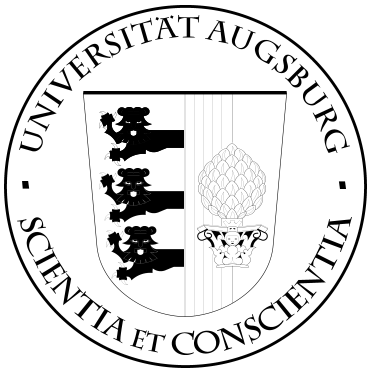
Omega algebra, demonic refinement algebra and commands

Peter Höfner, Kim Solin, Bernhard Möller

Angaben zur Veröffentlichung / Publication details:

Höfner, Peter, Kim Solin, and Bernhard Möller. 2006. “Omega algebra, demonic refinement algebra and commands.” Augsburg: Institut für Informatik, Universität Augsburg.

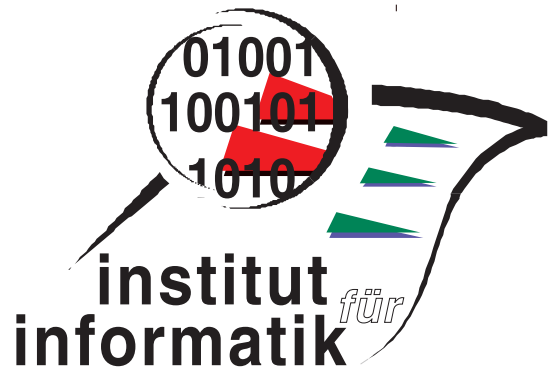
Universität Augsburg



Omega Algebra, Demonic Refinement Algebra and Commands

Peter Höfner **Kim Solin** **Bernhard Möller**

Report 2006-11 June 2006



Institut für Informatik
D-86135 Augsburg

Omega Algebra, Demonic Refinement Algebra and Commands

Peter Höfner[1⋆], Bernhard Möller[1], and Kim Solin[1,2]

[1] Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany
{hoefner,moeller}@informatik.uni-augsburg.de
[2] Turku Centre for Computer Science
Lemminkäinengatan 14 A, FIN-20520 Åbo, Finland
kim.solin@utu.fi

Abstract. Weak omega algebra and demonic refinement algebra are two ways of describing systems with finite and infinite iteration. We show that these independently introduced kinds of algebras can actually be defined in terms of each other. By defining modal operators on the underlying weak semiring, that result directly gives a demonic refinement algebra of commands. This yields models in which extensionality does not hold. Since in predicate-transformer models extensionality always holds, this means that the axioms of demonic refinement algebra do not characterise predicate-transformer models uniquely. The omega and the demonic refinement algebra of commands both utilise the convergence operator that is analogous to the halting predicate of modal μ-calculus. We show that the convergence operator can be defined explicitly in terms of infinite iteration and domain if and only if domain coinduction for infinite iteration holds.

1 Introduction

An omega algebra [2] is an extension of Kleene algebra [10] adding an infinite iteration operator to the signature. Demonic refinement algebra is an extension of a relaxed version of Kleene algebra (right-strictness, $a \cdot 0 = 0$, does not hold in general) adding a strong iteration operator to the signature. Demonic refinement algebra was devised in [20] for reasoning about total-correctness preserving program transformations. A structure satisfying all the axioms of omega algebra except right strictness (called a weak omega algebra [14]) always has a greatest element $\top$. As one of the main contributions of this paper, we show that weak omega algebra with the extra axiom $\top x = \top$ is equivalent to demonic refinement algebra in the sense that they can be defined in terms of each other.

We then consider commands, that is, pairs (a, p) such that a describes the state transition behaviour and p characterises the states with guaranteed termination. Möller and Struth have already shown how the addition of modal operators on the underlying semiring facilitates definitions of operators on commands

⋆ This research was supported by DFG (German Research Foundation).

such that they form a weak Kleene and a weak omega algebra, respectively [14]. The definitions of these operators use modal operators, defined from the domain operator of Kleene algebra with domain [4]. To define a demonic refinement algebra of commands, we need a strong iteration operator on commands [19]. We define this operator with the aid of the above-mentioned result. The demonic refinement algebra of commands gives rise to a model that is not extensional, thus showing that the axioms of demonic refinement algebra do not characterise predicate-transformer models uniquely.

The definition of infinite iteration and strong iteration on commands both utilise the convergence operator of [13], that is, the underlying structure is actually assumed to be a convergence algebra. The convergence operator is analogous to the halting predicate of modal μ-calculus [8]. As the third result in this paper, we show that the convergence operator can be explicitly defined in terms of infinite iteration and domain if and only if domain coinduction for the infinite iteration operator is assumed to hold in general.

The historic development of this paper has it starting point in Kozen's axiomatisation of Kleene algebra and his injection of tests into the algebra [11], rendering reasoning about control structures possible. As mentioned earlier, Cohen [2] conservatively extends Kleene algebra with an infinite iteration operator. Von Wright's demonic refinement algebra, introducing the strong iteration operator, was the first algebra that was genuinely an algebra intended for total-correctness reasoning about programs. Desharnais, Möller and Struth's domain-operator extension [4] was the seminal work for modal operators in Kleene algebra. The domain operator was investigated in the context of refinement algebra in [18]. Möller later weakened the axiomatisation to form left semirings and left Kleene algebras [12]. The former is one of the most foundational structures found in this paper.

The paper is organised as follows. We begin in Sect. 2 by the result concerning the equivalence of top-left-strict weak omega algebra and demonic refinement algebra, upon which in Sect. 3 we construct the demonic refinement algebra of commands and relate it to the demonic algebras with domain of de Carufel and Desharnais [3]. In Sect. 4 we give some remarks on refinement algebra in the light of Sect. 3. Before concluding, we consider the explicit definition of the convergence operator in Sect. 5.

2 Omega and Demonic Refinement Algebra

We begin by recapitulating some basic definitions. By a *left semiring* we shall understand a structure $(+, 0, \cdot, 1)$ such that the reduct $(+, 0)$ is a commutative and idempotent monoid, and the reduct structure $(\cdot, 1)$ is a monoid such that $\cdot$ distributes over $+$ in its left argument and is left-strict, i.e., $0 \cdot a = 0$. A *weak semiring* is a left semiring that is also right-distributive. A weak semiring with right-strictness is called a *full semiring* or simply *semiring*. When no risk for confusion arises $\cdot$ is left implicit. We define the *natural order* $\leq$ on a left semiring by $a \leq b \Leftrightarrow_{df} a + b = b$ for all a and b in the carrier set. With respect

to that order, 0 is the least element and multiplication as well as addition are isotone. Moreover, $a + b$ is the join of a and b.

A *(weak) Kleene algebra* is a structure $(+, 0, \cdot, 1, ^*)$ such that the reduct $(+, 0, \cdot, 1)$ is a (weak) semiring and the star * satisfies the axioms

$$1 + aa^* \leq a^* , \qquad 1 + a^*a \leq a^* , \qquad (* \text{ unfold})$$
$$b + ac \leq c \Rightarrow a^*b \leq c , \qquad b + ca \leq c \Rightarrow ba^* \leq c , \qquad (* \text{ induction})$$

for a, b and c in the carrier set of the structure. A *(weak) omega algebra* [14] is a structure $(+, 0, \cdot, 1, ^*, ^\omega)$ such that the reduct $(+, 0, \cdot, 1, ^*)$ is a (weak) Kleene algebra and the infinite iteration $^\omega$ satisfies the axioms

$$a^\omega = aa^\omega , \qquad (\omega \text{ unfold})$$
$$c \leq b + ac \Rightarrow c \leq a^\omega + a^*b , \qquad (\omega \text{ coinduction})$$

for a, b and c in the carrier set of the structure. In particular, a^ω is the greatest fixpoint of the function $f(x) = ax$. The element 1^ω is the greatest element and we denote it by $\top$. Since, by the ω unfold law, $a^\omega\top$ is a fixpoint of f, we have $a^\omega = a^\omega\top$ for all a. We call a weak omega algebra *top-left-strict* iff the equation $\top a = \top$ holds for all a. In that case we get

$$a^\omega b = a^\omega \top b = a^\omega \top = a^\omega . \qquad (1)$$

In general omega algebra only the inequation $a^\omega b \leq a^\omega$ holds. The above derivation (1) strengthens it to an equation. In fact we have the following result.

Proposition 2.1. *Top-left-strictness is equivalent to left ω annihilation, i.e.,*

$$\top b = \top \Leftrightarrow (\forall\, a \bullet a^\omega \leq a^\omega b) .$$

Proof. The implication $(\Rightarrow)$ follows from (1), whereas $(\Leftarrow)$ can be calculated by

$$\begin{array}{ll} & (\forall\, a \bullet a^\omega \leq a^\omega b) \\ \Rightarrow & \quad \{\![\text{ set } a = 1]\!\} \\ & 1^\omega \leq 1^\omega b \\ \Leftrightarrow & \quad \{\![1^\omega = \top]\!\} \\ & \top \leq \top b . \end{array}$$

The other inequation $(\top b \leq \top)$ holds since $\top$ is the greatest element. □

A *demonic refinement algebra* [19] is a structure $(+, 0, \cdot, 1, ^*, ^{\overline{\omega}})$ such that the reduct $(+, 0, \cdot, 1, ^*)$ is a weak Kleene algebra and the strong iteration operator $^{\overline{\omega}}$ satisfies the axioms

$$a^{\overline{\omega}} = aa^{\overline{\omega}} + 1 , \qquad (\overline{\omega} \text{ unfold})$$
$$a^{\overline{\omega}} = a^* + x^{\overline{\omega}}0 , \qquad (\overline{\omega} \text{ isolation})$$
$$c \leq ac + b \Rightarrow c \leq a^{\overline{\omega}}b , \qquad (\overline{\omega} \text{ coinduction})$$

for a, b and c in the carrier set of the structure. It is easily shown that $1^{\overline{\omega}}$ is the greatest element and satisfies $1^{\overline{\omega}}a = 1^{\overline{\omega}}$ for all a in the carrier set [20]. This element is again denoted by $\top$.

In the remainder of this section we present one of our main contributions, namely that top-left-strict weak omega algebra is equivalent to demonic refinement algebra in the sense that they can be defined in terms of each other. This is done in two steps: First we show that weak omega algebra subsumes demonic refinement algebra, then we show the converse subsumption.

Lemma 2.2. *Top-left-strict weak omega algebra subsumes demonic refinement algebra.*

Proof. Given a top-left-strict weak omega algebra, the strong iteration is defined by $a^{\overline{\omega}} =_{df} a^* + a^\omega$. It is sufficient to show that this definition satisfies the axioms of strong iteration; the other axioms of demonic refinement algebra are immediate from the axioms of top-left-strict weak omega algebra.

1. $\overline{\omega}$ unfold:

$$
\begin{array}{ll}
 & a^{\overline{\omega}} \\
= & \quad \{\![\text{ definition }]\!\} \\
 & a^* + a^\omega \\
= & \quad \{\![* \text{ and } \omega \text{ unfold }]\!\} \\
 & aa^* + 1 + aa^\omega \\
= & \quad \{\![\text{ commutativity }]\!\} \\
 & aa^* + aa^\omega + 1 \\
= & \quad \{\![\text{ distributivity }]\!\} \\
 & a(a^* + a^\omega) + 1 \\
= & \quad \{\![\text{ definition }]\!\} \\
 & aa^{\overline{\omega}} + 1
\end{array}
$$

2. isolation:

$$
\begin{array}{ll}
 & a^{\overline{\omega}} \\
= & \quad \{\![\text{ definition }]\!\} \\
 & a^* + a^\omega \\
= & \quad \{\![\text{ neutrality of 0 and (1) }]\!\} \\
 & a^*(1 + 0) + a^\omega 0 \\
= & \quad \{\![\text{ right-distributivity }]\!\} \\
 & a^* + a^*0 + a^\omega 0 \\
= & \quad \{\![\text{ left-distributivity }]\!\} \\
 & a^* + (a^* + a^\omega)0 \\
= & \quad \{\![\text{ definition }]\!\} \\
 & a^* + a^{\overline{\omega}}0
\end{array}
$$

3. $\overline{\omega}$ coinduction:

$$
\begin{array}{ll}
 & c \leq a^{\overline{\omega}} b \\
\Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\
 & c \leq (a^* + a^\omega) b \\
\Leftrightarrow & \quad \{\![\text{ left-distributivity }]\!\} \\
 & c \leq a^* b + a^\omega b \\
\Leftrightarrow & \quad \{\![(1)]\!\} \\
 & c \leq a^* b + a^\omega \\
\Leftarrow & \quad \{\![\omega \text{ coinduction }]\!\} \\
 & c \leq ac + b
\end{array}
$$

□

In a concrete predicate-transformer algebra, the same definition of $\overline{\omega}$ is made by Back and von Wright [1]. In the present paper the definition is given in an abstract setting for which (conjunctive) predicate transformers constitute a model.

Lemma 2.3. *Demonic refinement algebra subsumes top-left-strict weak omega algebra.*

Proof. Given a demonic refinement algebra, infinite iteration is defined as $a^\omega \ =_{df} \ a^{\overline{\omega}} 0$. It is sufficient to show that this definition satisfies the axioms for infinite iteration; the other axioms of the top-left-strict weak omega algebra are immediate from demonic refinement algebra.

1. ω unfold:

$$
\begin{array}{ll}
 & a^\omega \\
= & \quad \{\![\text{ definition }]\!\} \\
 & a^{\overline{\omega}} 0 \\
= & \quad \{\![\overline{\omega} \text{ unfold }]\!\} \\
 & (aa^{\overline{\omega}} + 1)0 \\
= & \quad \{\![\text{ left-distributivity and neutrality of } 1]\!\} \\
 & aa^{\overline{\omega}} 0 + 0 \\
= & \quad \{\![\text{ neutrality of } 0]\!\} \\
 & aa^{\overline{\omega}} 0 \\
= & \quad \{\![\text{ definition }]\!\} \\
 & aa^\omega
\end{array}
$$

2. top-left-strictness:

$$
\begin{array}{ll}
 & \top \leq \top a \\
\Leftrightarrow & \quad \{\![\top = 1^{\overline{\omega}}]\!\} \\
 & \top \leq 1^{\overline{\omega}} a
\end{array}
$$

$$
\begin{array}{ll}
\Leftarrow & \{\![\ \overline{\omega}\ \text{coinduction}\ ]\!\} \\
& \top \leq \top + a \\
\Leftrightarrow & \{\![\ \text{join}\ ]\!\} \\
& \mathsf{true}
\end{array}
$$

$\top a \leq \top$ holds since $\top$ is the greatest element.

3. ω coinduction:

$$
\begin{array}{ll}
& c \leq a^*b + a^\omega \\
\Leftrightarrow & \{\![\ \text{definition}\ ]\!\} \\
& c \leq a^*b + a^{\overline{\omega}}0 \\
\Leftrightarrow & \{\![\ \text{annihilation}\ ]\!\} \\
& c \leq a^*b + a^{\overline{\omega}}0b \\
\Leftrightarrow & \{\![\ \text{distributivity}\ ]\!\} \\
& c \leq (a^* + a^{\overline{\omega}}0)b \\
\Leftrightarrow & \{\![\ \text{isolation}\ ]\!\} \\
& c \leq a^{\overline{\omega}}b \\
\Leftarrow & \{\![\ \overline{\omega}\ \text{coinduction}\ ]\!\} \\
& c \leq ac + b
\end{array}
$$

□

The above lemmas directly yield the following theorem.

Theorem 2.4. *Top-left-strict weak omega algebra and demonic refinement algebra are equivalent in the sense that they can be defined in terms of each other.*

3 The Demonic Refinement Algebra of Commands

So far, our semiring elements could be viewed as abstract representations of state transition systems. We now want to introduce a way of dealing with sets of states in an abstract algebraic way. This is done using tests. A *test semiring* is a structure $(\mathcal{S}, \mathsf{test}(S))$, where $\mathcal{S} = (S, +, 0, \cdot, 1)$ is a semiring and $\mathsf{test}(S)$ is a Boolean subalgebra of the interval $[0, 1] \subseteq S$ with $0,\ 1 \in \mathsf{test}(S)$. Join and meet in $\mathsf{test}(S)$ coincide with $+$ and $\cdot$, the complement is denoted by $\neg$, 0 is the least and 1 is the greatest element. Furthermore, this definition of test semiring coincides with the definition on Kleene algebras given in [11]. We use $a, b, \ldots$ for general semiring elements and $p, q, \ldots$ for tests.

On a test semiring we axiomatise a domain operator $\ulcorner : S \to \mathsf{test}(S)$ by

$$a \leq \ulcorner a \cdot a\ , \tag{d1}$$

$$\ulcorner(pa) \leq p\ , \tag{d2}$$

$$\ulcorner(a\ulcorner b) \leq \ulcorner(ab)\ , \tag{d3}$$

for all $a \in S$ and $p \in \mathsf{test}(S)$. Inequations (d1) and (d3) can be strengthened to equations. Many properties of domain can be found in [4]. For example, we have stability of tests and additivity of domain, i.e.,

$$\ulcorner p = p \ , \tag{2}$$

$$\ulcorner(a+b) = \ulcorner a + \ulcorner b \ . \tag{3}$$

With the aid of this operator, we can define modal operators by

$$|a\rangle p =_{df} \ulcorner(ap) \quad \text{and} \quad |a]p =_{df} \neg|a\rangle\neg p \ .$$

This is the reason why we shall call a test semiring with a domain operator *modal*. All the structures above extending a weak semiring are called *modal* when the underlying weak semiring is modal.

Given a modal semiring $\mathcal{S} = (S, +, 0, \cdot, 1)$ we define the set of commands (over S) as $\mathrm{COM}(S) =_{df} S \times \mathsf{test}(S)$. Three basic non-iterative commands and two basic operators on commands are defined by

$$\begin{aligned} \mathsf{fail} &=_{df} (0,1) \\ \mathsf{skip} &=_{df} (1,1) \\ \mathsf{loop} &=_{df} (0,0) \\ (a,p) \,[\!]\, (b,q) &=_{df} (a+b, pq) \\ (a,p)\,;(b,q) &=_{df} (ab, p \cdot [a]q) \end{aligned}$$

As noted by Möller and Struth in [14] the structure $(\mathrm{COM}(S), [\!], \mathsf{fail}, ;, \mathsf{skip})$ forms a weak semiring. The natural order on the command weak semiring is given by $(a,p) \leq (b,q) \Leftrightarrow a \leq b \wedge q \leq p$. We will discuss below how it connects to the usual refinement relation.

If $\mathcal{S}$ is even a weak Kleene algebra, a star operator can be defined by

$$(a,p)^* =_{df} (a^*, |a^*]p)$$

and then $(\mathrm{COM}(S), [\!], \mathsf{fail}, ;, \mathsf{skip}, ^*)$ forms a weak Kleene algebra [14].

Defining an omega operator over the set of commands does not work as simply as for star. To do this, we also need to assume that the underlying modal omega algebra $(S, +, 0, \cdot, 1, ^*, ^\omega)$ comes equipped with a convergence operator [14] $\triangle : S \to \mathsf{test}(S)$ satisfying

$$|a](\triangle a) \leq \triangle a \ , \qquad (\triangle \text{ unfold})$$

$$q \cdot |a]p \leq p \Rightarrow \triangle a \cdot |a^*]q \leq p \ . \qquad (\triangle \text{ induction})$$

In [14] it is shown that $\triangle a$ is the least (pre-)fixed point of $|a]$. The test $\triangle a$ characterises the states from which no infinite transition paths emanate. It corresponds to the halting predicate of the modal μ-calculus [8].

The infinite iteration operator on commands can then be defined by

$$(a,p)^\omega =_{df} (a^\omega, \triangle a \cdot [a^*]p) \ .$$

The greatest command is $\mathsf{chaos} =_{df} \mathsf{skip}^{\omega} = (\top, 0)$.

The semiring of commands reflects the view of general correctness as introduced in [17]. Therefore it is not to be expected that it forms a demonic refinement algebra which was designed for reasoning about total correctness. Indeed, top-left-strictness fails unless it is already satisfied in the underlying semiring $\mathcal{S}$, since $\mathsf{chaos}\,;(a,p) = (\top a, 0) = \mathsf{chaos}$ iff $\top a = \top$.

There is, however, another possibility. One can define a refinement preorder on commands by

$$(a,p) \sqsubseteq (b,q) \;\Leftrightarrow_{df}\; q \leq p \wedge qa \leq b \;.$$

This is the converse of the usual refinement relation: $k \sqsubseteq l$ for any two commands k, l means that k refines l. We have chosen this direction, since by straightforward calculation we get the implication $k \leq l \;\Rightarrow\; k \sqsubseteq l$. The associated equivalence relation $\equiv$ is defined by

$$k \equiv l \;\Leftrightarrow_{df}\; k \sqsubseteq l \wedge l \sqsubseteq k \;.$$

Componentwise, it works out to $(a,p) \equiv (b,q) \Leftrightarrow p = q \wedge pa = pb$. The equivalence classes correspond to the designs of the Unifying Theories of Programming of [9] and hence represent a total correctness view.

It has been shown in [7] (in the setting of condition semirings that is isomorphic to that of test semirings) that the set of these classes forms again a left semiring and can be made into a weak Kleene and omega algebra by using exactly the same definitions as above (as class representatives).

Now top-left-strictness holds, since $\mathsf{chaos} \equiv \mathsf{loop}$ and loop is a left zero by the definition of command composition. Therefore the set of $\equiv$-classes of commands can be made into a demonic refinement algebra. Let $\mathrm{CCOM}(S)$ be the set of all these classes.

By Lemma 2.2 the strong iteration of commands is

$$(a,p)^{\overline{\omega}} = (a,p)^{*} \,[\!]\, (a,p)^{\omega} \;,$$

and thus $(\mathrm{CCOM}(S), [\!], \mathsf{fail}, ;, \mathsf{skip}, ^{*}, ^{\overline{\omega}})$ constitutes a demonic refinement algebra of commands. The above expression can be simplified by

$$\begin{array}{ll} & (a,p)^{*} \,[\!]\, (a,p)^{\omega} \\ = & \quad \{\![\text{ definition of } ^{*} \text{ and } ^{\omega} \text{ on commands }]\!\} \\ & (a^{*}, [a^{*}]p) \,[\!]\, (a^{\omega}, \triangle a \cdot [a^{*}]p) \\ = & \quad \{\![\text{ definition of } [\!] \;]\!\} \\ & (a^{*} + a^{\omega}, [a^{*}]p \cdot \triangle a \cdot [a^{*}]p) \\ = & \quad \{\![\text{ definition of } \overline{\omega}, \text{ commutativity and idempotence of tests }]\!\} \\ & (a^{\overline{\omega}}, \triangle a \cdot [a^{*}]p) \;. \end{array}$$

Thus strong iteration of commands can also be expressed as

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

We conclude this section by relating the command algebra to the demonic algebras (DA) of [3]. These are intended to capture the notion of total correctness in an algebraic fashion. Since their axiomatisation is extensive, we do not want to repeat it here. We only want to point out that a subalgebra of the command algebra yields a model of DA. This is formed by the $\equiv$-classes of *feasible* commands which are pairs (a, p) with $p \leq \lceil a$. So these model programs where no miraculous termination can occur; they correspond to the feasible designs of [9]. In [7] it is shown that the set $\mathrm{F}(S)$ classes of feasible commands can isomorphically be represented by simple semiring elements. The mediating functions are

$$\begin{array}{ll} E : \mathrm{F}(S) \to S \;, & D : S \to \mathrm{F}(S) \;, \\ E((a,p)) =_{df} pa \;, & D(a) =_{df} (a, \lceil a) \;. \end{array}$$

Then one has $E(D(a)) = a$ and $D(E(a,p)) \equiv (a,p)$. Moreover, the demonic refinement ordering of [3] is induced on S by

$$a \sqsubseteq b \Leftrightarrow_{df} D(a) \sqsubseteq D(b) \Leftrightarrow \lceil b \leq \lceil a \wedge \lceil b \cdot a \leq b$$

and demonic join and composition by

$$\begin{array}{lll} a \sqcup b & =_{df} & E(D(a) \mathbin{[]} D(b)) = \lceil a \cdot \lceil b \cdot (a+b) \;, \\ a \mathbin{\triangledown} b & =_{df} & E(D(a) \,;\, D(b)) = |a] \lceil b \cdot a \cdot b \;. \end{array}$$

Using pairs (p,p) as demonic tests in $\mathrm{F}(S)$ one even obtains a DA with domain. Further details are left to a future publication.

4 Two Remarks on Refinement Algebra

In this section we remark that demonic refinement algebra does not characterise predicate transformer models uniquely. We also remark that an equivalence similar to that of Theorem 2.4 cannot be established between general refinement algebra [20] and a top-left-strict strong left omega algebra.

Characterisation of the predicate transformer models. To connect the algebra of commands to predicate transformer models we first define

$$\mathsf{wp}.(a,p).q =_{df} p \cdot [a]q$$

and get

$$\mathsf{wp.fail}.q = 1 \qquad \text{and} \qquad \mathsf{wp.chaos}.q = 0 \;.$$

Hence fail can be interpreted as magic in the refinement calculus tradition and chaos as abort. Indeed, chaos is refined by every command and every command is refined by fail. Furthermore, we have the implications, for commands k, l,

$$k \leq l \;\Rightarrow\; k \sqsubseteq l \;\Rightarrow\; (\forall p \in \mathsf{test}(S) \bullet \mathsf{wp}.k.p \geq \mathsf{wp}.l.p) \;.$$

However, the command model of demonic refinement algebra is, unlike predicate transformer models as presented in [19, 20], in general not extensional in that we do not necessarily have the converse implications. In particular,

$$(\forall p \in \mathsf{test}(S) \bullet \mathsf{wp}.k.p = \mathsf{wp}.l.p) \Rightarrow k = l$$

holds iff already the underlying semiring $\mathcal{S}$ is *extensional*, i.e., satisfies, for $a, b \in S$,

$$[a] = [b] \Rightarrow a = b \ .$$

Contrarily, in concrete predicate transformer models the elements are mappings $T, U : \wp(\Sigma) \to \wp(\Sigma)$, where Σ is any set. They can be seen as semantic values that arise by applying the wp operator to concrete programming constructs. Their equality is defined by

$$T = U \ \Leftrightarrow_{df} \ (\forall p \in \wp(\Sigma) \bullet T.p \ = \ U.p) \ .$$

Hence in concrete predicate transformer models extensionality always holds.

Since the command model of DRA is non-extensional, this observation shows that the DRA axioms do notrestrict their models to algebras isomorphic to predicate transformer algebras and hence do not uniquely capture this type of algebras.

A similar move for general refinement algebra? A *left Kleene algebra* is a left semiring extended with two axioms for *

$$1 + aa^* \leq a^* \qquad \text{and} \qquad b + ac \leq c \ \Rightarrow \ a^*b \leq c \ ,$$

laid down in Sect. 2. A *left omega algebra* is a left Kleene algebra extended with an infinite iteration operator ω axiomatised as in Sect. 2. Clearly, every left omega algebra has a greatest element $\top$, and along the lines above we call a left omega algebra *top-left-strict* when $\top$ satisfies $\top a \ = \ \top$. A *general refinement algebra* [20] is a left Kleene algebra extended with the axioms for $\overline{\omega}$ found in Sect. 2, except the isolation axiom, i.e., $a^{\overline{\omega}} \ = \ a^* + a^{\overline{\omega}}0$ does not hold in general. A general refinement algebra becomes a demonic refinement algebra by adding the other two axioms for * of Sect. 2, right-distributivity and isolation.

It is tempting to try to show that top-left-strict left omega algebra corresponds to general refinement algebra in a similar way as top-left-strict weak omega algebra corresponds to demonic refinement algebra (Theorem 2.4). However, this is not possible as the following argument shows.

Let Σ be any set and let $T : \wp(\Sigma) \to (\Sigma)$ be any predicate transformer. If $p, q \in \wp(\Sigma)$ and T satisfies $p \subseteq q \Rightarrow T.p \subseteq T.q$ then T is *isotone*[1]. If T satisfies $T.(\bigcap_{i \in I} p_i) \ = \ \bigcap_{i \in I}(T.p_i)$, for any index set I, it is *conjunctive*. The isotone predicate transformers constitute a model for general refinement algebra [20]. The reason why isolation is dropped is that it does not hold for isotone predicate

[1] In the literature these predicate transformers are usually called monotone [1]. However, in other contexts the term monotone can mean isotone *or* antitone.

transformers in general [1, 20]. Since isolation is an essential property needed for proving ω coinduction under the interpretation $a^\omega =_{df} a^{\overline{\omega}}0$, it is not possible to prove that demonic refinement algebra subsumes top-left-strict strong left omega algebra. For the same reason, one cannot define strong iteration as $a^{\overline{\omega}} =_{df} a^* + a^\omega$ since this is valid only for conjunctive predicate transformers [1]. I.e., one cannot prove that top-left-strict strong left omega algebra subsumes general refinement algebra in an analogous way to the proof of Lemma 2.3.

5 Making Convergence Explicit

In this section, we prove a result concerning the convergence operator of Sect. 3: having a convergence operator such that $\triangle a = \neg\ulcorner a^\omega$ is equivalent to having ω coinduction for the domain operator. Since $\triangle a = \neg\ulcorner a^\omega$ does not hold in all models of weak omega algebra [5], we also know that ω coinduction for domain does not follow from the axioms of omega algebra.

Proposition 5.1. *Omega coinduction for the domain operator, i.e.,*

$$p \leq \ulcorner(q + ap) \Rrightarrow p \leq \ulcorner(a^\omega + a^*q) \ ,$$

holds if and only if $\triangle a = \neg\ulcorner a^\omega$ does.

Proof. The convergence operator is given by the implicit axiomatisation of Sect. 2. It is unique by the fact that it is a least fixpoint. We show that $\neg\ulcorner a^\omega$ always satisfies the $\triangle$ unfold axiom and that it satisfies the $\triangle$ induction axiom if and only if ω coinduction for the domain operator holds:

1. $|a]\neg\ulcorner a^\omega \leq \neg\ulcorner a^\omega$
   $\Leftrightarrow$ {[definition of $|\_]$ and Boolean algebra]}
   $\neg|a\rangle\ulcorner a^\omega \leq \neg\ulcorner a^\omega$
   $\Leftrightarrow$ {[shunting]}
   $\ulcorner a^\omega \leq \langle a\rangle\ulcorner a^\omega$
   $\Leftrightarrow$ {[definition of $|\_\rangle$]}
   $\ulcorner a^\omega \leq \ulcorner(a\ulcorner a^\omega)$
   $\Leftrightarrow$ {[(d3)]}
   $\ulcorner a^\omega \leq \ulcorner(aa^\omega)$
   $\Leftrightarrow$ {[ω unfold]}
   $\ulcorner a^\omega \leq \ulcorner a^\omega$
   $\Leftrightarrow$ {[reflexivity]}
   true

2. $q \cdot |a]p \leq p \ \Rightarrow\ \neg\ulcorner a^\omega \cdot [a^*]q \leq p$
   $\Leftrightarrow$ {[Boolean algebra]}
   $\neg p \leq \neg|a]p + \neg q \ \Rightarrow\ \neg p \leq \ulcorner a^\omega + \neg|a^*]q$
   $\Leftrightarrow$ {[definition of $|\_]$ and Boolean algebra]}

$$
\begin{array}{ll}
& \neg p \leq |a\rangle \neg p + \neg q \;\Rightarrow\; \neg p \leq \lceil a^\omega + |a^*\rangle \neg q \\
\Leftrightarrow & \quad \{\![\text{ definition of } |\_\rangle \;]\!\} \\
& \neg p \leq \lceil (a \neg p) + \neg q \Rightarrow \neg p \leq \lceil a^\omega + \lceil (a^* \neg q) \\
\Leftrightarrow & \quad \{\![\text{ set } \neg p = r \text{ and } \neg q = s \;]\!\} \\
& r \leq \lceil (ar) + s \Rightarrow r \leq \lceil a^\omega + \lceil (a^* s) \\
\Leftrightarrow & \quad \{\![\text{ (2) and (3) }]\!\} \\
& r \leq \lceil (ar + s) \Rightarrow r \leq \lceil (a^\omega + a^* s)
\end{array}
$$

Assume now that ω coinduction for the domain operator holds. By the above calculations $\neg\lceil a^\omega$ then satisfies both $\triangle$ unfold and $\triangle$ induction. Since these axioms impose uniqueness, we have that $\triangle a = \neg\lceil a^\omega$. If, conversely, $\triangle a = \neg\lceil a^\omega$ is assumed then the implication in the first line of the above calculation for 2. is true by $\triangle$ induction and hence ω coinduction for domain holds. □

This means that in a command omega or demonic refinement algebra based on an omega algebra where ω coinduction for the domain operator holds, infinite and strong iteration can be defined as

$$(a,p)^\omega =_{df} (a^\omega, \neg\lceil a^\omega \cdot [a^*]p) \qquad \text{and} \qquad (a,p)^{\overline{\omega}} =_{df} (a^{\overline{\omega}}, \neg\lceil a^\omega \cdot [a^*]p) \;,$$

respectively.

We finally note that the special case $q = 0$ of the ω coinduction rule for domain (Prop. 5.1) has been termed *cycle rule* and used as an additional postulate in the computation calculus of R. Dijkstra [6].

6 Conclusion

Top-left-strict omega algebra and demonic refinement algebra are equivalent in the sense that they can be defined in terms of each other. In particular, results from one of these frameworks can now be reused in the other. The equivalence also facilitates the definition of a demonic refinement algebra of commands, yielding a model in which extensionality does not hold. Since extensionality always holds in predicate-transformer models, it can be concluded that demonic refinement algebra does not characterise predicate transformers uniquely. A similar equality between general refinement algebra and top-left-strict left omega algebra as between demonic refinement algebra and top-left-strict weak omega algebra cannot be shown. The demonic refinement algebra and the omega algebra of commands are based on the convergence operator. In a modal demonic refinement or omega algebra that satisfies domain coinduction for infinite iteration, the convergence operator can be defined explicitly in terms of infinite iteration and domain.

Having set up the connections between various algebraic structures allows mutual re-use of the large existing body of results about Kleene/ω algebra with tests and modal Kleene/ω algebra as well as demonic refinement algebra and action systems. Having embedded the command algebras we can also apply the general algebraic results to UTP and related systems.

References

1. R.J. Back, J. von Wright: Refinement calculus: a systematic introduction. Springer 1998
2. E. Cohen: Separation and reduction. In R. Backhouse, J. Oliveira (eds.): Mathematics of Program Construction. LNCS 1837. Springer 2000, 45–59
3. J.-L. de Carufel, J. Desharnais: Demonic algebra with domain. In: R. Schmidt, G. Struth (eds.): Relations and Kleene Algebra in Computer Science. LNCS (this volume). Springer 2006 (to appear)
4. J. Desharnais, B. Möller, G. Struth: Kleene algebra with domain. Technical Report 2003-7, Universität Augsburg, Institut für Informatik, 2003. Revised version to appear in ACM TOCL
5. J. Desharnais, B. Möller, G. Struth: Termination in modal Kleene algebra. In J.-J. Lévy, E. Mayr, J. Mitchell (eds.): Exploring new frontiers of theoretical informatics. IFIP International Federation for Information Processing Series 155. Kluwer 2004, 653–666
6. R.M. Dijkstra: Computation calculus bridging a formalisation gap. Science of Computer Programming 37, 3-36 (2000)
7. W. Guttmann, B. Möller: Modal design algebra. In S. Dunne, B. Stoddart (eds.): Proc. First International Symposium on Unifying Theories of Programming. LNCS 4010. Springer 2006, 236–256
8. D. Harel, D. Kozen, J. Tiuryn: Dynamic Logic. MIT Press 2000
9. C.A.R. Hoare, J. He: Unifying theories of programming. Prentice Hall 1998
10. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Inf. Comput. 110, 366–390 (1994)
11. D. Kozen: Kleene algebra with tests. ACM Transactions on Programming Languages and Systems 19, 427–443 (1997)
12. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. LNCS 3125. Springer 2004, 252–273. Revised version: B. Möller: Kleene getting lazy. Sci. Comput. Prog. (to appear)
13. B. Möller, G. Struth: Modal Kleene algebra and partial correctness. In C. Rattray, S. Maharaj, C. Shankland (eds.): Algebraic methodology and software technology. LNCS 3116. Springer 2004, 379–393. Revised and extended version: B. Möller, G. Struth: Algebras of modal operators and partial correctness. Theoretical Computer Science 351, 221–239 (2006)
14. B. Möller, G. Struth: wp is wlp. In W. MacCaull, M. Winter, I. Düntsch (eds.): Relational methods in computer Science. LNCS 3929. Springer 2006, 200-211
15. C. Morgan: Data Refinement by Miracles. Inf. Process. Lett. 26, 243-246 (1988)
16. J.M. Morris, Laws of data refinement, Acta Informatica (26), 287-308 (1989)
17. G. Nelson: A generalization of Dijkstra's calculus. ACM TOPLAS 11, 517–561 (1989)
18. K. Solin and J. von Wright: Refinement algebra with operators for enabledness and termination. In T. Uustalu (ed.): Mathematics of Program Construction. LNCS 4014. Springer 2006, 397–415
19. J. von Wright: From Kleene algebra to refinement algebra. In E. Boiten, B. Möiller (eds.): Mathematics of Program Construction. LNCS 2386. Springer 2002, 233–262
20. J. von Wright: Towards a refinement algebra. Sci. Comput. Prog. 51, 23–45 (2004)