\!\} \\ & (a\cdot c, t \sqcap [\![a]\!]v) \sqcap (b\cdot c, u \sqcap [\![b]\!]v) \\ = & \quad \{\![\text{ definition }]\!\} \\ & ((a,t)\,;\,(c,v)) \sqcap ((b,u)\,;\,(c,v)) \end{array}$$

Next we show right-distributivity of ; over $\sqcap$.

$$\begin{array}{ll} & (a,t)\,;\,((b,u) \sqcap (c,v)) \\ = & \quad \{\![\text{ definition }]\!\} \\ & (a,t)\,;\,(b+c, u \sqcap v) \\ = & \quad \{\![\text{ definition }]\!\} \\ & (a\cdot(b+c), t \sqcap [\![a]\!](u \sqcap v)) \\ = & \quad \{\![\text{ distributivity of } \cdot\text{, conjunctivity of } [\![a]\!] \text{ }]\!\} \\ & (a\cdot b + a\cdot c, t \sqcap [\![a]\!]u \sqcap [\![a]\!]v) \\ = & \quad \{\![\text{ idempotence, associativity and commutativity} \end{array}$$

$$
\begin{array}{ll}
 & \quad \text{of } \cdot \text{ on tests, definition } \} \\
 & (a \cdot b, t \sqcap [\![a]\!]u) \,[]\, (a \cdot c, t \sqcap [\![a]\!]v) \\
= & \quad \{\![\text{ definition }]\!\} \\
 & ((a,t)\,;(b,u)) \,[]\, ((a,t)\,;(c,v))
\end{array}
$$

Next, we calculate the behaviour of fail and loop under $;$. First,

$$
\begin{array}{ll}
 & \mathsf{fail}\,;(a,t) \\
= & \quad \{\![\text{ definitions }]\!\} \\
 & (0 \cdot a, \top \sqcap [\![0]\!]t) \\
= & \quad \{\![\, [\![0]\!]t = \top \text{ and semiring properties }]\!\} \\
 & (0, \top) \\
= & \quad \{\![\text{ definition }]\!\} \\
 & \mathsf{fail}
\end{array}
$$

so that fail is a left zero. Second,

$$
\begin{array}{ll}
 & (a,t)\,;\mathsf{fail} \\
= & \quad \{\![\text{ definitions }]\!\} \\
 & (a \cdot 0, t \sqcap [\![a]\!]\top) \\
= & \quad \{\![\, [\![a]\!]\top = \top \text{ and semiring properties }]\!\} \\
 & (0,t)
\end{array}
$$

so that fail is not a right zero. Third,

$$
\begin{array}{ll}
 & \mathsf{loop}\,;(a,t) \\
= & \quad \{\![\text{ definitions }]\!\} \\
 & (0 \cdot a, 0 \sqcap [\![0]\!]t) \\
= & \quad \{\![\text{ semiring properties }]\!\} \\
 & (0,0) \\
= & \quad \{\![\text{ definition }]\!\} \\
 & \mathsf{loop}
\end{array}
$$

so that loop is a left zero. Fourth,

$$
\begin{array}{ll}
 & (a,t)\,;\mathsf{loop} \\
= & \quad \{\![\text{ definitions }]\!\} \\
 & (a \cdot 0, t \sqcap [\![a]\!]0) \\
= & \quad \{\![\, [\![a]\!]0 = \overline{\top a} \text{ and semiring properties }]\!\} \\
 & (0, t \sqcap \overline{\top a})
\end{array}
$$

so that loop is not a right zero.

Finally, the expression for the natural order is immediate from the definitions. □

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

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

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 [12] we say that command k is *(H4)* or *feasible* iff $k\,;\mathsf{loop} = \mathsf{loop}$. In the above proof we have shown the equation

$$(a,t)\,;\mathsf{loop} \;=\; (0, t \sqcap \overline{\Gamma a}) \;.$$

From this we immediately get, as announced above,

Corollary 6.2. *Command (a,t) is feasible iff $t \leq \Gamma a$.*

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

7 Refinement

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

$$k \leq l \;\Rightarrow\; \mathsf{wlp}.k \geq \mathsf{wlp}.l \;\wedge\; \mathsf{wp}.k \geq \mathsf{wp}.l \;, \tag{5}$$

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

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

We take this as the refinement relation between commands:

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

Due to our generalised setting we only have $k \sqsubseteq l \;\Rightarrow\; \mathsf{wp}.k \geq \mathsf{wp}.l$. But call a modal condition semiring S *extensional* if $\langle\!\langle a \rangle\!\rangle \leq \langle\!\langle b \rangle\!\rangle \;\Rightarrow\; a \leq b$ (the converse implication holds by isotonicity). For instance, REL is extensional, whereas TRC is not. The above calculation shows that over an extensional semiring we actually have $k \sqsubseteq l \;\Leftrightarrow\; \mathsf{wp}.k \leq \mathsf{wp}.l$.

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

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

We work this out componentwise:

$$\begin{array}{ll} & (a,t) \equiv (b,u) \\ \Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\ & u \leq t \wedge u \sqcap a \leq b \wedge t \leq u \wedge t \sqcap b \leq a \\ \Leftrightarrow & \quad \{\![\leq \text{ partial order }]\!\} \\ & t = u \wedge u \sqcap a \leq b \wedge t \sqcap b \leq a \\ \Leftrightarrow & \quad \{\![\text{ equality }]\!\} \\ & t = u \wedge t \sqcap a \leq b \wedge t \sqcap b \leq a \ . \end{array}$$

Now we simplify the second two conjuncts. By isotonicity and idempotence of meet,

$$t \sqcap a \leq b \wedge t \sqcap b \leq a \Rightarrow t \sqcap a \leq t \sqcap b \wedge t \sqcap b \leq t \sqcap a \Rightarrow t \sqcap a = t \sqcap b \ .$$

Conversely, by the lower bound property of $\sqcap$,

$$t \sqcap a = t \sqcap b \Rightarrow t \sqcap a \leq b \wedge t \sqcap b \leq a \ .$$

Altogether,

$$(a,t) \equiv (b,u) \Leftrightarrow t = u \wedge t \sqcap a = t \sqcap b \ . \tag{6}$$

This agrees with the behaviour of designs described in [12]. For instance,

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

Our relations between commands are put into perspective by

Lemma 7.1.

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

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

2. $(a,t) \,[\!]\, (b,u) \equiv (b,u) \Leftrightarrow (a+b, t \sqcap u) \equiv (b,u) \Leftrightarrow t \sqcap u = u \wedge u \sqcap (a+b) = u \sqcap b \Leftrightarrow u \leq t \wedge u \sqcap a + u \sqcap b = u \sqcap b \Leftrightarrow u \leq t \wedge u \sqcap a \leq u \sqcap b \Leftrightarrow u \leq t \wedge u \sqcap a \leq b \Leftrightarrow (a,t) \leq (b,u)$. □

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 7.2.

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., $u \leq t \;\wedge\; u \sqcap a \leq b$.
   For $[]$ we obtain from the definitions and the universal property of meet

   $$(a,t)\,[]\,(c,v) \sqsubseteq (b,u)\,[]\,(c,v) \;\Leftrightarrow\; u \sqcap v \leq t \sqcap v \;\wedge\; u \sqcap v \sqcap a \leq b + c \;\wedge\; u \sqcap v \sqcap c \leq b + c\;,$$

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

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

   The first conjunct is implied by the assumption $u \leq t$. The second one transforms by shunting into $[\![b]\!]v \leq \overline{u} + [\![a]\!]v = [\![u \sqcap a]\!]v$, which follows from the assumption $u \sqcap a \leq b$ and antitonicity of box. The third one transforms by Corollary 3.5 into $[\![b]\!]v \sqcap (u \sqcap a)\cdot c \leq b \cdot c$, which follows again from $u \sqcap a \leq b$ and isotonicity of composition.
   For the second argument of ; we obtain from the definitions

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

   The first conjunct is implied by the assumption $u \leq t$ and isotonicity of $[\![c]\!]$. The second one transforms by Lemma 5.2 into $v \sqcap [\![c]\!]u \sqcap c \cdot (u \sqcap a) \leq c \cdot b$, which follows from the assumption $u \sqcap a \leq b$ and isotonicity of composition.
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 7.3.

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

   $$(a,t) \sqcup (b,u) \;=\; (t \sqcap u \sqcap (a+b), t \sqcap u)\;.$$

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

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

Proof.

1. $(a,t) \sqsubseteq (c,v) \;\wedge\; (b,u) \sqsubseteq (c,v)$
$\Leftrightarrow$ {[definition]}
$v \le t \;\wedge\; v \sqcap a \le c \;\wedge\; v \le u \;\wedge\; v \sqcap b \le c$
$\Leftrightarrow$ {[lattice algebra]}
$v \le t \sqcap u \;\wedge\; v \sqcap a + v \sqcap b \le c$
$\Leftrightarrow$ {[distributivity]}
$v \le t \sqcap u \;\wedge\; v \sqcap (a+b) \le c$.

2. $(c,v) \sqsubseteq (a,t) \;\wedge\; (c,v) \sqsubseteq (b,u)$
$\Leftrightarrow$ {[definition]}
$t \le v \;\wedge\; t \sqcap c \le a \;\wedge\; u \le v \;\wedge\; u \sqcap c \le b$
$\Leftrightarrow$ {[lattice algebra, shunting]}
$t + u \le v \;\wedge\; c \le \overline{t} + a \;\wedge\; c \le \overline{u} + b$
$\Leftrightarrow$ {[lattice algebra]}
$t + u \le v \;\wedge\; c \le (\overline{t} + a) \sqcap (\overline{u} + b)$,

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

In the sequel we will be working 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).

8 Conditionals

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

$$\begin{aligned} t \rightarrow k &\stackrel{\text{def}}{=} (t \sqcap 1, \top)\,;k \;, \\ k \mathbin{[\!]\!\!\!-} l &\stackrel{\text{def}}{=} k \;[\!]\; (\overline{\mathsf{grd}.k} \rightarrow l) \;, \\ k \lhd t \rhd l &\stackrel{\text{def}}{=} (t \rightarrow k) \;[\!]\; (\overline{t} \rightarrow l) \;, \\ \mathsf{assert}\, t &\stackrel{\text{def}}{=} \mathsf{skip} \lhd t \rhd \mathsf{loop} \;, \\ \mathsf{assume}\, t &\stackrel{\text{def}}{=} \mathsf{skip} \lhd t \rhd \mathsf{chaos} \;. \end{aligned}$$

In particular, these commands are again $\sqsubseteq$-isotone so that $\equiv$ is a congruence w.r.t. them as well. The command $k \mathbin{[\!]\!\!\!-} l$ describes an asymmetric choice in which first k is tried; if k succeeds then its outcome is the overall outcome, if it fails then the overall outcome is that of l. it is useful in describing a general do od loop; for details see [16, 15].

Componentwise, the first three definitions work out to

$$\begin{aligned} t \rightarrow (b,u) &= (t \sqcap b, \overline{t} + u) \;, \\ (a,t) \mathbin{[\!]\!\!\!-} (b,u) &= (a + \overline{g} \sqcap b, t \sqcap (g + u)) \text{ where } g \stackrel{\text{def}}{=} \mathsf{grd}.(a,t) \;, \\ (b,u) \lhd t \rhd (c,v) &= (b \lhd t \rhd c, u \lhd t \rhd v) \;. \end{aligned}$$

For the latter one calculates by Boolean algebra

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

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

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

Second,

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

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 8.1. $(a,t)\,;(b,u)\lhd z\rhd(c,\top) = (z\sqcap a, t\lhd z\rhd\top)\,;(b,u) \mathbin{[\!]} (\overline{z}\sqcap c,\top)$.

Proof.
$$\begin{aligned}&((a,t)\,;(b,u))\lhd z\rhd(c,\top)\\ =\ & \quad \{\![\text{ command composition }]\!\}\\ & (a\cdot b, t\sqcap [\![a]\!]u)\lhd z\rhd(c,\top)\\ =\ & \quad \{\![\text{ command conditional }]\!\}\\ & (a\cdot b\lhd z\rhd c, t\sqcap [\![a]\!]u\lhd z\rhd\top)\\ =\ & \quad \{\![\text{ definition of conditional }]\!\}\\ & (z\sqcap(a\cdot b)+\overline{z}\sqcap c, z\sqcap t\sqcap [\![a]\!]u+\overline{z})\\ =\ & \quad \{\![\text{ Corollary 3.5 and Boolean algebra }]\!\}\\ & ((z\sqcap a)\cdot b+\overline{z}\sqcap c, (z\sqcap t+\overline{z})\sqcap([\![a]\!]u+\overline{z}))\\ =\ & \quad \{\![\text{ definition of conditional and box property }]\!\}\\ & ((z\sqcap a)\cdot b+\overline{z}\sqcap c, (t\lhd z\rhd\top)\sqcap [\![z\sqcap a]\!]u)\\ =\ & \quad \{\![\text{ command disjunction }]\!\}\\ & ((z\sqcap a)\cdot b, (t\lhd z\rhd\top)\sqcap [\![z\sqcap a]\!]u) \mathbin{[\!]} (\overline{z}\sqcap c,\top)\\ =\ & \quad \{\![\text{ command composition }]\!\}\\ & (z\sqcap a, t\lhd z\rhd\top)\,;(b,u) \mathbin{[\!]} (\overline{z}\sqcap c,\top).\end{aligned}$$

□

9 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 that will be used to define

the demonic operators on S. It is an abstract version of the mappings $\mathcal{I}_d$ and $\mathcal{H}_d$ on relations defined in [11], and given by

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

We will abbreviate $E((a,t))$ to $E(a,t)$. This function, which would even make sense 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 $\bar{t} \sqcap \ulcorner a$. For the resulting semiring element, no extra termination information is needed; this is reflected in the definition of D.

Lemma 9.1. *E and D are inverse to each other up to $\equiv$.*

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

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

By (cd1) we have $E(D(a)) = E(a, \ulcorner a) = \ulcorner a \sqcap a = a$. □

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 9.1.

The demonic refinement ordering is

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

By (6) and (cd1) $\sqsubseteq\!\!\!\!\sqsubseteq$ is antisymmetric, i.e., a partial order. Thus, by Lemma 9.1, 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

$$\begin{array}{rl} a \mathbin{▫} b & \stackrel{\mathrm{def}}{=} E(D(a) \,;\, D(b)) = E((a, \ulcorner a) \,;\, (b, \ulcorner b)) = E(a \cdot b, \ulcorner a \sqcap [\![a]\!] \ulcorner b) \\ & = \ulcorner a \sqcap [\![a]\!] \ulcorner b \sqcap a \cdot b = [\![a]\!] \ulcorner b \sqcap a \cdot b, \end{array}$$

since $a \cdot b \leq \ulcorner(a \cdot b) \leq \ulcorner a$ 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 the unit of demonic composition.

The demonic join is

$$\begin{array}{rl} a \sqcup\!\!\!\sqcup b & \stackrel{\mathrm{def}}{=} E(D(a) \mathbin{[\!]} D(b)) = E((a, \ulcorner a) \mathbin{[\!]} (b, \ulcorner b)) = E(a + b, \ulcorner a \sqcap \ulcorner b) \\ & = \ulcorner a \sqcap \ulcorner b \sqcap (a + b). \end{array}$$

The demonic meet, whenever it exists, is, by Lemma 7.3.2,

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

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

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

which is equivalent to $\ulcorner(a \sqcap b) = \ulcorner a \sqcap \ulcorner b$.

Finally, the demonic conditional is

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

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

The solutions to demonic recursions are also derived due to the order isomorphism and the following general Lemma.

Lemma 9.2. *1. Let $(A, \leq)$ 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 $f^\perp$ be the least fixed point of f, and $f^\top$ the greatest.
Then $h(f^\perp)$ 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 9.3. *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 $\nu_{\mathbb{\sqsubseteq}}(f) = E(\nu_{\sqsubseteq}(D \circ f \circ E))$.*

10 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

$$1 + a \cdot a^* \leq a^*$$
$$1 + a^* \cdot a \leq a^*$$
$$b + a \cdot c \leq c \Rightarrow a^* \cdot b \leq c$$
$$b + c \cdot a \leq c \Rightarrow b \cdot a^* \leq c$$

for $a, b, c \in K$ [13]. It follows that $a^* \cdot b$ 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 10.1. $v \sqcap (b + c \cdot a) \leq c \Rightarrow v \sqcap b \cdot a^* \leq c$.

Proof. By Boolean algebra and Corollary 3.5, $v \sqcap (b + c \cdot a) = v \sqcap b + v \sqcap (c \cdot a) = v \sqcap b + (v \sqcap c) \cdot a = v \sqcap b + (v \sqcap (c + \overline{v})) \cdot a = v \sqcap b + v \sqcap ((c + \overline{v}) \cdot a) = v \sqcap (b + (c + \overline{v}) \cdot a)$. Hence,

$$\begin{array}{ll} & v \sqcap (b + c \cdot a) \leq c \\ \Leftrightarrow & \quad \{\![\text{ above calculation }]\!\} \\ & v \sqcap (b + (c + \overline{v}) \cdot a) \leq c \\ \Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\ & b + (c + \overline{v}) \cdot a \leq c + \overline{v} \\ \Leftarrow & \quad \{\![\text{ Kleene star induction }]\!\} \\ & b \cdot a^* \leq c + \overline{v} \\ \Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\ & v \sqcap b \cdot a^* \leq c. \end{array}$$

□

Lemma 10.2. *1.* $v \leq [\![a]\!]v \Leftrightarrow a \cdot \overline{v} \leq \overline{v}$.
2. $v \leq t \sqcap [\![a]\!]v \Rightarrow v \leq [\![a^*]\!]t$.

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

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

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

□

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* [15].

Theorem 10.3. $(a,t)^* = (a^*, [\![a^*]\!] t)$.

Proof. We prove that $(a^*, [\![a^*]\!] t)$ satisfies the Kleene algebra axioms.

1. By command operations, properties of box, and the Kleene unfold axiom,
$$
\begin{aligned}
\mathsf{skip} \sqcap (a,t) \,;\, (a^*, [\![a^*]\!] t) &= (1, \top) \sqcap (a \cdot a^*, t \sqcap [\![a]\!][\![a^*]\!] t) \\
&= (1 + a \cdot a^*, [\![1]\!] t \sqcap [\![a \cdot a^*]\!] t) \\
&= (a^*, [\![1 + a \cdot a^*]\!] t) \\
&= (a^*, [\![a^*]\!] t).
\end{aligned}
$$

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

3. By command operations and ordering,
$$
\begin{aligned}
(b,u) \sqcap (a,t) \,;\, (c,v) \sqsubseteq (c,v) &\Leftrightarrow (b,u) \sqcap (a \cdot c, t \sqcap [\![a]\!] v) \sqsubseteq (c,v) \\
&\Leftrightarrow (b + a \cdot c, u \sqcap t \sqcap [\![a]\!] v) \sqsubseteq (c,v) \\
&\Leftrightarrow v \le t \sqcap u \sqcap [\![a]\!] v \wedge v \sqcap (b + a \cdot c) \le c.
\end{aligned}
$$
By Lemma 10.2.1, $a \cdot \overline{v} \le \overline{v}$, 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 $v \sqcap a^* \cdot b \le c$ by shunting. Moreover, $v \le [\![a^*]\!](t \sqcap u)$ by Lemma 10.2.2.

By command operations, properties of box, and the last two facts,

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

4. By command operations and ordering,

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

By Lemma 10.1, $v\sqcap b\cdot a^*\le c$. Moreover, $v\le [\![c]\!]t\le [\![v\sqcap b\cdot a^*]\!]t = \overline{v}+[\![b\cdot a^*]\!]t$ by box properties. By $v\le u$ and shunting, $v\le u\sqcap [\![b\cdot a^*]\!]t$.
Together, by command operations, and properties of box,

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

□

11 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

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

for $a,b,c\in K$ [14]. 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 $a^\omega\le a\cdot a^\omega$ [4]. The reverse inequality cannot be shown, however, in absence of the right annihilation law [14].

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 [15]. The convergence operation $\triangle : S\to \mathsf{cond}(S)$ satisfies the unfold and co-induction laws

$$[\![a]\!](\triangle a)\le\triangle a$$
$$t\sqcap[\![a]\!]u\le u \;\Rightarrow\; \triangle a\sqcap[\![a^*]\!]t\le u$$

The following lemma states a few properties of convergence.

Lemma 11.1. *1. $\triangle a\sqcap[\![a^*]\!]t$ is the least (pre-)fixed point of $\lambda u.t\sqcap[\![a]\!]u$. In particular, $\triangle a$ is the least (pre-)fixed point of $[\![a]\!]$.*
2. $\overline{\top a}\le\triangle a\le\overline{\top a^\omega}$ and hence $\triangle a\sqcap a^\omega = 0$.
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, $t \sqcap [\![a]\!](\triangle a \sqcap [\![a^*]\!]t) = t \sqcap [\![a]\!](\triangle a) \sqcap [\![a]\!][\![a^*]\!]t \leq \triangle a \sqcap [\![1 + a \cdot a^*]\!]t = \triangle a \sqcap [\![a^*]\!]t$. Hence, by the co-induction axiom, $\triangle a \sqcap [\![a^*]\!]t$ is the least pre-fixed point of $\lambda u.t \sqcap [\![a]\!]u$. 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,

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

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

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

Hence, $\overline{\pi a^\omega}$ is a fixed point of $[\![a]\!]$, and $\triangle a \leq \overline{\pi a^\omega}$ by 1.

3. By antitonicity 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 antitonicity of the box operator. □

In the special case of REL, $\triangle a = \overline{a^\omega}$ can be proved by Corollary 5.1.

Theorem 11.2. $(a, t)^\omega = (a^\omega, \triangle a \sqcap [\![a^*]\!]t) \equiv (0, \triangle a \sqcap [\![a^*]\!]t)$.

Proof. We prove that $(a^\omega, \triangle a \sqcap [\![a^*]\!]t)$ satisfies the weak omega axioms. The claimed equivalence then follows by Lemma 11.1.2.

1. By command operations, the fixed point property of a^ω and Lemma 11.1.1,

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

2. Assume

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

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

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

which by definitions and shunting is equivalent to $x \leq v \wedge c \leq a^\omega + a^* \cdot b + \overline{x}$, where $x \stackrel{\text{def}}{=} \triangle a \sqcap [\![a^*]\!](t \sqcap u)$.
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 $a^* \cdot \overline{w} \leq \overline{\overline{(a^* \cdot \overline{w})}} = \overline{[\![a^*]\!]w}$, so that it suffices to show $\overline{[\![a^*]\!]w} \leq \overline{x}$, equivalently $x \leq [\![a^*]\!]w$. Now, by box and star properties,

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

The first conjunct holds by definition of x. For the second one, since $x \leq v$ as shown above, it suffices by isotonicity of $[\![a^*]\!]$ to show $x \leq [\![a^*]\!]x$. Now, by disjunctivity of $[\![a^*]\!]$, Lemma 11.1.4 and star properties,

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

□

12 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 12.1.

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

Proof. We calculate the fixed points according to Corollary 9.3.

1. For the least fixed point we calculate

$$\begin{aligned} & \mu_{\sqsubseteq}(\lambda x.a \circ x \lhd t \rhd 1) \\ = & \quad \{\![\text{ Corollary 9.3 }]\!\} \\ & E(\mu_{\sqsubseteq}(\lambda(b,u).D(a \circ E(b,u) \lhd t \rhd 1))) \\ = & \quad \{\![\text{ demonic conditional: } \\ & \qquad D(a \lhd t \rhd b) = D(a) \lhd t \rhd D(b) \ ]\!\} \\ & E(\mu_{\sqsubseteq}(\lambda(b,u).D(a \circ E(b,u)) \lhd t \rhd D(1))) \\ = & \quad \{\![\text{ demonic composition: } D(a \circ b) = D(a) \,;\, D(b) \ ]\!\} \\ & E(\mu_{\sqsubseteq}(\lambda(b,u).D(a) \,;\, D(E(b,u)) \lhd t \rhd D(E(\mathsf{skip})))) \\ = & \quad \{\![\text{ Lemma 9.1 }]\!\} \\ & E(\mu_{\sqsubseteq}(\lambda(b,u).(a, \overline{\overline{a}}) \,;\, (b,u) \lhd t \rhd (1, \top))) \\ = & \quad \{\![\text{ Lemma 8.1 }]\!\} \\ & E(\mu_{\sqsubseteq}(\lambda(b,u).(t \sqcap a, \overline{\overline{a}} \lhd t \rhd \top) \,;\, (b,u) \,[\!]\, (\overline{t} \sqcap 1, \top))) \\ = & \quad \{\![\text{ definition of conditional and Boolean algebra }]\!\} \\ & E(\mu_{\sqsubseteq}(\lambda(b,u).(t \sqcap a, \overline{t} + \overline{\overline{a}}) \,;\, (b,u) \,[\!]\, (\overline{t} \sqcap 1, \top))) \\ = & \quad \{\![\ a^* \cdot b \text{ is the least fixed point of } (\lambda x.a \cdot x + b) \ ]\!\} \end{aligned}$$

$$
\begin{array}{ll}
& E((t \sqcap a, \bar{t} + \ulcorner a)^* \,;\, (\bar{t} \sqcap 1, \top)) \\
= & \quad \{\![\text{ Theorem 10.3 }]\!\} \\
& E(((t \sqcap a)^*, [\![(t \sqcap a)^*]\!](\bar{t} + \ulcorner a)) \,;\, (\bar{t} \sqcap 1, \top)) \\
= & \quad \{\![\text{ command composition }]\!\} \\
& E((t \sqcap a)^* \cdot (\bar{t} \sqcap 1), [\![(t \sqcap a)^*]\!](\bar{t} + \ulcorner a) \sqcap [\![(t \sqcap a)^*]\!]\top) \\
= & \quad \{\![\text{ box properties and definition of } E \ ]\!\} \\
& [\![(t \sqcap a)^*]\!](\bar{t} + \ulcorner a) \sqcap (t \sqcap a)^* \cdot (\bar{t} \sqcap 1).
\end{array}
$$

2. For the greatest fixed point we have

$$
\begin{array}{ll}
& \nu_{\sqsubseteq}(\lambda x.a \triangleright x \triangleleft t \triangleright 1) \\
= & \quad \{\![\text{ calculation as in 1. }]\!\} \\
& E(\nu_{\sqsubseteq}(\lambda(b,u).(t \sqcap a, \bar{t} + \ulcorner a) \,;\, (b,u) \,[]\, (\bar{t} \sqcap 1, \top))) \\
= & \quad \{\![\ a^* \cdot b + a^\omega \text{ is the greatest fixed point of } (\lambda x.a \cdot x + b) \ ]\!\} \\
& E((t \sqcap a, \bar{t} + \ulcorner a)^* \,;\, (\bar{t} \sqcap 1, \top) \,[]\, (t \sqcap a, \bar{t} + \ulcorner a)^\omega) \\
= & \quad \{\![\text{ Theorem 11.2 and calculation as in 1. }]\!\} \\
& E(((t \sqcap a)^* \cdot (\bar{t} \sqcap 1), [\![(t \sqcap a)^*]\!](\bar{t} + \ulcorner a)) \,[] \\
& \quad (0, \triangle(t \sqcap a) \sqcap [\![(t \sqcap a)^*]\!](\bar{t} + \ulcorner a))) \\
= & \quad \{\![\text{ command disjunction }]\!\} \\
& E((t \sqcap a)^* \cdot (\bar{t} \sqcap 1), \triangle(t \sqcap a) \sqcap [\![(t \sqcap a)^*]\!](\bar{t} + \ulcorner a)) \\
= & \quad \{\![\text{ 1. }]\!\} \\
& \triangle(t \sqcap a) \sqcap \mu_{\sqsubseteq}(\lambda x.a \triangleright x \triangleleft t \triangleright 1).
\end{array}
$$

□

13 Conclusion

The treatment has shown that almost all of the standard theory of normal designs can be carried over to the general case. One can even prove a generalisation of the fixed point theorem 3.1.6 of [12] 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 7 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 6.1 instead. Since the connection starting with Lemma 9.1 no longer holds, the loop semantics cannot be calculated that way.

The treatment of conditions as right ideals has been an interesting exercise but also 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 [15] for details).

It is to be hoped that the generalised results will be of use for handling trace semantics and other semantical models. The presented method could also serve as a model for the extension by parameters describing further observations as proposed by [12].

Acknowledgement: We are grateful to P. Höfner 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(4):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**. Berlin: Springer 1979, 553–592
4. Cohen, E.: Separation and reduction. In Backhouse, R., Oliveira, J., eds.: Mathematics of Program Construction. Number 1837 in Lecture Notes in Computer Science, Springer-Verlag (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 Transactions on Computational Logic (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, 2005 (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. Guttmann, W.: Non-termination in Unifying Theories of Programming. In Düntsch, I., Winter, M., eds.: 8th International Conference on Relational Methods in Computer Science (RelMiCS 8), Computer Science Department, Brock University, St. Catharines, Ontario, Canada (2005) 87–94
12. C.A.R. Hoare, J. He: Unifying theories of programming. Prentice Hall 1998
13. Kozen, D.: A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation **110** (1994) 366–390
14. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. Lecture Notes in Computer Science **3125**. Berlin: Springer 2004, 252–273
15. B. Möller, G. Struth: WP is WLP. Institut für Informatik, Universität Augsburg, Report 2004-14
16. G. Nelson: A generalization of Dijkstra's calculus. ACM Transactions on Programming Languages and Systems 11:517–561 (1989)

17. T.T. Nguyen: A relational model of nondeterministic programs. International J. Foundations Comp. Sci. 2:101–131 (1991)
18. D. Parnas: A generalized control structure and its formal definition. Commun. ACM 26:572–581 (1983)