wp is wlp

Bernhard Möller, Georg Struth

Angaben zur Veröffentlichung / Publication details:

Möller, Bernhard, and Georg Struth. 2006. "wp is wlp." *Lecture Notes in Computer Science* 3929: 200–211. https://doi.org/10.1007/11734673_16.

wp is wlp

Bernhard Möller[1] and Georg Struth[2]

[1] Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany
moeller@informatik.uni-augsburg.de
[2] Fakultät für Informatik, Universität der Bundeswehr München,
D-85577 Neubiberg, Germany
struth@informatik.unibw-muenchen.de

Abstract. Using only a simple transition relation one cannot model commands that may or may not terminate in a given state. In a more general approach commands are relations enriched with termination vectors. We reconstruct this model in modal Kleene algebra. This links the recursive definition of the do od loop with a combination of the Kleene star and a convergence operator. Moreover, the standard wp operator coincides with the wlp operator in the modal Kleene algebra of commands. Therefore our earlier general soundness and relative completeness proof for Hoare logic in modal Kleene algebra can be re-used for wp. Although the definition of the loop semantics is motivated via the standard Egli-Milner ordering, the actual construction does not depend on Egli-Milner-isotony of the constructs involved.

1 Introduction

Total correctness has been extensively studied, a.o. using relational methods. One line of research (see e.g. [3, 8, 9, 12, 24]) provides strongly demonic semantics for regular programs. There, however, one cannot model commands that may or may not terminate in a given state. A second line of research (e.g. [4, 5, 13, 23, 25]) provides a weakly demonic semantics that allows such more general termination behaviour. We reconstruct the latter approach in modal Kleene algebra. This provides a new connection between the recursive definition of the do od loop and a combination of the Kleene star with convergence algebra. Moreover, it turns out that the standard wp operator coincides with the wlp operator of a suitable modal algebra of commands. Therefore the general soundness and relative completeness proof for Hoare logic in modal Kleene algebra given in [21] can be re-used for wp (where now, of course, expressiveness has to cover termination). Although the definition of the loop semantics is motivated via the standard Egli-Milner ordering, its actual construction does not depend on Egli-Milner-isotony of the constructs involved. A number of simple proofs are omitted due to lack of space; they can be found in the technical report [22].

2 Weak and Modal Semirings

A *weak semiring* is a quintuple $(S, +, 0, \cdot, 1)$ such that $(S, +, 0)$ is a commutative monoid and $(S, \cdot, 1)$ is a monoid such that $\cdot$ distributes over $+$ and is *left-strict*, i.e., $0 \cdot a = 0$. S is *idempotent* if $+$ is. In this case the relation $a \leq b \stackrel{\text{def}}{\Leftrightarrow} a+b = b$ is an order, called the *natural order* on S, with least element 0. Moreover, $\cdot$ is isotone w.r.t. $\leq$. A *semiring* is a weak semiring where $\cdot$ is also right-strict, i.e, $a \cdot 0 = 0$.

An important idempotent semiring is REL, the algebra of binary relations under union and composition over a set. Other interesting examples of weak idempotent semirings can be found within the set of endofunctions on an upper semilattice $(L, \sqcup, \perp)$ with least element $\perp$, where addition is defined as $(f+g)(x) = f(x) \sqcup g(x)$ and multiplication by function composition. The set of disjunctive functions (satisfying $f(x \sqcup y) = f(x) \sqcup f(y)$) forms a weak idempotent semiring. The induced natural order is the pointwise order $f \leq g \Leftrightarrow \forall\, x \,.\, f(x) \leq g(x)$. The subclass of strict disjunctive functions (satisfying additionally $f(\perp) = \perp$) even forms an idempotent semiring. These types of semirings include predicate transformer algebras and are at the centre of von Wright's algebraic approach [27].

A *(weak) test semiring* is a pair $(S, \mathsf{test}(S))$, where S is a(weak) 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 definition corresponds to the one in [18]. In REL the tests are partial identity relations (also called *monotypes* or *coreflexives*), encoding sets of states. We use $a, b, \ldots$ for general semiring elements and $p, q, \ldots$ for tests. By $\neg p$ we denote the complement of p in $\mathsf{test}(S)$ and set $p \to q = \neg p + q$. Moreover, we sometimes write $p \wedge q$ for $p \cdot q$ and $p \vee q$ for $p + q$. We freely use the Boolean laws for tests. An important property is

$$p \cdot a \cdot q \leq 0 \Leftrightarrow a \cdot q \leq \neg p \cdot a \;. \tag{1}$$

For $(\Rightarrow)$ we note $a \cdot q = (p + \neg p) \cdot a \cdot q = p \cdot a \cdot q + \neg p \cdot a \cdot q = \neg p \cdot a \cdot q \leq \neg p \cdot a$ by $q \leq 1$. For $(\Leftarrow)$ we have $a \cdot q \leq \neg p \cdot a \Rightarrow p \cdot a \cdot q \leq p \cdot \neg p \cdot a = 0 \cdot a = 0$.

A *(weak) modal semiring* is a pair $(S, [\,])$, where S is a (weak) test semiring and the *box* $[\,] : S \to (\mathsf{test}(S) \to \mathsf{test}(S))$ satisfies

$$p \leq [a]q \Leftrightarrow p \cdot a \cdot \neg q \leq 0 \;, \qquad [(a \cdot b)]p = [a]([b]p) \;.$$

The diamond is the de Morgan dual of the box, i.e., $\langle a \rangle p = \neg [a] \neg p$.

The box generalises the notion of the *weakest liberal precondition* wlp to arbitrary weak modal semirings. When a models a transition relation, $[a]p$ models those states from which execution of a is impossible or guaranteed to terminate in a state in set q. In REL one has $(x,x) \in [R]q \Leftrightarrow \forall\, y : xRy \Rightarrow (y,y) \in q$. In arbitrary weak semirings the box need not exist; for more details see [10].

The box axioms are equivalent to the equational domain axioms of [10]. In fact the *domain* of element a is $\ulcorner a \stackrel{\text{def}}{=} \neg [a] 0$. Hence $\ulcorner a$ provides an abstract characterisation of the starting states of a. Conversely, $[a]q = \neg \ulcorner (a \cdot \neg q)$. Most of the consequences of the box axioms shown originally for strict modal semirings in [10] still hold for weak modal semirings (see [20]), in particular,

$$[a](p \cdot q) = [a]p \cdot [a]q \;, \qquad \langle a \rangle (p+q) = [a]p + [a]q \;, \tag{2}$$

$$[a+b]p = [a]p \cdot [b]p \;, \qquad \langle a+b \rangle p = \langle a \rangle p + \langle b \rangle p \;, \tag{3}$$

$$[p]q = p \to q \;, \qquad \langle p \rangle q = p \cdot q \;. \tag{4}$$

The latter implies $[1]q = q = \langle 1 \rangle q$ as well as $[0]p = 1$ and $\langle 0 \rangle p = 0$. By (3) $[a]$ and $\langle a \rangle$ are isotone. Moreover, by (3) box is antitone and diamond is isotone, i.e., $a \le b \Rightarrow [b] \le [a] \wedge \langle a \rangle \le \langle b \rangle$. In a semiring (i.e., assuming right-strictness of $\cdot$) we additionally get

$$[a]1 = 1 \ , \qquad \langle a \rangle 0 = 0 \ . \tag{5}$$

A (weak) modal semiring S is *extensional* if for all $a, b \in S$ we have $[a] \le [b] \Rightarrow b \ge a$. For example, REL is extensional. However, we can completely avoid extensionality, which makes our results much more widely applicable.

3 Commands and Correctness

While the previous section showed how to model the wlp-semantics of partial correctness in modal semirings, we now turn to total correctness. This requires modelling the states from which termination of a command can be guaranteed. The basic idea in [4, 5, 13, 23, 25] is to model a command as a pair (a, p) consisting of a transition a between states and a set p of states from which termination is guaranteed. Parnas [25] requires p to be contained in the domain of a. This allows distinguishing the "must-termination" given by p from the "may-termination" given by the domain and excludes "miraculous" commands that terminate without producing a result state. However, this entails that there is no neutral element w.r.t. demonic choice, since the obvious candidate fail with empty transition but full termination set does not satisfy Parnas's restriction. So there is not even an additive monoid structure. Nelson [23] dropped this restriction; we will base our treatment on his more liberal approach.

Assume now a modal semiring S (i.e., right-strictness of $\cdot$). we define the set of *commands* over S as $\mathrm{COM}(S) \stackrel{\text{def}}{=} S \times \mathsf{test}(S)$. In a command (a, p) the element $a \in S$ describes the state transition behaviour and $p \in \mathsf{test}(S)$ characterises the states with guaranteed termination; all states in $\neg p$ have the "result" of looping besides any proper states that may be reached from them under a. In this view the weakest (liberal) precondition can be defined as

$$\mathsf{wlp}.(a, p).q \stackrel{\text{def}}{=} [a]q \ , \qquad \mathsf{wp}.(a, p).q \stackrel{\text{def}}{=} p \cdot \mathsf{wlp}.(a, p).q \ .$$

Then by (5) we get $p = \mathsf{wp}.(a, p).1$, and hence, for command k, Nelson's *pairing condition* $\mathsf{wp}.k.q = \mathsf{wp}.k.1 \cdot \mathsf{wlp}.k.q$. The *guard* of a command,

$$\mathsf{grd}.(a, p) \stackrel{\text{def}}{=} \neg \mathsf{wp}.(a, p).0 = p \to \ulcorner a \ .$$

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

$$\mathsf{grd}.(a, p) = 1 \Leftrightarrow p \le \ulcorner a \ .$$

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.

$$\begin{aligned} \mathsf{fail} \stackrel{\text{def}}{=} (0,1)\ ,\quad \mathsf{skip} \stackrel{\text{def}}{=} (1,1)\ ,\quad \mathsf{loop} \stackrel{\text{def}}{=} (0,0)\ ,\\ (a,p)\,[\,]\,(b,q) \stackrel{\text{def}}{=} (a+b, p\cdot q)\ ,\\ (a,p)\,;(b,q) \stackrel{\text{def}}{=} (a\cdot b, p\cdot [a]q)\ . \end{aligned}$$

The straightforward proof of the following theorem can be found in [22].

Theorem 3.1 *The structure* $\mathrm{COM}(S) \stackrel{\text{def}}{=} (\mathrm{COM}(S), [\,], \mathsf{fail}, ;, \mathsf{skip})$ *over a semiring* S *is an idempotent weak semiring, the* command semiring *over* S*. However, it is not a semiring. The associated natural order on* $\mathrm{COM}(S)$ *is*

$$(a,p) \le (b,q) \ \Leftrightarrow\ a \le b \wedge p \ge q\ . \tag{6}$$

By antitony of box we obtain for commands k, l

$$k \le l \ \Rightarrow\ \mathsf{wlp}.k \ge \mathsf{wlp}.l \wedge \mathsf{wp}.k \ge \mathsf{wp}.l\ ,$$

where $\ge$ is the pointwise order between test transformers. The second conjunct is the converse of the usual refinement relation. If the underlying semiring is extensional then the converse implication holds as well.

By standard order theory, if S is a complete lattice then $\mathrm{COM}(S)$ is a complete lattice again with

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

Likewise, if S has a greatest element $\top$ then $\mathsf{chaos} \stackrel{\text{def}}{=} (\top,0)$ is the greatest element of $\mathrm{COM}(S)$, whereas $\mathsf{havoc} \stackrel{\text{def}}{=} (\top,1)$ represents the most nondeterministic everywhere terminating command.

4 Modalities for Commands

We now want to make $\mathrm{COM}(S)$ into a weak *modal* semiring as well. From (6) and $p \le 1$ it is immediate that $(a,p) \le \mathsf{skip} \Leftrightarrow a \le 1 \wedge p = 1$. It is easy to check that the elements of this shape are closed under ; and $[\,]$. Therefore it seems straightforward to use the *test commands* $\underline{p} \stackrel{\text{def}}{=} (p,1)$ and to choose

$$\mathsf{test}(\mathrm{COM}(S)) \stackrel{\text{def}}{=} \{\underline{p}\,|\,p\in\mathsf{test}(S)\}\ .$$

Clearly, this yields a Boolean algebra with $\neg\,\underline{p} \ =\ \underline{\neg p}$, $\underline{0} = \mathsf{fail}$ and $\underline{1} = \mathsf{skip}$.

Using this, we can also introduce a guarded statement as

$$p \longrightarrow k \ =\ \underline{p}\,;k\ . \tag{7}$$

To check the first box axiom we calculate, using the definitions and $[a]1 = 1$ (we assume a semiring, i.e., right-strictness of $\cdot$),

$$(p,1)\,;(c,r)\,;\neg(q,1) \ =\ (p\cdot c, p\to r)\,;(\neg q,1) \ =\ (p\cdot c\cdot\neg q, p\to r)\ ,$$

so that, by (6) and shunting,

$$(p,1)\,;(c,r)\,;\neg(q,1) \le (0,1) \;\Leftrightarrow\; p\cdot c\cdot\neg q \le 0 \;\wedge\; p\to r \ge 1$$
$$\Leftrightarrow\; p \le [c]q \;\wedge\; p \le r \;\Leftrightarrow\; p \le \mathsf{wp}.(c,r).q\ .$$

For the second box axiom we calculate, using the definitions, the second box axiom, conjunctivity of $[a]$ and the definitions again,

$$\mathsf{wp}.((a,p)\,;(b,q)).r \;=\; p\cdot[a]q\cdot[a\cdot b]r \;=\; p\cdot[a]q\cdot[a]([b]r)$$
$$=\; p\cdot[a](q\cdot[b]r) \;=\; \mathsf{wp}.(a,p).(\mathsf{wp}(b,q).r)\ .$$

Altogether, we have shown

Theorem 4.1 *Setting* $[k]\underline{q} \stackrel{\text{def}}{=} \underline{\mathsf{wp}.k.q}$ *makes* $\mathrm{COM}(S)$ *a weak modal semiring.*

Hence the general definitions for modal semirings tie in nicely with the wp semantics. This equation explains the title of our paper: wp is nothing but wlp in the weak modal semiring of commands.

Now the usual properties of wlp and wp come for free, since both are box operators in modal semirings:

$$\mathsf{w(l)p.fail}.r \;=\; 1\ , \qquad \mathsf{w(l)p.skip}.r \;=\; r\ ,$$
$$\mathsf{w(l)p}.(k \mathbin{[\,]} l).r \;=\; \mathsf{w(l)p}.k.r \;\wedge\; \mathsf{w(l)p}.l.r\ ,$$
$$\mathsf{w(l)p}.(p \longrightarrow l).r \;=\; p \to \mathsf{w(l)p}.l.r\ .$$

The only command that does not have an abstract counterpart in all modal semirings is loop. For it the box operators behave asymmetrically:

$$\mathsf{wlp.loop}.r \;=\; 1\ , \qquad \mathsf{wp.loop}.r \;=\; 0\ . \tag{8}$$

Theorem 4.1 implies, moreover, that for $k \in \mathrm{COM}(S)$ we have $\ulcorner k = \underline{\mathsf{grd}.k}$, another pleasing connection with the general theory of weak modal semirings. From this observation we obtain the usual guard laws for free:

$$\mathsf{grd.fail} \;=\; 0\ , \quad \mathsf{grd.skip} \;=\; 1\ , \quad \mathsf{grd}.(p \longrightarrow k) \;=\; p\cdot\mathsf{grd}.k\ ,$$
$$\mathsf{grd}.(k \mathbin{[\,]} l) \;=\; \mathsf{grd}.k + \mathsf{grd}.l\ , \quad \mathsf{grd}.(k\,;l) \;=\; \neg\mathsf{wp}.k.(\neg\mathsf{grd}.l)\ .$$

Additionally, $\mathsf{grd.loop} \;=\; 1$.

Finally, we define Nelson's biased choice operator $\boxminus$ that will be used in the definition of the if fi command in the next section:

$$k \boxminus l \stackrel{\text{def}}{=} k \mathbin{[\,]} (\neg\mathsf{grd}.k \longrightarrow l)\ .$$

Then $\boxminus$ is the *overwrite* operation in $\mathrm{COM}(S)$ that in general weak modal semirings is defined as $a|b \stackrel{\text{def}}{=} a + \neg\ulcorner a\cdot b$. A corresponding operator is used in B [1] and Z [26], but also in calculating with pointer and object structures [14, 19]. This operation satisfies a number of useful laws from which we get three properties of biased choice for free:

$$a|0 = a = 0|a\ , \qquad k \boxminus \mathsf{fail} = k = \mathsf{fail} \boxminus k\ ,$$
$$a|(b|c) = (a|b)|c\ , \qquad k \boxminus (l \boxminus m) = (k \boxminus l) \boxminus m\ ,$$
$$\ulcorner(a+b) = \ulcorner a + \ulcorner b\ , \qquad \mathsf{grd}.(k \boxminus l) = \mathsf{grd}.k + \mathsf{grd}.l\ .$$

To ease reading we will simply write p instead of $\underline{p}$ in the remainder; the context will make clear where the lifting would have to be filled in.

5 Loops, Kleene Algebra and the Egli-Milner Order

So far we have not dealt with iteration. We show now that the semantics of Dijkstra's $\mathsf{do}\,\mathsf{od}$ loop can be defined in closed terms if we assume that the underlying modal semiring S is a *convergence algebra*, that is, has additional operations * of finite iteration and $\triangle$ that yields termination information.

Let us give the necessary definitions. A *weak left Kleene algebra* is a structure $(S,^*)$ such that S is an idempotent weak semiring and the *star* * satisfies, for $a, b, c \in S$, the *left unfold* and *left induction axioms*

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

Hence $a^* \cdot b$ is the least pre-fixpoint and the least fixpoint of the function $\lambda x \,.\, a \cdot x + b$. As a consequence, star is $\leq$-isotone. Symmetrically, a *weak right Kleene algebra* $(S,^*)$ satisfies the *right unfold* and *right induction axioms*

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

A *weak left (right) modal Kleene algebra* is a weak left (right) Kleene algebra in which S is modal. Finally, a left (right) modal Kleene algebra is a weak left (right) modal Kleene algebra with a full underlying semiring. The law

$$a \cdot c \leq c \cdot b \ \Rightarrow \ a^* \cdot c \leq c \cdot b^* \tag{9}$$

holds in every left Kleene algebra: For the right-hand side it suffices by left induction to show that $c + a \cdot c \cdot b^* \leq c \cdot b^*$. But $c + a \cdot c \cdot b^* \leq c + c \cdot b \cdot b^* = c \cdot (1 + b \cdot b^*) \leq c \cdot b^*$. Even in weak left modal Kleene algebras we have $p^* = 1$ for all $p \in \mathsf{test}(S)$ and the following induction law [10].

Lemma 5.1 *In a left modal Kleene algebra,* $q \leq p \cdot [a]q \Rightarrow q \leq p \cdot [a^*]p$.

Proof. Assume $q \leq p \cdot [a]q$, i.e., $q \leq p \ \wedge \ q \leq [a]q$. The claim is equivalent to $q \leq p \ \wedge \ q \leq [a^*]q$. The first conjunct is an assuption. For the second one we calculate $q \leq [a]q \ \Leftrightarrow \ a \cdot \neg q \leq \neg q \cdot a \ \Rightarrow \ a^* \cdot \neg q \leq \neg q \cdot a^* \ \Leftrightarrow \ q \leq [a^*]q$. The first and third steps follow from (1), the second one from (9). $\square$

Now we are ready to show

Theorem 5.2 *The command semiring over a left Kleene algebra can be made into a left modal Kleene algebra by setting* $(a,p)^* \stackrel{\text{def}}{=} (a^*, [a^*]p)$.

Proof. For the left unfold axiom we calculate, using the definitions, the second box axiom, (3) and the left unfold axiom for S,

$$\begin{aligned}(1,1) \,[\!]\, (a,p) \,;\, (a^*,[a^*]p) \ &= \ (1 + a \cdot a^*, p \cdot [a]([a^*]p) \\ &= \ (1 + a \cdot a^*, [1 + a \cdot a^*]p) \ = \ (a^*, [a^*]p) \ .\end{aligned}$$

For the left induction axiom assume $(b,q) \,[\!]\, (a,p) \,;\, (c,r) \leq (c,r)$, i.e., $b + a \cdot c \leq c \ \wedge \ q \cdot p \cdot [a]r \geq r$, which by left star induction for S and Lemma 5.1 implies

$$a^* \cdot b \leq c \ \wedge \ [a^*](q \cdot p) \geq r \ . \tag{$*$}$$

Now we calculate, using the definitions, conjunctivity of $[a^*]$ and $(*)$,

$$(a^*, [a^*]p) \,;\, (b,q) \ = \ (a^* \cdot b, [a^*]p \cdot [a^*]q) \ = \ (a^* \cdot b, [a^*](p \cdot q)) \ \leq \ (c,r) \ . \qquad \square$$

Analogously one shows that under the same definition of star the command semiring over a right Kleene algebra is a right Kleene algebra again.

A *weak Kleene algebra* is a structure $(S, ^*)$ that is both a left and a right Kleene algebra over a weak semiring S; it is a *Kleene algebra* if S is a strict semiring. The notion of a *(weak) modal Kleene algebra* is defined analogously. Summarizing the above remarks we have

Theorem 5.3 *The command semiring over a (modal) Kleene algebra can again be made into a (modal) Kleene algebra by the above definition.*

Let us now look at the semantics x of the loop $\mathsf{do}\,k\,\mathsf{od}$. It is supposed to satisfy the recursion equation (cf. [23])

$$x \;=\; (k\,;x) \,[]\, \neg\mathsf{grd}.k \longrightarrow \mathsf{skip}\;. \tag{10}$$

Given the Kleene algebra structures of commands it is tempting to define the semantics of the loop $\mathsf{do}\,k\,\mathsf{od}$ as the $\leq$-least solution, viz. by the standard expression $k^*\,;\neg grd.k$. However, for $k = \mathsf{skip}$ we obtain $k^*\,;\neg grd.k \;=\; \mathsf{skip}\,;\mathsf{fail} \;=\; \mathsf{fail}$, whereas the semantics of $\mathsf{do}\,\mathsf{skip}\,\mathsf{od}$ should be loop.

So $\leq$ is not the adequate approximation order for recursions such as the one for loops; it is in a sense "too angelic". Instead, one uses the *Egli-Milner approximation relation* $\sqsubseteq$ over COM(S), given by (see [23])

$$k \sqsubseteq_{\mathrm{EM}} l \;\Leftrightarrow\; \mathsf{wp}.k \leq \mathsf{wp}.l \;\wedge\; \mathsf{wlp}.l \leq \mathsf{wlp}.k\;.$$

It is an order iff S is extensional. Equivalently, $k \sqsubseteq_{\mathrm{EM}} l \;\Leftrightarrow\; \mathsf{wp}.k.1 \leq \mathsf{wp}.l.1 \;\wedge$ $\mathsf{wp}.k \leq \mathsf{wlp}.l \;\wedge\; \mathsf{wlp}.l \leq \mathsf{wlp}.k$. Thus, to allow S to be non-extensional, we define

$$(a,p) \sqsubseteq (b,q) \;\stackrel{\mathrm{def}}{=}\; p \leq q \;\wedge\; \mathsf{wp}.(a,p) \leq \mathsf{wlp}.(b,q) \;\wedge\; a \leq b\;.$$

Lemma 5.4 *The relation* $\sqsubseteq$ *is an order with least element* loop.

Proof. Antisymmetry follows from that of $\leq$, while reflexivity is immediate from that of $\leq$ and $\mathsf{wp}.k \leq \mathsf{wlp}.k$. For transitivity, assume $(a,p) \sqsubseteq (b,q)$ and $(b,q) \sqsubseteq (c,r)$. From transitivity of $\leq$ we get $a \leq c$ and $p \leq r$. Consider now an arbitrary $s \in \mathsf{test}(S)$. First, $\mathsf{wp}.(a,p).s = p \cdot [a]s = q \cdot p \cdot [a]s = q \cdot \mathsf{wp}.(a,p).s$, since $p \leq q$. Now, $\mathsf{wp}.(a,p).s \;=\; q \cdot \mathsf{wp}.(a,p).s \;\leq\; q \cdot \mathsf{wlp}.(b,q).s \;=\; \mathsf{wp}.(b,q).s \;\leq\; \mathsf{wlp}.(c,r).s$. Finally, $\sqsubseteq$-leastness of loop follows from $\leq$-leastness of 0 and (8). □

The meaning of a recursive command then is the $\sqsubseteq$-least fixpoint of the associated function (provided it exists; $\sqsubseteq$ need not induce a cpo in general). A treatment of full recursion will be the subject of a later paper. To actually find a convenient representation of the $\sqsubseteq$-least solution of (10) we need an additional concept that captures termination information.

A *convergence algebra* [11] is a pair $(S, \triangle)$ where S is a left modal Kleene algebra and the *convergence* operation $\triangle : S \to \mathsf{test}(S)$ satisfies, for all $a \in S$ and $p, q \in \mathsf{test}(S)$, the unfold and coinduction laws

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

This axiomatises $\triangle a \cdot [a^*]q$ as the least pre-fixpoint and least fixpoint of the function $\lambda p\,.\,[a]p \cdot q$; in particular, $\triangle a$ is the least pre-fixpoint and the least fixpoint of $[a]$. For the pre-fixpoints of $[a]$ we have $[a]p \le p \Leftrightarrow \neg p \le \langle a \rangle \neg p$. Since $q \le \langle a \rangle q$ means that every state in q has a successor in q, the complements of the pre-fixpoints consist of states with the possibility of nontermination under iterated execution of a. Hence the *least* pre-fixpoint $\triangle a$ characterises the states from which a does not admit infinite transition sequences. It corresponds to the *halting predicate* of the modal μ [16]). Hence we call an element *a Noetherian* if $\triangle a = 1$. For $p \in \mathsf{test}(S)$ we have $\triangle p = \neg p$.

For our treatment of loops we now assume a convergence algebra as the underlying semiring. First we extend the convergence operation to commands and define a particular command that captures termination information by setting, for $a \in S, p \in \mathsf{test}(S)$ and $k \in \mathrm{COM}(S)$,

$$\triangle(a,p) \stackrel{\text{def}}{=} \triangle a \;, \qquad \mathsf{trm}.k \stackrel{\text{def}}{=} (0, \triangle k) \;.$$

We define command k to be *Noetherian*, in signs $\mathrm{NOE}(k)$, if $\triangle k = 1$.

Lemma 5.5 *1.* $\mathsf{trm}.(a,p)$ *is the* $\sqsubseteq$*-least solution of the equation* $x = (a,1)\,;x$.
2. $\mathsf{trm}.(a,p)$ *(like all commands of the form* $(0,q)$*) is a left zero w.r.t.* $;$ *.*

To tackle the semantics of the loop $\mathsf{do}\,k\,\mathsf{od}$, we slightly generalise and define the command $\mathsf{do}\,k\,\mathsf{exit}\,l\,\mathsf{od}$ as the $\sqsubseteq$-least solution of the recursion equation

$$x \;=\; (k\,;x) \;[\!]\; \neg\mathsf{grd}.k \longrightarrow l \;. \tag{11}$$

Let us calculate conditions for such a solution (y,t). Assume

$$(y,t) \;=\; ((a,p)\,;(y,t)) \;[\!]\; \neg g \longrightarrow (b,q)$$

where $g \stackrel{\text{def}}{=} \mathsf{grd}.(a,p)$. Plugging in the definitions, we have to satisfy

$$y \;=\; a \cdot y + \neg g \cdot b \;, \qquad t \;=\; [a]t \cdot p \cdot (\neg g \to q) \;.$$

To get a $\sqsubseteq$-least solution (y,t), we have to use the $\le$-least solutions of these equations, which by left star induction and convergence induction are

$$y \;=\; a^* \cdot \neg g \cdot b \;, \qquad t \;=\; \triangle a \cdot [a^*](p \cdot \neg g \to q) \;.$$

We show that (y,t) is indeed the $\sqsubseteq$-least solution of (11). Consider an arbitrary solution (z,u). In remains to verify that $\mathsf{wp}.(y,t) \le \mathsf{wlp}.(z,u)$. First, for arbitrary s, using the fixpoint property of (z,u), (3) and the second box axiom

$$\mathsf{wlp}.(z,u).s \;=\; [a \cdot z + \neg g \cdot b]s \;=\; [a]([z]s) \cdot [\neg g \cdot b]s \;=\; [a](\mathsf{wlp}.(z,u).s) \cdot [\neg g \cdot b]s \;.$$

Hence by the convergence induction axiom we have

$$\triangle a \cdot [a^*]([\neg g \cdot b]s) \le \mathsf{wlp}.(z,u).s \;.$$

Now, by definition and the second box axiom,

$$\begin{aligned} \mathsf{wp}.(y,t).s \;&=\; t \cdot [y]s \;=\; \triangle a \cdot [a^*](p \cdot \neg g \to q) \cdot [a^* \cdot \neg g \cdot b]s \\ &\le\; \triangle a \cdot [a^* \cdot \neg g \cdot b]s \;=\; \triangle a \cdot [a^*]([\neg g \cdot b]s) \;. \end{aligned}$$

Next, we bring our least solution (y,t) into somewhat nicer form:

$$
\begin{array}{ll}
& (a^* \cdot \neg g \cdot b, \triangle a \cdot [a^*](p \cdot \neg g \to q) \\
= & \quad \{\!|\text{ definition of } [\!]\ |\!\} \\
& (a^* \cdot \neg g \cdot b, [a^*](p \cdot \neg g \to q))\ [\!]\ (0, \triangle a) \\
= & \quad \{\!|\text{ conjunctivity of } [a^*]\ |\!\} \\
& (a^* \cdot \neg g \cdot b, [a^*]p \cdot [a^*](\neg g \to q))\ [\!]\ (0, \triangle a) \\
= & \quad \{\!|\text{ definition of } ;\ |\!\} \\
& ((a^*, [a^*]p) ; (\neg g \cdot b, \neg g \to q))\ [\!]\ (0, \triangle a) \\
= & \quad \{\!|\text{ definition of star and } \longrightarrow\ |\!\} \\
& ((a, p)^* ; (\neg g \longrightarrow (b, q))\ [\!]\ (0, \triangle a)\ .
\end{array}
$$

Altogether we have shown

Theorem 5.6 $\mathsf{do}\, k\, \mathsf{exit}\, l\, \mathsf{od} \ = \ (k^* ; \neg\mathsf{grd}.k \longrightarrow l)\ [\!]\ \mathsf{trm}.k.$

Note that this theorem does not depend on completeness of the underlying semiring nor on Egli-Milner-isotony of the command-building operations involved. Moreover, the form of the expressions in the semantics has arisen directly from the star and convergence axioms.

For $l = \mathsf{skip}$ we obtain the semantics $\mathsf{do}\, k\, \mathsf{od} \ = \ (k^* ; \neg\mathsf{grd}.k)\ [\!]\ \mathsf{trm}.k$. And now, indeed, $\mathsf{do}\, \mathsf{skip}\, \mathsf{od} \ = \ \mathsf{loop}$. We have the following connection.

Lemma 5.7 $\mathsf{do}\, k\, \mathsf{exit}\, l\, \mathsf{od} \ = \ \mathsf{do}\, k\, \mathsf{od} \,; l.$

Moreover, we obtain the semantics of the $\mathsf{if}\, \mathsf{fi}$ command which, according to [23], should be the $\sqsubseteq$-least solution of the equation $x \ = \ k \ [\!\!]\ x$. Plugging in the definition of $[\!\!]$ we can rewrite that into

$$x \ = \ (\neg\mathsf{grd}.k \,; x)\ [\!]\ \mathsf{grd}.k \longrightarrow k$$

and the above theorem and lemma yield

$$\mathsf{if}\, k\, \mathsf{fi} \ = \ \mathsf{do}\, \neg\mathsf{grd}.k\, \mathsf{exit}\, k\, \mathsf{od} \ = \ \mathsf{do}\, \neg\mathsf{grd}.k \longrightarrow \mathsf{skip}\, \mathsf{od} \,; k\ .$$

In particular, $\mathsf{if}\, \mathsf{fail}\, \mathsf{fi} \ = \ \mathsf{loop}$.

6 Hoare Calculus for WP

Since we have seen that wp is wlp in an appropriate weak modal semiring, we can use the general soundness and relative completeness proof for propositional Hoare logic from [21], since that proof nowhere uses strictness of the underlying semiring. This yields fairly quickly a sound and relatively complete proof system for wp. In an arbitrary weak modal semiring, soundness of a Hoare triple $\{p\}\ a\ \{q\}$ with tests p, q is defined as $p \leq [a]q$. The proof in [21], an abstract representation of the standard proof (see e.g. [2]) shows that relative completeness is achieved if the triple $\{[a]q\}\ a\ \{q\}$ is derivable for every command a and every test q (where one has to assume sufficient expressiveness, i.e., that the assertion logic is rich enough to express all tests $[a]q)$. For the atomic commands this yields the axioms

$$\{1\}\ \mathsf{fail}\ \{q\} \qquad \{0\}\ \mathsf{loop}\ \{q\} \qquad \{q\}\ \mathsf{skip}\ \{q\} \qquad \{\triangle k\}\ \mathsf{trm}.k\ \{q\}$$

An appropriate rule for demonic choice is

$$\frac{\{p\}\ k\ \{r\} \qquad \{q\}\ l\ \{r\}}{\{p \cdot q\}\ k \mathbin{[\!]} l\ \{r\}}$$

For the loop we observe that, except for the termination part, $\mathsf{do}\, k\, \mathsf{od}$ behaves like $\mathsf{while}\ \mathsf{grd}.k\, \mathsf{do}\, k$. For that, the usual while rule

$$\frac{\{q \wedge p\}\ k\ \{q\}}{\{q\}\ \mathsf{while}\ p\mathsf{do}\, k\ \{\neg p \wedge q\}}$$

is sound and relatively complete. Combining this with the rule for choice we obtain, after some simplification, the sound and relatively complete rule

$$\frac{\{p\}\ k\ \{p\}}{\{\triangle k \cdot p\}\ \mathsf{do}\, k\, \mathsf{od}\ \{p \cdot \neg\mathsf{grd}.k\}}$$

From that one can derive the rule

$$\frac{\{p\}\ k\ \{p\} \qquad \mathrm{NOE}(k)}{\{p\}\ \mathsf{do}\, k\, \mathsf{od}\ \{p \cdot \neg\mathsf{grd}.k\}}$$

7 Extensions: Angelic Choice and Infinite Iteration

In this section we give two extensions of the basic language of commands.

First, in $\mathrm{COM}(S)$ an angelic choice operator can be defined as

$$(a,p) \mathbin{\lfloor\!\rfloor} (b,q) \stackrel{\text{def}}{=} (a+b, p+q)\ .$$

It is clearly idempotent, associative and commutative.

Lemma 7.1 *The operators* $\lfloor\!\rfloor$ *and* $[\!]$ *distribute over each other; in particular,* $\lfloor\!\rfloor$ *is* $\leq$*-isotone. Moreover,* $k \mathbin{[\!]} l \leq k \mathbin{\lfloor\!\rfloor} l$ *with* $\mathsf{wlp}.(k \mathbin{\lfloor\!\rfloor} l) = \mathsf{wlp}.(k \mathbin{[\!]} l)$ *and*

$$\mathsf{wp}.(k \mathbin{\lfloor\!\rfloor} l).r = \mathsf{wp}.k.r \cdot \mathsf{wlp}.l.r + \mathsf{wp}.l.r \cdot \mathsf{wlp}.k.r\ .$$

The second extension concerns infinite iteration. A *weak omega algebra* [6, 20] is a structure $(S, {}^\omega)$ consisting of a left Kleene algebra S and a unary *omega* operation ${}^\omega$ that satisfies, for $a, b, c \in S$, the *unfold* and *coinduction laws*

$$a^\omega = a \cdot a^\omega\ , \tag{12}$$

$$c \leq a \cdot c + b \Rightarrow c \leq a^\omega + a^* \cdot b\ . \tag{13}$$

This axiomatises $a^\omega + a^* \cdot b$ as the greatest fixpoint of the function $\lambda x\,.\,a \cdot x + b$. In particular, a^ω is the greatest fixpoint of $\lambda x\,.\,a \cdot x$. Every weak omega algebra S has a greatest element $\top = 1^\omega$.

As in the case of Kleene algebras, we want to make the command semiring $\mathrm{COM}(S)$ over a weak omega algebra into a weak omega algebra, too. Let us find solutions to the recursion equation

$$(y,t) \;=\; ((a,p)\,;(y,t))\,[\!]\,(b,q)\ .$$

From the definitions we get the equations

$$y \;=\; a \cdot y + b\ , \qquad t \;=\; p \cdot [a]t \cdot q\ .$$

To get a $\leq$-greatest solution in $\mathrm{COM}(S)$ we have to take the $\leq$-greatest solution for y and the $\leq$-least solution for t, which are, by omega coinduction and convergence induction,

$$y \;=\; a^\omega + a^* \cdot b\ , \qquad t \;=\; \triangle a \cdot [a^*](p \cdot q)\ .$$

Setting $(b,q) \;=\; \mathsf{fail}$, we obtain

Lemma 7.2 *Over a weak omega algebra S that is also a convergence algebra, the semiring* $\mathrm{COM}(S)$ *can be made into a weak omega algebra by setting*

$$(a,p)^\omega \;\stackrel{\text{def}}{=}\; (a^\omega, \triangle a \cdot [a^*]p)\ .$$

8 Conclusion and Outlook

The modal view of the weakly demonic semantical model has led to a number of new insights. In particular, the possibility of combining the "angelic" semantics provided by the star operation with termination information through a demonic choice to get the appropriate demonic semantics seems to be novel.

The techniques of the present paper have in [15] been adapted to give an algebraic semantics for the normal designs as used in Hoare and He's Unifying Theories of Programming [17].

Future work will concern an analogous treatment of full recursion as well as applications to deriving new refinement laws.

Acknowledgements: We are grateful to J. Desharnais, W. Guttmann, P. Höfner and the anonymous referees for helpful discussions and remarks.

References

1. J.-R. Abrial: The B-Book. Cambridge University Press 1996
2. K.-R. Apt, E.-R. Olderog: Verification of Sequential and Concurrent Programs, 2nd edition. Springer 1997
3. R. C. Backhouse, J. van der Woude: Demonic operators and monotype factors. Mathematical Structures in Computer Science, 3(4):417–433 (1993)
4. R. Berghammer, H. Zierer: Relational algebraic semantics of deterministic and non-deterministic programs. Theoretical Computer Science, 43:123–147 (1986)
5. 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

6. E. Cohen: Separation and reduction. In R. Backhouse, J. N. Oliveira(eds.): Mathematics of Program Construction. Lecture Notes in Computer Science **1837**. Berlin: Springer 2000, 45–59
7. J.H. Conway: Regular algebra and finite machines. London: Chapman and Hall 1971
8. 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)
9. 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
10. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. ACM Transactions on Computational Logic (to appear)
11. J. Desharnais, B. Möller, G. Struth: Termination in modal Kleene algebra. In J.-J. Lévy, E. Mayr, and J. Mitchell, editors, Exploring new frontiers of theoretical informatics. IFIP International Federation for Information Processing Series **155**. Kluwer 2004, 653–666
12. 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)
13. 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
14. T. Ehm: The Kleene algebra of nested pointer structures: theory and applications. Universität Augsburg, PhD Thesis, Dec. 2003
15. W. Guttmann, B. Möller: Modal design algebra. In: S. Dunne (ed.): Proc. First International Symposium on Unifying Theories of Programming, Walworth Castle, 5–7 Feb. 2006. To appear in LNCS. Preliminary version: Institut für Informatik, Universität Augsburg, Report 2005-15
16. D. Harel, D. Kozen, J. Tiuryn: Dynamic Logic. MIT Press 2000
17. C.A.R. Hoare, J. He: Unifying theories of programming. Prentice Hall 1998
18. D. Kozen: Kleene algebras with tests. ACM TOPLAS 19:427–443 (1997)
19. B. Möller: Towards pointer algebra. Science of Computer Programming 21:57–90 (1993)
20. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. Lecture Notes in Computer Science **3125**. Berlin: Springer 2004, 252–273
21. B. Möller, G. Struth: Modal Kleene algebra and partial correctness. In C. Rattray, S. Maharaj, C. Shankland (eds.): Algebraic methods and software technology. Lecture Notes in Computer Science **3116**. Berlin: Springer 2004, 379–393
22. B. Möller, G. Struth: WP is WLP. Institut für Informatik, Universität Augsburg, Report 2004-14
23. G. Nelson: A generalization of Dijkstra's calculus. ACM Transactions on Programming Languages and Systems 11:517–561 (1989)
24. T.T. Nguyen: A relational model of nondeterministic programs.International J. Foundations Comp. Sci. 2:101–131 (1991)
25. D. Parnas: A generalized control structure and its formal definition. Commun. ACM 26:572–581 (1983)
26. J. M. Spivey: Understanding Z. Cambrigde University Press 1988
27. J. von Wright: Towards a refinement algebra. Science of Computer Programming 51:23–45 (2004)