

UNIVERSITÄT AUGSBURG

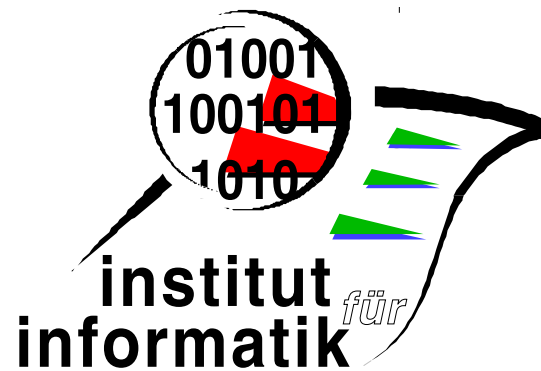


wp is wlp

Bernhard Möller Georg Struth

Report 2004-14

October 2004



INSTITUT FÜR INFORMATIK
D-86135 AUGSBURG

Copyright © Bernhard Möller Georg Struth
Institut für Informatik
Universität Augsburg
D-86135 Augsburg, Germany
<http://www.Informatik.Uni-Augsburg.DE>
— all rights reserved —

wp is wlp

Bernhard Möller¹ and Georg Struth²

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-isotonicity of the constructs involved.

1 Introduction

Total correctness has been extensively studied, a.o. using relational methods. One line of research (see e.g. [3,8,9,12,21]) 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. [4,5,13,20,22]) 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 [19] 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-isotonicity of the constructs involved.

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., $0 \cdot a = 0$. The weak semiring is *idempotent* if $+$ is idempotent. In this case the relation $a \leq b \stackrel{\text{def}}{\Leftrightarrow} a + b = b$ is an order, called the *natural order* on S . It has 0 as its least element. Moreover, \cdot is isotone w.r.t. \leq . A *semiring* is a weak semiring where \cdot is also right-strict.

An important weak semiring (and semiring) is REL, the algebra of binary relations under union and composition over a set. Other interesting examples of weak 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 semiring. The induced natural order is the pointwise ordering

$$f \leq g \Leftrightarrow \forall x \in L. f(x) \leq g(x) .$$

The subclass of strict disjunctive functions (satisfying additionally $f(\perp) = \perp$) even forms a semiring. These types of semirings include predicate transformer algebras and are at the centre of the algebraic approach of von Wright [24].

A (*weak*) *test semiring* is a pair $(S, \text{test}(S))$, where S is an idempotent (weak) semiring and $\text{test}(S) \subseteq [0, 1]$ is a Boolean subalgebra of the interval $[0, 1]$ of S such that $0, 1 \in \text{test}(S)$ and join and meet in $\text{test}(S)$ coincide with $+$ and \cdot . This definition corresponds to the one in [16]. We use a, b, \dots for general semiring elements and p, q, \dots for tests. By $\neg p$ we denote the complement of p in $\text{test}(S)$ and set $p \rightarrow q = \neg p + q$. 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.

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

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

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

The box axioms are equivalent to the equational domain axioms of [10]. In fact the *domain* of element a is $\ulcorner a \stackrel{\text{def}}{=} \neg[a]0$. Conversely, $[a]q = \neg\ulcorner(a \cdot \neg q)$. Most of the consequences of the box axioms shown originally for full modal semirings in [10] still hold for weak modal semirings (see [18]).

The box generalises the notion of the weakest liberal precondition **wlp** to arbitrary weak modal semirings. If we view a as the transition relation of a command then the test $[a]p$ characterises those states from which no transition under a is possible or the execution of a is guaranteed to end up in a final state that satisfies test p . Hence $\ulcorner a$ provides an abstract characterisation of the starting states of a .

From the definitions it is immediate that

$$[a]1 = 1 , \quad \langle a \rangle 0 = 0 , \quad (1)$$

$$[0]p = 1 , \quad \langle 0 \rangle p = 0 , \quad (2)$$

$$[a](p \cdot q) = [a]p \cdot [a]q , \quad \langle a \rangle (p + q) = [a]p + [a]q , \quad (3)$$

$$[a + b]p = [a]p \cdot [b]p , \quad \langle a + b \rangle p = \langle a \rangle p + \langle b \rangle p . \quad (4)$$

Hence $[a]$ and $\langle a \rangle$ are isotone. Moreover, box is antitone and diamond is isotone in its first argument. For a test p we get $[p]q = p \rightarrow q$ and $\langle p \rangle q = p \cdot q$. Hence, $[1] = \langle 1 \rangle$ is the identity function on tests. Moreover, $\langle 0 \rangle p = 0$ and $[0]p = 1$.

A weak modal semiring S is *extensional* if for all $a, b \in S$ we have $[a] \leq [b] \Rightarrow b \geq a$. For example, REL is extensional. However, we can completely avoid extensionality, which makes the 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 the integration of information about the states from which termination of a command can be guaranteed. The basic idea in [4,5,13,20,22] 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 [22] 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 [20] dropped this restriction; we will base our treatment on his more liberal approach.

Assume a modal semiring S . Then the set of *commands* over is $\text{COM}(S) \stackrel{\text{def}}{=} S \times \text{test}(S)$. In a command (a, p) the element $a \in S$ describes the state transition behaviour and $p \in \text{test}(S)$ characterises the states with guaranteed termination; all states in $\neg p$ have the looping “outcome” besides any proper states that may be reached from them under a . In this view the weakest (liberal) precondition can be defined as

$$\text{wlp}.(a, p).q \stackrel{\text{def}}{=} [a]q, \quad \text{wp}.(a, p).q \stackrel{\text{def}}{=} p \cdot \text{wlp}.(a, p).q. \quad (5)$$

Then $p = \text{wp}.(a, p).1$, so that, for command k ,

$$\text{wp}.k.q = \text{wp}.k.1 \cdot \text{wlp}.k.q. \quad (6)$$

This *pairing condition* is at the centre of Nelson’s approach.

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

$$\text{grd}.(a, p) \stackrel{\text{def}}{=} \neg \text{wp}.(a, p).0 = p \rightarrow \ulcorner a. \quad (7)$$

It 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:

$$\text{grd}.(a, p) = 1 \Leftrightarrow p \leq \ulcorner a.$$

Nelson remarks that totality of command k is also equivalent to Dijkstra’s law of the excluded miracle $\text{wp}.k.0 = 0$.

We now define the non-iterative commands.

$$\begin{aligned}
\text{fail} &\stackrel{\text{def}}{=} (0, 1) , \\
\text{skip} &\stackrel{\text{def}}{=} (1, 1) , \\
\text{loop} &\stackrel{\text{def}}{=} (0, 0) , \\
(a, p) \square (b, q) &\stackrel{\text{def}}{=} (a + b, p \cdot q) , \\
(a, p) ; (b, q) &\stackrel{\text{def}}{=} (a \cdot b, p \cdot [a]q) , \\
p \longrightarrow (b, q) &\stackrel{\text{def}}{=} (p \cdot b, p \rightarrow q) , \\
k \square l &\stackrel{\text{def}}{=} k \square (\neg \text{grd}.k \longrightarrow l) .
\end{aligned}$$

We now show that the commands form a weak semiring. Note that it is essential that the underlying semiring S is a full semiring.

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

$$(a, p) \leq (b, q) \Leftrightarrow a \leq b \wedge p \geq q . \quad (8)$$

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

Next we show associativity of $;$:

$$\begin{aligned}
&(a, p) ; ((b, q) ; (c, r)) \\
= &\quad \{\text{definition}\} \\
&(a, p) ; (b \cdot c, q \cdot [b]r) \\
= &\quad \{\text{definition}\} \\
&(a \cdot (b \cdot c), p \cdot [a](q \cdot [b]r)) \\
= &\quad \{\text{associativity of } \cdot, \text{ conjunctivity of } [a]\} \\
&((a \cdot b) \cdot c, p \cdot [a]q \cdot [a][b]r) \\
= &\quad \{\text{modality}\} \\
&((a \cdot b) \cdot c, p \cdot [a]q \cdot [a \cdot b]r) \\
= &\quad \{\text{definition}\} \\
&((a, p) ; (b, q)) ; (c, r)
\end{aligned}$$

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

$$\begin{aligned}
&((a, p) \square (b, q)) ; (c, r) \\
= &\quad \{\text{definition}\} \\
&(a + b, p \cdot q) ; (c, r) \\
= &\quad \{\text{definition}\}
\end{aligned}$$

$$\begin{aligned}
& ((a + b) \cdot c, p \cdot q \cdot [a + b]r) \\
= & \{ \text{distributivity of } \cdot, \text{ antisjunctionivity of } [-] \} \\
& (a \cdot c + b \cdot c, p \cdot q \cdot [a]r \cdot [b]r) \\
= & \{ \text{associativity and commutativity of } \cdot \text{ on tests, definition } \} \\
& (a \cdot c, p \cdot [a]r) \sqcap (b \cdot c, q \cdot [b]r) \\
= & \{ \text{definition } \} \\
& ((a, p) ; (c, r)) \sqcap ((b, q) ; (c, r))
\end{aligned}$$

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

$$\begin{aligned}
& (a, p) ; ((b, q) \sqcap (c, r)) \\
= & \{ \text{definition } \} \\
& (a, p) ; (b + c, q \cdot r) \\
= & \{ \text{definition } \} \\
& (a \cdot (b + c), p \cdot [a](q \cdot r)) \\
= & \{ \text{distributivity of } \cdot, \text{ conjunctivity of } [a] \} \\
& (a \cdot b + a \cdot c, p \cdot [a]q \cdot [a]r) \\
= & \{ \text{idempotence, associativity and commutativity} \\
& \quad \text{of } \cdot \text{ on tests, definition } \} \\
& (a \cdot b, p \cdot [a]q) \sqcap (a \cdot c, p \cdot [a]r) \\
= & \{ \text{definition } \} \\
& ((a, p) ; (b, q)) \sqcap ((a, p) ; (c, r))
\end{aligned}$$

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

$$\begin{aligned}
& \text{fail} ; (a, p) \\
= & \{ \text{definitions } \} \\
& (0 \cdot a, 1 \cdot [0]p) \\
= & \{ [0]p = 1 \text{ and semiring properties } \} \\
& (0, 1) \\
= & \{ \text{definition } \} \\
& \text{fail}
\end{aligned}$$

so that fail is a left zero. Second,

$$\begin{aligned}
& (a, p) ; \text{fail} \\
= & \{ \text{definitions } \}
\end{aligned}$$

$$\begin{aligned}
& (a \cdot 0, p \cdot [a]1) \\
= & \{ [a]1 = 1 \text{ and semiring properties} \} \\
& (0, p)
\end{aligned}$$

so that `fail` is not a right zero. Third,

$$\begin{aligned}
& \text{loop} ; (a, p) \\
= & \{ \text{definitions} \} \\
& (0 \cdot a, 0 \cdot [0]p) \\
= & \{ \text{semiring properties} \} \\
& (0, 0) \\
= & \{ \text{definition} \} \\
& \text{loop}
\end{aligned}$$

so that `loop` is a left zero. Fourth,

$$\begin{aligned}
& (a, p) ; \text{loop} \\
= & \{ \text{definitions} \} \\
& (a \cdot 0, p \cdot [a]0) \\
= & \{ [a]0 = \neg a \text{ and semiring properties} \} \\
& (0, p \cdot \neg a)
\end{aligned}$$

so that `loop` is not a right zero. □

By antitonicity of `box` we obtain for commands k, l

$$k \leq l \Rightarrow \text{wlp}.k \geq \text{wlp}.l \wedge \text{wp}.k \geq \text{wp}.l, \quad (9)$$

where \geq 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 $\text{COM}(S)$ is a complete lattice again with

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

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

4 Modalities for Commands

We now want to make $\text{COM}(S)$ into a weak *modal* semiring as well. From (8) and $p \leq 1$ it is immediate that $(a, p) \leq \text{skip} \Leftrightarrow a \leq 1 \wedge p = 1$. It is easy to check that the elements of this shape are closed under $;$ and \square . Therefore it seems straightforward to use the *test commands* $\underline{p} \stackrel{\text{def}}{=} (p, 1)$ and to choose

$$\text{test}(\text{COM}(S)) \stackrel{\text{def}}{=} \{\underline{p} \mid p \in \text{test}(S)\} .$$

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

Using this, we can also express guarded statements as

$$p \rightarrow k = \underline{p}; k , \quad (10)$$

as is shown by the calculation

$$(p, 1); (b, q) = (p \cdot b, 1 \cdot [p]q) = (p \cdot b, p \rightarrow q) = p \rightarrow (b, q) .$$

Let us now check the first axiom for the box. We calculate, using the definitions and $[a]1 = 1$,

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

so that, by (8) and shunting,

$$\begin{aligned} (p, 1); (c, r); \neg(q, 1) \leq (0, 1) &\Leftrightarrow p \cdot c \cdot \neg q \leq 0 \wedge p \rightarrow r \geq 1 \\ &\Leftrightarrow p \leq [c]q \wedge p \leq r \Leftrightarrow p \leq \text{wp} \cdot (c, r) \cdot q . \end{aligned}$$

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

$$\begin{aligned} \text{wp} \cdot ((a, p); (b, q)) \cdot r &= p \cdot [a]q \cdot [a \cdot b]r = p \cdot [a]q \cdot [a]([b]r) \\ &= p \cdot [a](q \cdot [b]r) = \text{wp} \cdot (a, p) \cdot (\text{wp}(b, q) \cdot r) . \end{aligned}$$

Altogether, we have shown

Theorem 4.1 $\text{COM}(S)$ becomes a weak modal semiring by setting $[k]q = \text{wp} \cdot k \cdot q$.

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 wlp come for free, since both are box operators in right-distributive modal semirings:

$$\begin{aligned} \text{w}(l)\text{p} \cdot \text{fail} \cdot r &= 1 , \\ \text{w}(l)\text{p} \cdot \text{skip} \cdot r &= r , \\ \text{w}(l)\text{p} \cdot (k \square l) \cdot r &= \text{w}(l)\text{p} \cdot k \cdot r \wedge \text{w}(l)\text{p} \cdot l \cdot r , \\ \text{w}(l)\text{p} \cdot (p \rightarrow l) \cdot r &= p \rightarrow \text{w}(l)\text{p} \cdot l \cdot r , \\ \text{w}(l)\text{p} \cdot (p \boxplus l) \cdot r &= \text{w}(l)\text{p} \cdot k \cdot r \wedge \neg \text{grd} \cdot k \rightarrow \text{w}(l)\text{p} \cdot l \cdot r . \end{aligned}$$

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

$$\text{wlp.loop}.r = 1 , \quad \text{wp.loop}.r = 0 . \quad (11)$$

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

$$\begin{aligned} \text{grd.fail} &= 0 , \\ \text{grd.skip} &= 1 , \\ \text{grd.}(k \boxplus l) &= \text{grd}.k + \text{grd}.l , \\ \text{grd.}(k ; l) &= \neg \text{wp}.k . \neg \text{grd}.l , \\ \text{grd.}(p \rightarrow k) &= p \cdot \text{grd}.k . \end{aligned}$$

Additionally,

$$\text{grd.loop} = 1 .$$

Finally, \boxplus is the *overwrite* operation in $\text{COM}(S)$; in weak modal semirings it is defined as

$$a \boxplus b \stackrel{\text{def}}{=} a + \neg \ulcorner a \cdot b .$$

A corresponding operator is used in B [1] and Z [23], but also in calculating with pointer and object structures [14,17]. This operation satisfies a number of useful laws. From these we get the following properties for free:

$$\begin{aligned} k \boxplus \text{fail} &= k = \text{fail} \boxplus k , \\ k \boxplus (l \boxplus m) &= (k \boxplus l) \boxplus m , \\ \text{grd.}(k \boxplus l) &= \text{grd}.s + \text{grd}.l . \end{aligned}$$

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

5 The Egli-Milner Order and Loops

So far we have not dealt with repetition. We show now that the semantics of Dijkstra's `do 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 Δ that yields termination information.

Let us give the necessary definitions. A *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*

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

Therefore, $a^* \cdot b$ 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. A *left modal Kleene algebra* is a left Kleene algebra in which the underlying weak semiring is modal. For all $p \in \text{test}(S)$ we have $p^* = 1$. Moreover, as in [10] one can prove the induction law

$$q \leq p \cdot [a]q \Rightarrow q \leq [a^*]p . \quad (12)$$

Lemma 5.1 *The command semiring $\text{COM}(S)$ over a left Kleene algebra S can be made into a left 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, (4) and the left unfold axiom for S ,

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

For the left induction axiom assume $(b, q) \square (a, p) ; (c, r) \leq (c, r)$, 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 (12) implies

$$a^* \cdot b \leq c \wedge [a^*](q \cdot p) \geq r . \quad (13)$$

Now we calculate, using the definitions, conjunctivity of $[a^*]$ and (13),

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

Symmetrically, one can define a right Kleene algebra over a weak semiring by requiring the *right unfold* and *right induction axioms*

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

Analogously to above 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 that is both a left and a right Kleene algebra over a weak semiring S ; it is a *Kleene algebra* if S is actually a full semiring. The notion of a *(weak) modal Kleene algebra* is defined analogously. Summarizing the above remarks we have

Lemma 5.2 *The command semiring over a (weak)(modal) Kleene algebra can again be made into a (weak)(modal) Kleene algebra by the above definition.*

Let us now look at the semantics x of the loop `do k od`. It is supposed to satisfy the recursion equation (cf. [20])

$$x = (k ; x) \square \neg\text{grd}.k \rightarrow \text{skip} . \quad (14)$$

Given the Kleene algebra structures of commands it is tempting to define the semantics of the loop `do k od` as the \leq -least solution, viz. by the standard expression $k^* ; \neg\text{grd}.k$. However, for $k = \text{skip}$ we obtain $k^* ; \neg\text{grd}.k = \text{skip} ; \text{fail} = \text{fail}$, whereas the semantics of `do skip 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 $\text{COM}(S)$, given by (see [20])

$$k \sqsubseteq l \Leftrightarrow \text{wp}.k \leq \text{wp}.l \wedge \text{wlp}.l \leq \text{wlp}.k .$$

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

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

Lemma 5.3 *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 $\text{wp}.k \leq \text{wlp}.k$.

For transitivity, assume $(a, p) \sqsubseteq (b, q)$ and $(b, q) \sqsubseteq (c, r)$. From transitivity of \leq we get $a \leq c$ and $p \leq r$. Moreover, for all s ,

$$\begin{aligned}
& \text{wp}.(a, p).s \\
= & \quad \{\{ \text{definitions} \}\} \\
& p \cdot [a]s \\
= & \quad \{\{ p \leq q \text{ by } (a, p) \sqsubseteq (b, q) \}\} \\
& p \cdot q \cdot [a]s \\
\leq & \quad \{\{ \text{isotonicity of } \cdot \text{ and } p \cdot [a]s \leq [b]s \text{ by } (a, p) \sqsubseteq (b, q) \}\} \\
& q \cdot [b]s \\
\leq & \quad \{\{ q \cdot [b]s \leq [c]s \text{ by } (b, q) \sqsubseteq (c, r) \}\} \\
& [c]s \\
= & \quad \{\{ \text{definitions} \}\} \\
& \text{wlp}.(c, r).s .
\end{aligned}$$

Finally, \sqsubseteq -leastness of `loop` follows from \leq -leastness of 0 and (11). □

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 (14) we need an additional concept that captures termination information.

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

$$[a](\Delta a) \leq \Delta a, \quad [a]p \cdot q \leq p \Rightarrow \Delta a \cdot [a^*]q \leq p . \quad (15)$$

This axiomatises $\Delta a \cdot [a^*]q$ as the least pre-fixpoint and least fixpoint of the function $\lambda p. [a]p \cdot q$; in particular, Δa least pre-fixpoint and the least fixpoint of $[a]$. Hence, if $\text{test}(S)$ is complete then Δ is guaranteed to exist.

For the pre-fixpoints of $[a]$ we have

$$[a]p \leq p \Leftrightarrow \neg p \leq \langle a \rangle \neg p .$$

Since $q \leq \langle a \rangle q$ 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 Δa characterises the states from which a cannot diverge. It corresponds to the *halting predicate* of the modal

μ -calculus [15]). Hence we call an element a *Noetherian* if $\Delta a = 1$. For $p \in \text{test}(S)$ we have $\Delta p = \neg p$.

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 $a \in S, p \in \text{test}(S)$ and $k \in \text{COM}(S)$,

$$\Delta(a.p) \stackrel{\text{def}}{=} \Delta a, \quad \text{trm}.k \stackrel{\text{def}}{=} (0, \Delta k).$$

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

Lemma 5.4 1. $\text{trm}.(a, p)$ is the \sqsubseteq -least solution of the equation $x = (a, 1); x$.
 2. $\text{trm}.(a, p)$ is a left zero w.r.t. composition (as are all commands of the form $(0, q)$).

Proof. First, $\text{trm}.(a, p)$ is a solution, since by the semiring and convergence axioms

$$(a, 1); (0, \Delta a) = (a \cdot 0, [a](\Delta a)) = (0, \Delta a).$$

Assume now that (b, q) is another solution, i.e., $b = a \cdot b$ and $[a]q = q$. Then by the convergence axioms $\Delta a \leq q$. Since $0 \leq b$ is trivial, it remains to show $\text{wp}.(0, \Delta a) \leq \text{wp}.(b, q)$. Now, by the definitions, for all s ,

$$\text{wp}.(0, \Delta a).s = \Delta a \cdot [0]s = \Delta a$$

by (2). On the other hand, for all s , by the assumption and the second box axiom,

$$\text{wp}.(b, q).s = [b]s = [a \cdot b]s = [a]([b]s),$$

so that $[b]s$ is a fixpoint of $[a]$. but then $\Delta a \leq [b]s$, which shows the claim.

Finally,

$$(0, q); (c, r) = (0 \cdot c, q \cdot [0]r) = (0, q)$$

by the semiring axioms and (2). □

Now we can tackle the semantics of the loop `do k od`. We investigate a slight generalisation and define the command `do k exit l od` as the \sqsubseteq -least solution of the recursion equation

$$x = (k; x) \sqcap \neg \text{grd}.k \rightarrow l. \tag{16}$$

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

$$(y, t) = ((a, p); (y, t)) \sqcap \neg g \rightarrow (b, q)$$

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

$$y = a \cdot y + \neg g \cdot b, \quad t = [a]t \cdot p \cdot (\neg g \rightarrow q).$$

Since we are looking for an \sqsubseteq -least solution (y, t) , we have to use the \leq -least solutions of these equations. By the left star induction axiom and the convergence induction axiom these are

$$y = a^* \cdot \neg g \cdot b, \quad t = \Delta a \cdot [a^*](p \cdot \neg g \rightarrow q).$$

We show that (y, t) is indeed the \sqsubseteq -least solution of (16). Consider an arbitrary solution (z, u) . It remains to verify that $\text{wp}.(y, t) \leq \text{wlp}.(z, u)$. First we observe, for arbitrary s , using the fixpoint property of (z, u) , (4) and the second box axiom

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

Hence by the convergence induction axiom we have

$$\Delta a \cdot [a^*](\neg g \cdot b]s) \leq \text{wlp}.(z, u).s.$$

On the other hand, by definition and the second box axiom,

$$\begin{aligned} \text{wp}.(y, t).s &= t \cdot [y]s = \Delta a \cdot [a^*](p \cdot \neg g \rightarrow q) \cdot [a^* \cdot \neg g \cdot b]s \\ &\leq \Delta a \cdot [a^* \cdot \neg g \cdot b]s = \Delta a \cdot [a^*](\neg g \cdot b]s), \end{aligned}$$

and we are done.

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

$$\begin{aligned} &(a^* \cdot \neg g \cdot b, \Delta a \cdot [a^*](p \cdot \neg g \rightarrow q)) \\ &= \{ \text{definition of } \sqsubseteq \} \\ &(a^* \cdot \neg g \cdot b, [a^*](p \cdot \neg g \rightarrow q)) \sqsubseteq (0, \Delta a) \\ &= \{ \text{conjunctivity of } [a^*] \} \\ &(a^* \cdot \neg g \cdot b, [a^*]p \cdot [a^*](\neg g \rightarrow q)) \sqsubseteq (0, \Delta a) \\ &= \{ \text{definition of } ; \} \\ &((a^*, [a^*]p) ; (\neg g \cdot b, \neg g \rightarrow q)) \sqsubseteq (0, \Delta a) \\ &= \{ \text{definition of star and } \rightarrow \} \\ &((a, p)^* ; (\neg g \rightarrow (b, q))) \sqsubseteq (0, \Delta a). \end{aligned}$$

Altogether we have shown

Theorem 5.5 $\text{do } k \text{ exit } l \text{ od} = (k^* ; \neg \text{grd}.k \rightarrow l) \sqsubseteq \text{trm}.k$.

Note that this theorem does not depend on completeness of the underlying semiring nor on Egli-Milner-isotonicity 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 $l = \text{skip}$ we obtain the semantics

$$\text{do } k \text{ od} = (k^* ; \neg \text{grd}.k) \sqsubseteq \text{trm}.k. \quad (17)$$

And now, indeed, $\text{do skip od} = \text{loop}$. We have the following connection.

Lemma 5.6 $\text{do } k \text{ exit } l \text{ od} = \text{do } k \text{ od} ; l$.

Proof. $\text{do } k \text{ od} ; l$

$$\begin{aligned}
&= \{ \text{by (17)} \} \\
&\quad ((k^* ; \neg \text{grd}.k) \sqcap \text{trm}.k) ; l \\
&= \{ \text{left distributivity} \} \\
&\quad (k^* ; \neg \text{grd}.k ; l) \sqcap (\text{trm}.k ; l) \\
&= \{ \text{by Lemma 5.4.2} \} \\
&\quad (k^* ; \neg \text{grd}.k ; l) \sqcap \text{trm}.k \\
&= \{ \text{by (10)} \} \\
&\quad (k^* ; (\neg \text{grd}.k \rightarrow l)) \sqcap \text{trm}.k .
\end{aligned}$$

□

Moreover, we obtain the semantics of the if fi command which, according to [20], should be the \sqsubseteq -least solution of the equation $x = k \sqcap x$. Plugging in the definition of \sqcap we can rewrite that into

$$x = (\neg \text{grd}.k ; x) \sqcap \text{grd}.k \rightarrow k$$

and the above theorem and lemma yield

$$\text{if } k \text{ fi} = \text{do } \neg \text{grd}.k \text{ exit } k \text{ od} = \text{do } \neg \text{grd}.k \rightarrow \text{skip od} ; k .$$

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

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 [19]. 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 [19], 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

$$\{1\} \text{fail} \{q\} \quad \{0\} \text{loop} \{q\} \quad \{q\} \text{skip} \{q\} \quad \{\Delta k\} \text{trm}.k \{q\}$$

An appropriate rule for demonic choice is

$$\frac{\{p\} k \{r\} \quad \{q\} l \{r\}}{\{p \cdot q\} k \sqcap l \{r\}}$$

For the loop we observe that, except for the termination part, `do k od` behaves like `while grd.k do k` (which also coincides with the exhaustive iteration `exh k = k*`; `¬grd.k` in [11]). For that, the usual while rule

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

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

$$\frac{\{p\} k \{p\}}{\{\Delta k \cdot p\} \text{ do } k \text{ od } \{p \cdot \neg \text{grd}.k\}}$$

From that one can derive the rule

$$\frac{\{p\} k \{p\} \quad \text{NOE}(k)}{\{p\} \text{ do } k \text{ od } \{p \cdot \neg \text{grd}.k\}}$$

7 Extensions: Angelic Choice and Infinite Iteration

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

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

$$(a, p) \parallel (b, q) \stackrel{\text{def}}{=} (a + b, p + q) .$$

It is clearly idempotent, associative and commutative.

Lemma 7.1 *The operators \parallel and \sqcap distribute over each other; in particular, \parallel is \leq -isotone. Moreover, $k \sqcap l \leq k \parallel l$ with $\text{wlp}.(k \sqcap l) = \text{wlp}.(k \parallel l)$ and*

$$\text{wp}.(k \sqcap l).r = \text{wp}.k.r \cdot \text{wlp}.l.r + \text{wp}.l.r \cdot \text{wlp}.k.r .$$

Proof. For distributivity of \sqcap over \parallel we calculate, using the definitions and semiring properties,

$$\begin{aligned} ((a, p) \parallel (b, q)) \sqcap (c, r) &= (a + b + c, (p + q) \cdot r) \\ &= (a + c + b + c, p \cdot r + q \cdot r) \\ &= ((a, p) \sqcap (c, r)) \parallel ((b, q) \sqcap (c, r)) . \end{aligned}$$

For distributivity of \parallel over \sqcap we calculate, using the definitions and semiring properties,

$$\begin{aligned} ((a, p) \sqcap (b, q)) \parallel (c, r) &= (a + b + c, p \cdot q + r) \\ &= (a + c + b + c, (p + r) \cdot (q + r)) \\ &= ((a, p) \parallel (c, r)) \sqcap ((b, q) \parallel (c, r)) . \end{aligned}$$

Next we have, by distributivity and idempotence,

$$(k \sqcap l) \sqcap (k \parallel l) = (k \sqcap l \sqcap k) \parallel (k \sqcap l \parallel l) = (k \sqcap l) \parallel (k \sqcap l) = (k \parallel l) ,$$

which shows $k \sqcap l \leq k \sqcap l$.

The statement about wlp is immediate from the definition. For wp we calculate

$$\begin{aligned}
& \text{wp}.\left((a, p) \sqcap (b, q)\right).r \\
= & \quad \{\{\text{definitions}\}\} \\
& (p + q) \cdot [a + b]r \\
= & \quad \{\{\text{distributivity and conjunctivity of } [a]\}\} \\
& p \cdot [a]r \cdot [b]r + q \cdot [a]r \cdot [b]r \\
= & \quad \{\{\text{definitions}\}\} \\
& \text{wp}.(a, b).r \cdot \text{wlp}.(b, q).r + \text{wp}.(b, q).r \cdot \text{wlp}.(a, b).r .
\end{aligned}$$

□

The second extension concerns infinite iteration. A *weak omega algebra* [6,18] is a structure (S, ω) consisting of a left Kleene algebra S and a unary *omega* operation ω that satisfies, for $a, b, c \in S$, the *unfold* and *coinduction laws*

$$a^\omega = a \cdot a^\omega , \quad (18)$$

$$c \leq a \cdot c + b \Rightarrow c \leq a^\omega + a^* \cdot b . \quad (19)$$

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 $\top = 1^\omega$. If S is also a weak test semiring then $p^\omega = p \cdot \top$ for all $p \in \text{test}(S)$.

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

$$(y, t) = ((a, p) ; (y, t)) \sqcap (b, q) .$$

From the definitions we get the equations

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

To get a \leq -greatest solution in $\text{COM}(S)$ 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,

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

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

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

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

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.

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 and P. Höfner 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. Belkhit, 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. D. Harel, D. Kozen, J. Tiuryn: *Dynamic Logic*. MIT Press 2000

16. D. Kozen: Kleene algebras with tests. *ACM TOPLAS* 19:427–443 (1997)
17. B. Möller: Towards pointer algebra. *Science of Computer Programming* 21:57–90 (1993)
18. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): *Mathematics of Program Construction*. Lecture Notes in Computer Science **3125**. Berlin: Springer 2004, 252–273
19. 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
20. G. Nelson: A generalization of Dijkstra’s calculus. *ACM Transactions on Programming Languages and Systems* 11:517–561 (1989)
21. T.T. Nguyen: A relational model of nondeterministic programs. *International J. Foundations Comp. Sci.* 2:101–131 (1991)
22. D. Parnas: A generalized control structure and its formal definition. *Commun. ACM* 26:572–581 (1983)
23. J. M. Spivey: *Understanding Z*. Cambridge University Press 1988
24. J. von Wright: Towards a refinement algebra. *Science of Computer Programming* 51:23–45 (2004)