General Correctness Algebra

Walter Guttmann

Institut für Programmiermethodik und Compilerbau
Universität Ulm, 89069 Ulm, Germany
walter.guttmann@uni-ulm.de

Abstract. General correctness offers a finer semantics of programs than partial and total correctness. We give an algebraic account continuing and extending previous approaches. In particular, we propose axioms, correctness statements, a correctness calculus, specification constructs and a loop refinement rule. The Egli-Milner order is treated algebraically and we show how to obtain least fixpoints, used to solve recursion equations, in terms of the natural order.

1 Introduction

Relational approaches to program semantics vary in their treatment of termination according to [19].

Partial correctness does not distinguish between terminating and possibly non-terminating programs. Recursion is modelled by least fixpoints with respect to the subset order, which leads to angelic non-determinism. If the same program admits both a terminating and a non-terminating execution, the terminating one is chosen. Theories of partial correctness include Hoare logic [16], weakest liberal preconditions [9] and Kleene algebra with tests [21].

Total correctness does not distinguish between non-terminating and possibly terminating programs. Recursion is modelled by greatest fixpoints with respect to the subset order, which leads to demonic non-determinism. If the same program admits both a terminating and a non-terminating execution, the non-terminating one is chosen. Theories of total correctness include weakest preconditions [9], the Unifying Theories of Programming [17], demonic refinement algebra [26] and demonic algebra [5].

General correctness [2, 4, 19, 3, 25, 10, 24] distinguishes terminating and non-terminating executions. Recursion is modelled by least fixpoints with respect to the Egli-Milner order, which leads to erratic non-determinism.

Technically, partial correctness is the simplest approach, since there is no need to represent non-termination. For total and general correctness, this is done by adding a special value, predicate or variable. In total correctness, additionally, non-termination absorbs termination. This price is paid to keep the subset order, while in general correctness the more complicated Egli-Milner order must be used for fixpoints. Refinement is the subset order in all three approaches.

In this paper we focus on the algebraic treatment of general correctness. It offers a finer distinction than partial and total correctness [19, 11]. We build upon a number of works, as discussed in the following.

In [10] the Unifying Theories of Programming are adapted to general correctness using a restricted class of predicates called ‘prescriptions’. They are generalised using matrices over semirings in [23]. While the semantics of loops is missing for prescriptions, it is given in [24] using ‘commands’ over modal semirings and the Egli-Milner order. Still missing, however, is the semantics of full recursion. This is contributed by Section 6 of the present paper.

Another result of [24] is that weakest preconditions are actually the weakest liberal preconditions of an appropriate modal semiring. It is used to derive a Hoare calculus for weakest preconditions. As such, the calculus is useful for total correctness claims. To this end, however, a total correctness semantics of commands, such as the one given in [14], would be more appropriate and also more simple by not having to use the Egli-Milner order. Another way to overcome the mismatch is to devise a calculus for general correctness claims. This is contributed by Section 4 of the present paper.

In [12] the absence of loop refinement rules is noted for general correctness, in contrast to total correctness. They are necessary to introduce loops when specifications are refined into programs. A general correctness loop rule is given based on prescriptions. Section 5 of the present paper contributes an algebraic statement and proof of that rule, using the calculus of Section 4.

As another ingredient of refinement, [26] discusses specifications given only by preconditions and postconditions in demonic refinement algebra. Such ‘pre-post specifications’ can conveniently be used to express rules like the one for loop refinement. To this end, Section 5 also contributes specifications suitable for general correctness.

All contributions are wrapped in an algebraic theory of general correctness encompassing those of [10, 24, 23, 12] along the lines of [15]. It is based on Kleene algebra with a domain operator and developed in Section 2 of the present paper. Section 3 takes it as a guide and contributes an axiomatic description of the key constituents of general correctness, such as the Egli-Milner order. The axioms are used to derive the results announced above.

2 Semirings and prescriptions

Prescriptions have been introduced in [10] to model general correctness in the Unifying Theories of Programming. An algebraic account using modal semirings is given in [24] and, using matrices over modal semirings, in [23]. In this section, we adapt these approaches and develop them further according to our treatment of total correctness [15].

We first recall how to extend semirings by axioms for conditions, which represent subsets of states. Based on this structure, we algebraically define prescriptions, which model programs and specifications in general correctness. To conveniently express the semantics of loops, we then introduce the Kleene star and omega operations. We finally impose further structure using the domain operation, which is necessary for our axiomatic treatment of general correctness in Section 3.

2.1 Condition semirings

A *weak semiring* is a structure $(S,+,0,\cdot,1)$ such that $(S,+,0)$ is a commutative monoid, $(S,\cdot,1)$ is a monoid, the operation $\cdot$ distributes over $+$ in both arguments and 0 is a left annihilator, that is, $0\cdot x=0$. We assume $0\neq 1$, otherwise S would be trivial. A weak semiring is *idempotent* if $+$ is, that is, if $x+x=x$. In an idempotent weak semiring the relation $x\leq y \Leftrightarrow_{\mathrm{def}} x+y=y$ is a partial order, called the *natural order* on S, and $\cdot$ and $+$ are isotone. A *semiring* is a weak semiring in which 0 is also a right annihilator, that is, $x\cdot 0=0$. The $\cdot$ operation is extended elementwise to sets $A,B\subseteq S$ by $A\cdot B=_{\mathrm{def}}\{a\cdot b\mid a\in A\wedge b\in B\}$ and $A\cdot b=_{\mathrm{def}} A\cdot\{b\}$ for $b\in S$. We frequently abbreviate $a\cdot b$ with ab.

A structure $(S,T,+,0,\cdot,1,\sqcap,\top,\overline{})$ is a *condition semiring* if the following properties hold.

- $(S,+,0,\cdot,1)$ is an idempotent weak semiring having a greatest element $\top$.
- $(T,+,0)$ is a submonoid of $(S,+,0)$ and $T\subseteq T\cdot\top$.
- The *restriction operation* $\sqcap : T\times S\to S$ distributes over $+$, that is,
  - $\forall a\in S:\forall t,u\in T:(t+u)\sqcap a=(t\sqcap a)+(u\sqcap a)$ and
  - $\forall a,b\in S:\forall t\in T:t\sqcap(a+b)=(t\sqcap a)+(t\sqcap b)$.
- $\forall a\in S:\top\sqcap a=a$.
- $(T,+,0,\sqcap,\top,\overline{})$ is a Boolean algebra; in particular, $0\in T$ and $\top\in T$.

We abbreviate condition semirings with (S,T) and call the elements of T *conditions*. A condition semiring (S,T) is an *ideal condition semiring* if $S\cdot T\subseteq T$, hence T is a left ideal of S. An (ideal) condition semiring is *strict* if the underlying weak semiring is a semiring, that is, if 0 is both a left and a right annihilator.

Our notation reflects the intended, relational model (where 0, 1 and $\top$ are the empty, identity and universal relations, respectively, and $\leq$ is the subset order), so that $0\leq 1\leq\top$ holds, for example. To avoid confusion, it should be kept in mind that other approaches in the literature use different conventions (for example, demonic refinement algebra [26] uses the reverse order).

In relational semantics, a condition semiring (S,T) is used as follows. The state transition relation or input/output behaviour of programs is represented by elements of S. The elements of T represent subsets of states by relating each initial state in the subset to all final states. The operations $+$, $\cdot$ and $\sqcap$ model non-deterministic choice, sequential composition and input-restriction, respectively. In particular, $t\sqcap a$ restricts the transitions permitted by a to those starting in a state described by the condition t. The elements of T are also used as preconditions that represent those states from which a non-terminating execution of the program exists.

The following, basic properties are proved in [15]. In a condition semiring (S,T), the operation $\sqcap$ is associative, isotone, the greatest lower bound on $T\times S$ and satisfies the shunting rule $t\sqcap a\leq b\Leftrightarrow a\leq\overline{t}+b$ as well as $(t\sqcap a)\cdot b=t\sqcap(a\cdot b)$ for all $t\in T$ and $a,b\in S$. Reminding us that conditions represent the vectors of relation algebra, we have $t\cdot\top=t$ for all $t\in T$, and thus $T\cdot\top=T$. In an ideal condition semiring (S,T) this extends to $S\cdot T=S\cdot\top=T\cdot\top=T$.

2.2 Prescriptions

We continue with the matrix representation of prescriptions, generalised to the present axiomatisation. Let (S, T) be an ideal condition semiring. The set of *normal prescriptions* over (S, T) is

$$\mathrm{NP}(S,T) =_{\mathrm{def}} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S^{2\times 2} \;\middle|\; a = \top \wedge b = 0 \wedge c \in T \right\} .$$

The components a and b are for structural purposes, making composition work as expected. The components c and d are the precondition and transition elements mentioned above. The adjective 'normal' [10] refers to the restriction $c \in T$, by which preconditions are indeed conditions on the initial states and not arbitrary relations between input and output states. For $t \in T$ and $a \in S$, we define the *normal prescription*

$$(t \Vdash a) =_{\mathrm{def}} \begin{pmatrix} \top & 0 \\ \overline{t} & a \end{pmatrix} .$$

It represents the program whose execution performs transitions allowed by a and is guaranteed to terminate when started in states described by t.

Particular normal prescriptions are $\mathsf{skip} =_{\mathrm{def}} (\top \Vdash 1)$, $\mathsf{loop} =_{\mathrm{def}} (0 \Vdash 0)$, $\mathsf{fail} =_{\mathrm{def}} (\top \Vdash 0)$, $\mathsf{havoc} =_{\mathrm{def}} (\top \Vdash \top)$ and $\mathsf{chaos} =_{\mathrm{def}} (0 \Vdash \top)$. For example, skip models the program which must terminate without changing the state, and loop the one which must not terminate, see [25].

These special prescriptions are landmarks of the structure inherent to normal prescriptions as follows. Let (S, T) be a strict ideal condition semiring, then $(\mathrm{NP}(S,T), +, \mathsf{fail}, \cdot, \mathsf{skip})$ is an idempotent weak semiring. Using the set $C =_{\mathrm{def}} \{(\overline{t} \Vdash t) \mid t \in T\}$ as conditions, $(\mathrm{NP}(S,T), C, +, \mathsf{fail}, \cdot, \mathsf{skip}, \sqcap, \mathsf{chaos}, \overline{})$ is a condition semiring. The operations $+$ and $\sqcap$ act elementwise on the matrices, $\cdot$ is the matrix product, and $\overline{}$ applies to both arguments of $\Vdash$. Both strictness and the ideal property are necessary for these results, which are proved analogously to the corresponding ones in [15] that apply to 'normal designs' modelling total correctness. The technical difference is that the matrices for normal designs satisfy $b = \top$ instead of $b = 0$ and the additional restriction $c \leq d$ that lets nontermination absorb terminating transitions (for example, $c = \top$ forces $d = \top$).

To appreciate the different structures introduced above we note the following distinctions. Relations form a strict ideal condition semiring. Normal designs over relations [15], which are the basis of the Unifying Theories of Programming, form an ideal condition semiring that is not strict. Normal prescriptions over relations, which are the basis of general correctness semantics, form a condition semiring that is not an ideal condition semiring. Every idempotent weak semiring with $\top$ forms a condition semiring with 0 and $\top$ as the only conditions, but all previous structures generally contain additional conditions.

In the remainder of this paper, we omit the adjective 'normal'. Several consequences about the natural order, sum and product of prescriptions are

- $(t \Vdash a) \leq (u \Vdash b) \Leftrightarrow u \leq t \wedge a \leq b$,
- $(t \Vdash a) + (u \Vdash b) = (t \sqcap u \Vdash a + b)$ and

– $(t \Vdash a) \cdot (u \Vdash b) = (t \sqcap \overline{a\overline{u}} \Vdash ab)$.

Hence prescriptions are equal just if both components are equal, fail is the least prescription and chaos the greatest. Moreover, $(t \Vdash 0)$ is a left annihilator for each $t \in T$. The vector property of prescriptions is derived by

$$(\bar{t} \Vdash t) \cdot (0 \Vdash \top) = (\bar{t} \sqcap \overline{t\overline{0}} \Vdash t\top) = (\bar{t} \sqcap \overline{t\top} \Vdash t) = (\bar{t} \sqcap \bar{t} \Vdash t) = (\bar{t} \Vdash t) \; .$$

An intuitive interpretation of the natural order is that non-terminating executions may be refined to terminating ones that do not introduce new transitions. This contrasts with designs, where any terminating execution can be introduced by such a refinement.

2.3 Kleene algebra and omega algebra

A *(weak) Kleene algebra* [20, 22] is a structure $(S, {}^*)$ such that S is an idempotent (weak) semiring and the operation star * satisfies the unfold and induction laws

$$\begin{aligned} 1 + a \cdot a^* &\le a^* & \qquad b + a \cdot c \le c &\Rightarrow a^* \cdot b \le c \\ 1 + a^* \cdot a &\le a^* & \qquad b + c \cdot a \le c &\Rightarrow b \cdot a^* \le c \end{aligned}$$

for $a, b, c \in S$. Hence a^*b is the least fixpoint of $\lambda x.ax + b$, denoted $\mu x.ax + b$. The star operation on prescriptions is derived using the general matrix construction presented, for example, in [13]. Let (S, T) be an ideal condition semiring such that S is a Kleene algebra, then $(\mathrm{NP}(S, T), +, \mathsf{fail}, \cdot, \mathsf{skip}, {}^*)$ is a weak Kleene algebra, where

$$\begin{pmatrix} \top & 0 \\ t & a \end{pmatrix}^* = \begin{pmatrix} (\top + 0a^*t)^* & (\top + 0a^*t)^*0a^* \\ (a + t\top^*0)^*t\top^* & (a + t\top^*0)^* \end{pmatrix} = \begin{pmatrix} \top^* & 0 \\ a^*t\top & a^* \end{pmatrix} = \begin{pmatrix} \top & 0 \\ a^*t & a^* \end{pmatrix} ,$$

hence $(t \Vdash a)^* = (\overline{a^*\overline{t}} \Vdash a^*)$.

A *(weak) omega algebra* [6, 22] is a structure $(S, {}^\omega)$ such that S is a (weak) Kleene algebra and the operation omega ${}^\omega$ satisfies the unfold and co-induction laws

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

for $a, b, c \in S$. Hence $a^\omega + a^*b$ is the greatest fixpoint of $\lambda x.ax + b$, denoted $\nu x.ax + b$. It follows that $a^\omega\top = a^\omega = a^*a^\omega$ and $c \le a \cdot c \Rightarrow c \le a^\omega$. The omega operation on prescriptions cannot be derived via the matrix construction since the greatest prescription is not the matrix with four $\top$ entries. Nevertheless, a direct argument can be used to show the following result. Let (S, T) be an ideal condition semiring such that S is an omega algebra, then $(\mathrm{NP}(S, T), +, \mathsf{fail}, \cdot, \mathsf{skip}, {}^*, {}^\omega)$ is a weak omega algebra, where $(t \Vdash a)^\omega = (\overline{a^\omega + a^*\overline{t}} \Vdash a^\omega)$.

2.4 Tests and domain

A *test semiring* [22] is an idempotent weak semiring $(S, +, 0, \cdot, 1)$ with a distinguished set of elements $\mathrm{test}(S) \subseteq S$ called *tests* and a *negation* operation $\neg$

such that $(\mathrm{test}(S), +, 0, \cdot, 1, \neg)$ is a Boolean algebra. By slightly generalising a proof of [15] we can show that any condition semiring $(S, T, +, 0, \cdot, 1, \sqcap, \top, \overline{})$ is a test semiring, where $\mathrm{test}(S, T) =_{\mathrm{def}} \{t \sqcap 1 \mid t \in T\}$ and $\neg p =_{\mathrm{def}} \overline{p\top} \sqcap 1$ for $p \in \mathrm{test}(S, T)$. Hence prescriptions form a test semiring with tests of the form

$$(\bar{t} \Vdash t) \sqcap (\top \Vdash 1) = \begin{pmatrix} \top & 0 \\ t & t \end{pmatrix} \sqcap \begin{pmatrix} \top & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \top & 0 \\ 0 & t \sqcap 1 \end{pmatrix} = (\top \Vdash t \sqcap 1) \,,$$

and negation $\neg(\top \Vdash t \sqcap 1) = (\top \Vdash \bar{t} \sqcap 1)$. This allows us to represent conditional statements by either $(t \sqcap a) + (\bar{t} \sqcap b)$ or $pa + \neg pb$, using either the condition t or its corresponding test $p = t \sqcap 1$. The use of conditions (or another set satisfying the ideal property) in the underlying semiring is necessary if prescriptions are to be represented by matrices; otherwise tests can be used for the termination information as in [24].

A *domain semiring* [8] is a structure $(S, {}^{\ulcorner})$ such that S is a test semiring and the domain operation ${}^{\ulcorner} : S \to \mathrm{test}(S)$ satisfies the axioms

$$a \le {}^{\ulcorner}a \cdot a \qquad\qquad {}^{\ulcorner}(p \cdot a) \le p \qquad\qquad {}^{\ulcorner}(a \cdot {}^{\ulcorner}b) \le {}^{\ulcorner}(a \cdot b)$$

for $a, b \in S$ and $p \in \mathrm{test}(S)$. Useful properties for $a, b \in S$ and $p \in \mathrm{test}(S)$ are

$$\begin{array}{llll} {}^{\ulcorner}a \le p \Leftrightarrow a \le pa & a \le b \Rightarrow {}^{\ulcorner}a \le {}^{\ulcorner}b & a = {}^{\ulcorner}aa & {}^{\ulcorner}p = p \\ a \le 0 \Leftrightarrow {}^{\ulcorner}a \le 0 & {}^{\ulcorner}(a + b) = {}^{\ulcorner}a + {}^{\ulcorner}b & {}^{\ulcorner}(pa) = p{}^{\ulcorner}a & {}^{\ulcorner}(a \cdot {}^{\ulcorner}b) = {}^{\ulcorner}(a \cdot b) \end{array}$$

If a greatest element $\top$ exists, another characterisation is ${}^{\ulcorner}a \le p \Leftrightarrow a \le p\top$ [1]. For prescriptions we obtain ${}^{\ulcorner}(t \Vdash a) = (\top \Vdash \neg{}^{\ulcorner}t + {}^{\ulcorner}a)$ this way. If the test semiring is induced from an ideal condition semiring as above, we even have ${}^{\ulcorner}a = a\top \sqcap 1$.

Domain induces the operations *diamond of a* given by $\langle a \rangle p =_{\mathrm{def}} {}^{\ulcorner}(ap)$ and its dual *box of a* given by $[a]p =_{\mathrm{def}} \neg\langle a \rangle \neg p$. For prescriptions they amount to $\langle t \Vdash a \rangle(\top \Vdash {}^{\ulcorner}u) = (\top \Vdash \neg{}^{\ulcorner}t + \langle a \rangle{}^{\ulcorner}u)$ and $[t \Vdash a](\top \Vdash {}^{\ulcorner}u) = (\top \Vdash {}^{\ulcorner}t \cdot [a]{}^{\ulcorner}u)$.

3 Towards axioms for general correctness

Kleene star and omega cannot be used directly to express the general correctness semantics of loops. This is due to the fact that star and omega are taken with respect to the natural order $\le$ that corresponds to the subset order used for partial and total correctness, but not to the Egli-Milner order.

For example, consider the endless loop while true do skip. Its partial correctness semantics is the least fixpoint $(\mu x.x) = 1^* \cdot 0 = 1 \cdot 0 = 0$. The total correctness semantics is the greatest fixpoint $(\nu x.x) = 1^\omega + 1^* \cdot 0 = 1^\omega = \top$. Instantiated to prescriptions, they are fail and chaos, respectively. However, the general correctness semantics is loop that lies properly between the least and the greatest fixpoints with respect to the natural order.

Another difference between partial, total and general correctness is observed about the term $\top \cdot 0$. For partial correctness, Kleene algebra is used where $\top \cdot 0 = 0$ (assuming $\top$ exists). For total correctness, this right annihilation axiom is dropped to obtain weak Kleene algebra, with the freedom to impose the left annihilation axiom $\top \cdot 0 = \top$ instead, as done by [26, 5, 15]. For general correctness, we have to drop this left annihilation axiom, too. This is easily observed from prescriptions, since the product of the greatest and the least prescription is

$$(0 \Vdash \top) \cdot (\top \Vdash 0) = \begin{pmatrix} \top & 0 \\ \top & \top \end{pmatrix} \cdot \begin{pmatrix} \top & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \top & 0 \\ \top & 0 \end{pmatrix} = (0 \Vdash 0) \ ,$$

which is neither the greatest nor the least prescription, but again loop. Since the term $\top \cdot 0$ cannot be simplified in weak Kleene or omega algebra, but is important as the intended least element of the Egli-Milner order, we call it $\mathsf{L} =_{\mathrm{def}} \top \cdot 0$.

In the following, we work towards axiomatising the structure that underlies prescriptions and their use in general correctness. We start by assuming a weak omega algebra and domain semiring S, since we have seen that prescriptions form one. Hence $\mathsf{L} = \top \cdot 0$ exists and already satisfies a number of properties.

Lemma 1. $\top\mathsf{L} = \mathsf{L}^\omega = \mathsf{L} \neq 1$ *and* $\mathsf{L}^* = 1{+}\mathsf{L}$. *Let* $x \in S$, *then* $x\mathsf{L} \leq {\ulcorner}x\mathsf{L} \leq \mathsf{L} = \mathsf{L}x$ *and* $x0 \leq {\ulcorner}(x0)\mathsf{L}$.

Proof. $x\mathsf{L} \leq \top\mathsf{L} = \top\top 0 = \top 0 = \mathsf{L}$, thus $x\mathsf{L} \leq {\ulcorner}xx\mathsf{L} \leq {\ulcorner}x\mathsf{L} \leq \mathsf{L}$, and $\mathsf{L}x = \top 0x = \top 0 = \mathsf{L}$. Hence $\mathsf{L}^* = 1 + \mathsf{L}\mathsf{L}^* = 1 + \mathsf{L}$ and $\mathsf{L}^\omega = \mathsf{L}\mathsf{L}^\omega = \mathsf{L}$. Assuming $\mathsf{L} = 1$ gives the contradiction $0 = 1 \cdot 0 = \mathsf{L} \cdot 0 = \mathsf{L} = 1$. Moreover, $x0 = x0\mathsf{L} \leq {\ulcorner}(x0)\mathsf{L}$. □

However, other properties which we expect to hold (since they hold for prescriptions) cannot be derived from the axioms of weak omega algebra. We therefore have to introduce further axioms.

$$\begin{array}{ll} x \leq \mathsf{L} \Rightarrow x \leq x0 & \qquad (\mathsf{L0}) \\ {\ulcorner}x\mathsf{L} \leq x\mathsf{L} & \qquad (\mathsf{L1}) \\ 1 \leq {\ulcorner}\mathsf{L} & \qquad (\mathsf{L2}) \end{array}$$

Axiom (L0) is provisional and follows from axioms presented below. Its consequent can equivalently be replaced by $x = x0$. Its backward implication holds by $x \leq x0 \leq \top 0 = \mathsf{L}$. The term $x0$ represents the states which may lead to non-termination. Axioms (L1) and (L2) can equivalently be strengthened to equalities. Consequences of these axioms are recorded in the next lemma.

Lemma 2. *Let* $x, y \in S$ *and* $p, q \in \mathrm{test}(S)$. *Axiom* (L0) *implies* $x \leq \mathsf{L} \Rightarrow x = xy$ *and* $\mathsf{L} \neq \top$ *and* $px0 \leq 0 \wedge pxq \leq \mathsf{L} \Rightarrow pxq \leq 0$ *and* $x0 = \inf\{x, \mathsf{L}\}$. *Axiom* (L2) *implies* ${\ulcorner}(x\mathsf{L}) = {\ulcorner}x$ *and* $\mathsf{L} \neq 0$. *Axioms* (L0) *and* (L2) *together are equivalent to* ${\ulcorner}\mathsf{L}x \leq \mathsf{L} \Rightarrow x = x0$. *Axiom* (L1) *implies* ${\ulcorner}(x0)\mathsf{L} \leq x$, *which is equivalent to* ${\ulcorner}(x0)\mathsf{L} = x0$ *and together with* (L2) *conversely implies* (L1).

Proof. For $x \leq \mathsf{L}$ we have $xy \leq x0y = x0 \leq x$ and $x \leq x0 \leq xy$ by (L0). Assuming $1 \leq \mathsf{L}$ gives the contradiction $1 \leq 1 \cdot 0 = 0$. Let $px0 \leq 0$ and $pxq \leq \mathsf{L}$, then $pxq \leq pxq0 = px0 \leq 0$. Let $z \leq x$ and $z \leq \mathsf{L}$, then $z \leq z0 \leq x0$ by (L0), and $x0$ is a lower bound of x and L since $x0 \leq x1 = x$ and $x0 \leq \top 0 = \mathsf{L}$.

${\ulcorner}(x\mathsf{L}) = {\ulcorner}(x{\ulcorner}\mathsf{L}) = {\ulcorner}(x1) = {\ulcorner}x$; assuming $\mathsf{L} = 0$ gives the contradiction $1 \leq {\ulcorner}0 = 0$.

Let $\ulcorner\mathsf{L}x \le \mathsf{L}$, then $x \le \mathsf{L}$ by ($\mathsf{L2}$), hence $x = x0$ by ($\mathsf{L0}$). Let $\ulcorner\mathsf{L}x \le \mathsf{L} \Rightarrow x = x0$ hold, then $x \le \mathsf{L}$ implies $\ulcorner\mathsf{L}x \le x \le \mathsf{L}$, hence $x = x0$, which shows ($\mathsf{L0}$). Moreover, $\ulcorner\mathsf{L}\neg\ulcorner\mathsf{L} = 0 \le \mathsf{L}$ implies $\neg\ulcorner\mathsf{L} = \neg\ulcorner\mathsf{L}0 = 0$, and hence ($\mathsf{L2}$).

$\ulcorner(x0)\mathsf{L} \le x0\mathsf{L} = x0 \le x$ by ($\mathsf{L1}$). This implies $x0 \le \ulcorner(x0)\mathsf{L} = \ulcorner(x0)\mathsf{L}0 \le x0$ by Lemma 1. Conversely, $\ulcorner x\mathsf{L} = \ulcorner(x\mathsf{L})\mathsf{L} = \ulcorner(x\mathsf{L}0)\mathsf{L} \le x\mathsf{L}$ by ($\mathsf{L2}$) and Lemma 1. □

Let us define the initial states of $x \in S$ from which infinite transition paths emerge as $\nabla x =_{\mathrm{def}} \ulcorner x^\omega$, and the 'convergent' states $\Delta x =_{\mathrm{def}} \neg\nabla x$. In presence of ($\mathsf{L1}$) and ($\mathsf{L2}$), this complies with the axiomatisation of ∇ given in [7]. To see this, observe that $\ulcorner x^\omega = \ulcorner(xx^\omega) = \langle x\rangle\ulcorner x^\omega$ by omega unfold, and $p \le \langle x\rangle p + q$ implies $p\mathsf{L} \le \ulcorner(xp)\mathsf{L} + q\mathsf{L} \le xp\mathsf{L} + q\mathsf{L}$ by ($\mathsf{L1}$), hence $p\mathsf{L} \le x^\omega + x^*q\mathsf{L}$ by omega co-induction, thus $p = \ulcorner(p\mathsf{L}) \le \ulcorner x^\omega + \langle x^*\rangle q$ by Lemma 2. Particular consequences are $\ulcorner(x^*0) \le \ulcorner(x^*x^\omega) = \ulcorner x^\omega = \nabla x$ and $x^\omega = \ulcorner x^\omega x^\omega = \nabla x x^\omega \le \nabla x\top$. By ($\mathsf{L1}$) we also obtain $\nabla x\mathsf{L} = \ulcorner x^\omega\mathsf{L} = x^\omega\mathsf{L} = x^\omega\top 0 = x^\omega 0$.

Another prescription that needs a representation is havoc. To this end, we introduce the element $\mathsf{H} \in S$ by the following axioms that relate L and H to represent programs as pairs of termination and state transition information.

$$x \le y + \mathsf{L} \wedge x \le y + \mathsf{H} \Rightarrow x \le y \qquad (\mathsf{H1})$$

$$x \le x0 + \mathsf{H} \qquad (\mathsf{H2})$$

Instantiating $y = x0$ in ($\mathsf{H1}$) gives $x \le x0 + \mathsf{L} \Rightarrow x \le x0$ by ($\mathsf{H2}$), which implies ($\mathsf{L0}$) immediately. Instantiating $x = \top$ in ($\mathsf{H2}$) gives $\top = \mathsf{L} + \mathsf{H}$. Instantiating $x = \mathsf{H}$ in ($\mathsf{H1}$) results in $\mathsf{H} \le y + \mathsf{L} \Rightarrow \mathsf{H} \le y$. Together we obtain $\top \le \mathsf{L} + y \Leftrightarrow \mathsf{H} \le y$, thus H is the least additive pseudo-complement of L. In particular, H is unique if it exists. An equivalent formulation of ($\mathsf{H1}$) is $x + \mathsf{L} = y + \mathsf{L} \wedge x + \mathsf{H} = y + \mathsf{H} \Rightarrow x = y$. In particular, we also obtain $x \le \mathsf{L} \wedge x \le \mathsf{H} \Rightarrow x = 0$.

Lemma 3. ($\mathsf{H1}$) *implies* $\mathsf{H}0 \le 0$ *and* ($\mathsf{H2}$) *implies* $x0 \le 0 \Rightarrow x \le \mathsf{H}$ *for* $x \in S$.

Proof. $\mathsf{H}0 \le \top 0 = \mathsf{L}$ and $\mathsf{H}0 \le \mathsf{H}1 = \mathsf{H}$, hence $\mathsf{H} = 0$ by ($\mathsf{H1}$). Let $x0 \le 0$, then $x \le x0 + \mathsf{H} \le \mathsf{H}$ by ($\mathsf{H2}$). □

The two conditions shown in the previous lemma are the axioms of [26] for havoc, but in a total correctness setting. Together, they are equivalent to $x0 \le 0 \Leftrightarrow x \le \mathsf{H}$, thus H is the greatest strict element. The next lemma records further consequences of our axioms.

Lemma 4. *Axiom* ($\mathsf{H2}$) *implies* $1 \le \mathsf{H} \le \mathsf{H}^2$ *and* $\top\mathsf{H} = \top = \mathsf{H}\top = \mathsf{H}^\omega$ *and* $\mathsf{HL} = \mathsf{L}$. *Axioms* ($\mathsf{H1}$) *and* ($\mathsf{H2}$) *together imply* $\mathsf{H}^* = \mathsf{H}^2 = \mathsf{H} \ne \mathsf{L}$. *Axioms* ($\mathsf{H1}$) *and* ($\mathsf{L2}$) *together imply* $\mathsf{H} \ne \top$.

Proof. $1 \le 1 \cdot 0 + \mathsf{H} = 0 + \mathsf{H} = \mathsf{H}$ by ($\mathsf{H2}$). Hence $\mathsf{H} \le \mathsf{H}^2$ and $\top \le \top\mathsf{H}$ and $\top \le \mathsf{H}\top$ by isotony, thus $\mathsf{HL} = \mathsf{H}\top\mathsf{L} = \top\mathsf{L} = \mathsf{L}$ by Lemma 1, and $\top \le \mathsf{H}^\omega$.

$\mathsf{H}^2 \le \mathsf{H}$ follows by Lemma 3 since $\mathsf{H}^2 0 \le \mathsf{H}0 \le 0$ by the same lemma using ($\mathsf{H2}$) and ($\mathsf{H1}$), respectively. Hence $1 + \mathsf{H}^2 \le \mathsf{H}$, which implies $\mathsf{H}^* \le \mathsf{H}$. Assuming $\mathsf{H} = \mathsf{L}$ gives the contradiction $1 \le \mathsf{H} = \mathsf{L} = \mathsf{L}0 = \mathsf{H}0 = 0$ by ($\mathsf{H2}$), Lemma 1 and Lemma 3 using ($\mathsf{H1}$).

Assuming $\mathsf{H} = \top$ gives the contradiction $0 \ne \mathsf{L} = \top 0 = \mathsf{H}0 = 0$ by Lemma 2 using ($\mathsf{L2}$) and Lemma 3 using ($\mathsf{H1}$). □

For prescriptions over relations we generally have $\mathsf{H} \neq 1$, but this cannot be proved from the axioms since the underlying semiring may be such that $1 = \top$ and hence havoc is skip (the relations ≤ 1 are an example).

We are now ready to define the Egli-Milner order $\sqsubseteq$ based on our axioms:

$$x \sqsubseteq y \Leftrightarrow_{\mathrm{def}} x \leq y + \mathsf{L} \wedge y \leq x + \ulcorner(x0)\mathsf{H} \ .$$

This definition is justified by the instance for prescriptions: We obtain the characterisation expected from [25, 24, 12] by calculating

$$\begin{aligned}
&(t \Vdash a) \sqsubseteq (u \Vdash b) \\
\Leftrightarrow\ &(t \Vdash a) \leq (u \Vdash b) + (0 \Vdash 0) \wedge (u \Vdash b) \leq (t \Vdash a) + \ulcorner((t \Vdash a)(\top \Vdash 0))(\top \Vdash \top) \\
\Leftrightarrow\ &(t \Vdash a) \leq (0 \Vdash b) \wedge (u \Vdash b) \leq (t \Vdash a + \overline{t}) \\
\Leftrightarrow\ &a \leq b \wedge t \leq u \wedge b \leq a + \overline{t} \ ,
\end{aligned}$$

since $(u \Vdash b) + (0 \Vdash 0) = (u \sqcap 0 \Vdash b + 0) = (0 \Vdash b)$ and

$$\begin{aligned}
&(t \Vdash a) + \ulcorner((t \Vdash a)(\top \Vdash 0))(\top \Vdash \top) = (t \Vdash a) + \ulcorner(t \sqcap \overline{a0} \Vdash a0)(\top \Vdash \top) \\
&= (t \Vdash a) + \ulcorner(t \Vdash 0)(\top \Vdash \top) = (t \Vdash a) + (\top \Vdash \neg\ulcorner t)(\top \Vdash \top) \\
&= (t \Vdash a) + (\top \Vdash \neg\ulcorner t\top) = (t \Vdash a + \overline{t}) \ ,
\end{aligned}$$

since $\neg\ulcorner t\top = (\overline{\ulcorner t\top} \sqcap 1)\top = \overline{\ulcorner t\top} = \overline{(t\top \sqcap 1)\top} = \overline{t\top} = \overline{t}$. The following lemma shows basic properties of $\sqsubseteq$.

Lemma 5. *Axiom* (H1) *implies that* $\sqsubseteq$ *is a partial order. Axioms* (L2) *and* (H2) *together imply that* L *is its least element. Axioms* (H1) *and* (H2) *together imply that* $\sqsubseteq$ *has no greatest element.*

Proof. Reflexivity follows immediately. For transitivity, let $x \sqsubseteq y$ and $y \sqsubseteq z$. Then $x \leq y + \mathsf{L}$ and $y \leq z + \mathsf{L}$, which implies $x \leq z + \mathsf{L} + \mathsf{L} = z + \mathsf{L}$. Moreover $y \leq x + \ulcorner(x0)\mathsf{H}$ and $z \leq y + \ulcorner(y0)\mathsf{H}$, hence

$$z \leq x + \ulcorner(x0)\mathsf{H} + \ulcorner((x + \ulcorner(x0)\mathsf{H})0)\mathsf{H} = x + \ulcorner(x0)\mathsf{H} + \ulcorner(\ulcorner(x0)\mathsf{H}0)\mathsf{H} = x + \ulcorner(x0)\mathsf{H}$$

by Lemma 3. Together we have $x \sqsubseteq z$. For antisymmetry, let $x \sqsubseteq y$ and $y \sqsubseteq x$. Then $x \leq y + \mathsf{L}$ and $y \leq x + \ulcorner(x0)\mathsf{H} \leq x + \mathsf{H}$ and $y \leq x + \mathsf{L}$ and $x \leq y + \ulcorner(y0)\mathsf{H} \leq y + \mathsf{H}$. Hence $x \leq y$ and $y \leq x$ by (H1).

For any $x \in S$ we have $x \leq \top = \mathsf{L} + \mathsf{H} = \mathsf{L} + \ulcorner\mathsf{L}\mathsf{H} = \mathsf{L} + \ulcorner(\mathsf{L}0)\mathsf{H}$ by (H2), (L2) and Lemma 1. With $\mathsf{L} \leq x + \mathsf{L}$ we obtain $\mathsf{L} \sqsubseteq x$.

Assume that $0 \sqsubseteq x$ and $1 \sqsubseteq x$, then $x \leq 0 + \ulcorner(0 \cdot 0)\mathsf{H} = \ulcorner 0\mathsf{H} = 0\mathsf{H} = 0$, and therefore $1 \leq x + \mathsf{L} \leq \mathsf{L}$. Since $1 \leq \mathsf{H}$ by Lemma 4, we obtain the contradiction $1 \leq 0$ by (H1). □

It can furthermore be shown that $\cdot$ and $+$ are isotone with respect to $\sqsubseteq$. We have thus derived a number of useful properties from our axioms. In the remainder of this paper we assume that (L1), (L2), (H1) and (H2) hold in S.

Least fixpoints with respect to the Egli-Milner order, denoted by ξ, are used to define the general correctness semantics of recursion. In particular, the semantics of loops is while p do $a =_{\mathrm{def}} \xi x.pax + \neg p$.

Theorem 6. *Let $p \in \mathrm{test}(S)$ and $a \in S$, then* $\mathsf{while}\ p\ \mathsf{do}\ a = \nabla(pa)\mathsf{L} + (pa)^*\neg p$.

A direct proof can be given using Lemmas 1 and 2. It is omitted since the result follows from our treatment of full recursion in Section 6.

4 General correctness

Consider a domain semiring D, an element $a \in D$ and two tests $p, q \in \mathrm{test}(D)$. Soundness of the Hoare triple $p\,\{a\}\,q$ is defined by [24] as $p \leq [a]q$, which is equivalent to $pa\neg q \leq 0$ [21]. This claims partial correctness: When started in a state satisfying p, the program a will not lead to a state satisfying $\neg q$. Thus $[a]q$ is the weakest liberal precondition of statement a and postcondition q.

The remarkable observation of [24] is that the *same* triple claims total correctness if it is interpreted in an appropriate semiring. In particular, $[a]q$ then is the weakest precondition of statement a and postcondition q. This is beneficial, since statements proved in general domain semirings automatically hold in both interpretations. For example, a calculus for weakest liberal preconditions in domain semirings yields one for weakest preconditions.

An appropriate semiring to interpret the Hoare triple is given by prescriptions. Let us verify that the Hoare triple indeed yields a total correctness claim:

$$\begin{aligned}&(\top \Vdash p)(t \Vdash a)\neg(\top \Vdash q) = (\overline{p\bar{t}} \Vdash pa)(\top \Vdash \neg q) = (\overline{p\bar{t}} \Vdash pa\neg q) \leq (\top \Vdash 0)\\ \Leftrightarrow\ & p\bar{t} \leq 0 \wedge pa\neg q \leq 0\ .\end{aligned}$$

Hence the termination claim $p\bar{t} \leq 0$ is a part of the Hoare triple. It is equivalent to $p \leq {\ulcorner}t$ and expresses that the starting state must be one in which the execution of $(t \Vdash a)$ is guaranteed to terminate.

Such a claim is characteristic of total correctness. Actually, the same claim is obtained for the Hoare triple interpreted in the semiring of designs [15]. Working with designs would then have the additional advantage of not having to deal with the Egli-Milner order. Instead, the semantics of recursion uses the simpler natural order of the semiring.

Another conclusion is that the Hoare triple does not express general correctness adequately. To derive a more suitable correctness claim, we again look at the concrete instance of prescriptions. The two occurrences of the precondition p in the claim above have to be separated as in $r\bar{t} \leq 0 \wedge pa\neg q \leq 0$. Now r describes the initial states from where termination has to be guaranteed, and p describes the initial states which do not lead to states satisfying $\neg q$. Partial correctness is recovered by choosing $r = 0$ and total correctness by $r = p$, but we can now make full use of the 'generality' provided by general correctness to distinguish claims about terminating and non-terminating executions.

For prescriptions we observe that the first condition is obtained by

$$(\top \Vdash r)(t \Vdash a)(\top \Vdash 0) = (\overline{r\bar{t}} \Vdash ra)(\top \Vdash 0) = (\overline{r\bar{t}} \Vdash 0) \leq (\top \Vdash 0) \Leftrightarrow r\bar{t} \leq 0\ ,$$

and the second by

$$(\top \Vdash p)(t \Vdash a)\neg(\top \Vdash q) = (\overline{p\bar{t}} \Vdash pa\neg q) \leq (0 \Vdash 0) \Leftrightarrow pa\neg q \leq 0\ .$$

Generalised to our axiomatic framework of Section 3, we thus obtain the general correctness statement

$$ra0 \leq 0 \wedge pa\neg q \leq \mathsf{L} \ .$$

A notation analogous to Hoare triples would be a quadruple containing the program a, the termination precondition r, the precondition p and the postcondition q. We rather observe that the first claim $ra0 \leq 0$ is equivalent to the Hoare triple $r\,\{a\}\,1$, which can be derived using existing Hoare calculi except for constructs based on L or H. For these we can derive $0\,\{a\}\,1$ and $a \leq \mathsf{H} \Rightarrow r\,\{a\}\,1$ for any $a \in S$ and $r \in \mathrm{test}(S)$, thus in particular $0\,\{\mathsf{L}\}\,1$ and $1\,\{\mathsf{H}\}\,1$. For the while loop we calculate using Theorem 6

$$[\mathsf{while}\ p\ \mathsf{do}\ a]1 = \neg\ulcorner((\nabla(pa)\mathsf{L} + (pa)^*\neg p)0) = \neg(\ulcorner(\nabla(pa)\mathsf{L}) + \ulcorner((pa)^*0)) = \neg\nabla(pa)$$

to obtain the triple $\Delta(pa)\,\{\mathsf{while}\ p\ \mathsf{do}\ a\}\,1$.

New rules are, however, necessary for the second claim $pa\neg q \leq \mathsf{L}$, which we denote by $p \llparenthesis a \rrparenthesis q$ since it amounts to 'weak correctness' of [26]. To see this, we show $pa\neg q \leq \mathsf{L} \Leftrightarrow pa = paq$. The forward implication follows since $pa\neg q \leq \mathsf{L}$ implies $pa\neg q = pa0$ by ($\mathsf{L0}$), hence $pa = paq + pa\neg q = paq + pa0 = paq$. The backward implication follows since $pa\neg q = paq\neg q = pa0 \leq \top 0 = \mathsf{L}$. The rules for weak correctness are provided by the following theorem.

Theorem 7. *Let $a, b \in S$ and $p, q, r \in \mathrm{test}(S)$. Then*

$$\begin{array}{ll}
p \llparenthesis 0 \rrparenthesis q \qquad p \llparenthesis \mathsf{L} \rrparenthesis q \qquad q \llparenthesis 1 \rrparenthesis q & pr \llparenthesis 1 \rrparenthesis q \Rightarrow p \llparenthesis r \rrparenthesis q \\
p \llparenthesis a \rrparenthesis q \wedge p \llparenthesis b \rrparenthesis q \Rightarrow p \llparenthesis a + b \rrparenthesis q & p \llparenthesis a \rrparenthesis q \wedge q \llparenthesis b \rrparenthesis r \Rightarrow p \llparenthesis ab \rrparenthesis r \\
rp \llparenthesis a \rrparenthesis q \wedge \neg rp \llparenthesis b \rrparenthesis q \Rightarrow p \llparenthesis ra + \neg rb \rrparenthesis q & pq \llparenthesis a \rrparenthesis q \Rightarrow q \llparenthesis \mathsf{while}\ p\ \mathsf{do}\ a \rrparenthesis \neg pq
\end{array}$$

Proof. $p0\neg q = 0 \leq \mathsf{L}$ and $p\mathsf{L}\neg q \leq \mathsf{L}$ and $q1\neg q = 0 \leq \mathsf{L}$. The rule for tests is immediate and the rule for choice follows by $p(a+b)\neg q = pa\neg q + pb\neg q \leq \mathsf{L}$ from its premises. Composition is calculated as

$$pa\neg q \leq \mathsf{L} \wedge qb\neg r \leq \mathsf{L} \Rightarrow pab\neg r = paqb\neg r + pa\neg qb\neg r \leq pa\mathsf{L} + \mathsf{L}b\neg r \leq \mathsf{L}$$

by Lemma 1. A consequence of the rules for 1 and tests is $p \llparenthesis q \rrparenthesis pq$. Using this and the rules for composition and choice we obtain the rule for the conditional.

To obtain the rule for the while loop, we first derive $q \llparenthesis a \rrparenthesis q \Rightarrow q \llparenthesis a^* \rrparenthesis q$. Assume $qa\neg q \leq \mathsf{L}$, then

$$q + (\mathsf{L} + qa^*q)a = qq + \mathsf{L}a + qa^*qaq + qa^*qa\neg q \leq qa^*q + \mathsf{L} + qa^*\mathsf{L} \leq \mathsf{L} + qa^*q$$

by Lemma 1, hence $qa^* \leq \mathsf{L} + qa^*q$ by star induction, thus

$$qa^*\neg q \leq \mathsf{L}\neg q + qa^*q\neg q = \top 0 + qa^*0 = \top 0 = \mathsf{L} \ .$$

Second, we derive $pq \llparenthesis a \rrparenthesis q \Rightarrow q \llparenthesis (pa)^*\neg p \rrparenthesis \neg pq$. This follows by the composition rule, since $q \llparenthesis p \rrparenthesis pq \Rightarrow q \llparenthesis pa \rrparenthesis q \Rightarrow q \llparenthesis (pa)^* \rrparenthesis q$ and $q \llparenthesis \neg p \rrparenthesis \neg pq$. Third, we have $q \llparenthesis \nabla(pa)\mathsf{L} \rrparenthesis \neg pq$ by the rules for L and composition, since $q \llparenthesis \nabla(pa) \rrparenthesis q\nabla(pa)$ holds. Apply the choice rule to these claims and Theorem 6. $\square$

5 Pre-post specifications

Complementary to the verification approach using correctness claims that can be derived through a calculus is the transformation approach, where specifications are refined into implementations. Specifications given by pre- and postconditions are well-known in total correctness and treated algebraically in [26]. In this section we propose specifications suitable for general correctness refinement.

Our specification $(r \,|\, p \leadsto q)$ consists of three components. One of them is new: The termination precondition r describes the initial states from which execution must terminate. The other two are as usual: If the precondition p holds in the initial state, the postcondition q must be established. We axiomatise the specification as the greatest element of S satisfying our general correctness claim of Section 4 for tests $r, p, q \in \mathrm{test}(S)$:

$$
\begin{aligned}
& r(r \,|\, p \leadsto q)0 = 0 && (\mathsf{G1})\\
& p(r \,|\, p \leadsto q)\neg q \le \mathsf{L} && (\mathsf{G2})\\
& rx0 = 0 \wedge px\neg q \le \mathsf{L} \Rightarrow x \le (r \,|\, p \leadsto q) && (\mathsf{G3})
\end{aligned}
$$

The greatest element leaves the greatest amount of freedom in implementation, since $x \le y$ means that x refines y. The conjunction of $(\mathsf{G1})$, $(\mathsf{G2})$ and $(\mathsf{G3})$ can equivalently be stated as $rx0 = 0 \wedge px\neg q \le \mathsf{L} \Leftrightarrow x \le (r \,|\, p \leadsto q)$, thus the specification is unique if it exists. These axioms are stated to show the intention, but in our algebra of Section 3 we can give an explicit characterisation.

Theorem 8. *Let $p, q, r \in \mathrm{test}(S)$. Then $(r \,|\, p \leadsto q) = \neg r\mathsf{L} + \neg p\mathsf{H} + \mathsf{H}q$.*

Proof. To show that $\neg r\mathsf{L} + \neg p\mathsf{H} + \mathsf{H}q$ satisfies $(\mathsf{G1})$ and $(\mathsf{G2})$, we calculate

$$
\begin{aligned}
r(\neg r\mathsf{L} + \neg p\mathsf{H} + \mathsf{H}q)0 &= r\neg r\mathsf{L}0 + r\neg p\mathsf{H}0 + r\mathsf{H}q0 = 0 + r\neg p0 + r\mathsf{H}0 = 0\\
p(\neg r\mathsf{L} + \neg p\mathsf{H} + \mathsf{H}q)\neg q &= p\neg r\mathsf{L}\neg q + p\neg p\mathsf{H}\neg q + p\mathsf{H}q\neg q \le \mathsf{L} + 0 + \mathsf{H}0 = \mathsf{L}
\end{aligned}
$$

by Lemma 3. For $(\mathsf{G3})$, let $rx0 = 0$ and $px\neg q \le \mathsf{L}$. Then $rx \le \mathsf{H}$ by Lemma 3 and $px = pxq$ as shown in Section 4. Therefore $x \le \neg r\mathsf{L} + \neg p\mathsf{H} + \mathsf{H}q$ follows from the cases

$$
\begin{aligned}
prxq &\le rxq \le \mathsf{H}q & prx\neg q &= prxq\neg q \le p\mathsf{H}0 = p0 = 0\\
p\neg rx\neg q &\le \neg r\mathsf{L} & p\neg rxq &\le \neg r\top q = \neg r\mathsf{L}q + \neg r\mathsf{H}q \le \neg r\mathsf{L} + \mathsf{H}q\\
\neg prx &\le \neg p\mathsf{H} & \neg p\neg rx &\le \neg p\neg r\top = \neg p\neg r\mathsf{L} + \neg p\neg r\mathsf{H} \le \neg r\mathsf{L} + \neg p\mathsf{H}
\end{aligned}
$$

which hold by Lemma 3. □

Thus the total correctness pre-post specification $[p, q]$ of [26] can be recovered as $(p \,|\, p \leadsto q)$, where both preconditions coincide. This again characterises general correctness by its separated treatment of the termination precondition. Furthermore, we can recover the special elements $0 = (1 \,|\, 1 \leadsto 0)$, $\top = (0 \,|\, 0 \leadsto 0)$, $\mathsf{L} = (0 \,|\, 1 \leadsto 0)$ and $\mathsf{H} = (1 \,|\, 1 \leadsto 1)$. The representation in these terms is not necessarily unique: For example, $\top = (0 \,|\, 1 \leadsto 1)$ also holds. The following two corollaries establish basic properties of our specification elements.

Corollary 9. $(r_1 \,|\, p_1 \leadsto q_1) + (r_2 \,|\, p_2 \leadsto q_2) = (r_1 r_2 \,|\, p_1 p_2 \leadsto q_1 + q_2)$. *Hence* $(\cdot \,|\, \cdot \leadsto \cdot)$ *is antitone in its first and second arguments, and isotone in its third. Moreover,* $q_1 \leq r_2 p_2$ *implies* $(r_1 \,|\, p_1 \leadsto q_1) \cdot (r_2 \,|\, p_2 \leadsto q_2) \leq (r_1 p_1 \,|\, p_1 \leadsto q_2)$.

Proof. Let $q_1 \leq r_2 p_2$, then

$$\begin{aligned}
&(r_1 \,|\, p_1 \leadsto q_1) \cdot (r_2 \,|\, p_2 \leadsto q_2) \\
&= (\neg r_1 \mathsf{L} + \neg p_1 \mathsf{H} + \mathsf{H} q_1) \cdot (\neg r_2 \mathsf{L} + \neg p_2 \mathsf{H} + \mathsf{H} q_2) \\
&\leq \neg r_1 \mathsf{L} + \neg p_1 \mathsf{H} \mathsf{L} + \neg p_1 \mathsf{H} \mathsf{H} + \mathsf{H} q_1 \neg r_2 \mathsf{L} + \mathsf{H} q_1 \neg p_2 \mathsf{H} + \mathsf{H} \mathsf{H} q_2 \\
&= \neg r_1 \mathsf{L} + \neg p_1 \mathsf{L} + \neg p_1 \mathsf{H} + \mathsf{H} 0 + \mathsf{H} 0 + \mathsf{H} q_2 \\
&= \neg (r_1 p_1) \mathsf{L} + \neg p_1 \mathsf{H} + \mathsf{H} q_2 \\
&= (r_1 p_1 \,|\, p_1 \leadsto q_2)
\end{aligned}$$

by Theorem 8 and Lemmas 1, 3 and 4. The other claims are proved similarly. □

For prescriptions, we obtain $((\top \Vdash r) \,|\, (\top \Vdash p) \leadsto (\top \Vdash q)) = (r\top \Vdash \overline{p\top} + \top q)$. Let us furthermore mention the interpretation of $(r \,|\, p \leadsto p)$ for $r \in \{0, p, 1\}$. We call such a specification an 'invariant' since it guarantees that p holds after the execution if it holds before. If $r = 0$ or $r = 1$ or $r = p$, termination is not guaranteed or always guaranteed or guaranteed if p holds, respectively.

Corollary 10. $1 \leq (r \,|\, p \leadsto p) = (r \,|\, p \leadsto p)^2$ *for* $p \in \mathrm{test}(S)$ *and* $r \in \{0, p, 1\}$.

Proof. $1 = \neg p + p \leq \neg p \mathsf{H} + \mathsf{H} p \leq (r \,|\, p \leadsto p)$ by Lemma 4 and Theorem 8. Thus,

$$(\neg p \mathsf{H} + \mathsf{H} p) \cdot (\neg p \mathsf{H} + \mathsf{H} p) \leq \neg p \mathsf{H}^2 + \mathsf{H} 0 + \mathsf{H}^2 p = \neg p \mathsf{H} + \mathsf{H} p \leq (\neg p \mathsf{H} + \mathsf{H} p)^2$$

by Lemmas 3 and 4. Moreover, $(\neg p \mathsf{H} + \mathsf{H} p) \neg r \mathsf{L} \leq \neg r \mathsf{L}$ by Lemma 1 if $r = 0$, by Lemma 3 if $r = 1$, and by both lemmas if $r = p$. Therefore,

$$\begin{aligned}
&(r \,|\, p \leadsto p)^2 = (\neg r \mathsf{L} + \neg p \mathsf{H} + \mathsf{H} p) \cdot (\neg r \mathsf{L} + \neg p \mathsf{H} + \mathsf{H} p) \\
&= \neg r \mathsf{L} + (\neg p \mathsf{H} + \mathsf{H} p) \neg r \mathsf{L} + (\neg p \mathsf{H} + \mathsf{H} p)^2 = \neg r \mathsf{L} + \neg p \mathsf{H} + \mathsf{H} p = (r \,|\, p \leadsto p)
\end{aligned}$$

by Theorem 8 and Lemma 1. □

The characterisation $rx0 = 0 \wedge px = pxq \Leftrightarrow x \leq (r \,|\, p \leadsto q)$ can be used to axiomatise our general correctness pre-post specifications without the use of L and H which can be added by defining them as particular specifications. While a number of properties, such as those shown in Lemmas 1 and 3, follow from this axiomatisation, the axioms ($\mathsf{L0}$), ($\mathsf{L1}$), ($\mathsf{L2}$), ($\mathsf{H1}$) and ($\mathsf{H2}$) cannot be derived.

We can now use the specifications to algebraically state and prove a loop introduction rule for general correctness semantics given by [12]. Note the use of the invariant $(0 \,|\, q \leadsto q)$.

Theorem 11. *Let* $a \in S$ *and* $p, q, r \in \mathrm{test}(S)$ *such that* $pa \leq (0 \,|\, q \leadsto q)$ *and* $r \leq \Delta(pa)$. *Then* $\mathsf{while}\ p\ \mathsf{do}\ a \leq (r \,|\, q \leadsto q \neg p)$.

Proof. By ($\mathsf{G3}$) it remains to show $r \,\{\mathsf{while}\ p\ \mathsf{do}\ a\}\, 1$ and $q \,\llparenthesis \mathsf{while}\ p\ \mathsf{do}\ a \rrparenthesis\, q \neg p$. The first claim is immediate from $r \leq \Delta(pa)$ and $\Delta(pa) \,\{\mathsf{while}\ p\ \mathsf{do}\ a\}\, 1$ derived in Section 4. The second claim follows by Theorem 7 from $pq \,\llparenthesis a \rrparenthesis\, q$, which holds since $qpa \neg q \leq q(0 \,|\, q \leadsto q) \neg q \leq \mathsf{L}$ by the assumption and ($\mathsf{G2}$). □

6 Recursion

In this section we generalise from loops to full recursion, an open issue of [24]. In particular, we show how to calculate least fixpoints with respect to the Egli-Milner order from fixpoints with respect to the natural order.

Throughout this section let $f : S \to S$ be isotone with respect to $\leq$ and $\sqsubseteq$, and assume that the least fixpoint μf and the greatest fixpoint νf of f with respect to $\leq$ exist. The least fixpoint of f with respect to $\sqsubseteq$ is denoted by ξf.

Theorem 12. *Let $x \in S$, then $x = \xi f \Leftrightarrow \mu f \leq x \leq \nu f \wedge x \sqsubseteq \mu f \wedge x \sqsubseteq \nu f$.*

Proof. The forward implication is immediate since ξf is the least fixpoint with respect to $\sqsubseteq$. For the backward implication, let $\mu f \leq x \leq \nu f \wedge x \sqsubseteq \mu f \wedge x \sqsubseteq \nu f$. By isotony of f we obtain $\mu f = f(\mu f) \leq f(x) \leq f(\nu f) = \nu f$ and $f(x) \sqsubseteq f(\mu f) = \mu f$ and $f(x) \sqsubseteq f(\nu f) = \nu f$. From these facts and the assumptions we obtain:

- $x \sqsubseteq f(x)$ since $x \leq \mu f + \mathsf{L} \leq f(x) + \mathsf{L}$ and $f(x) \leq \nu f \leq x + {}^\ulcorner(x0)\mathsf{H}$.
- $f(x) \sqsubseteq x$ since $f(x) \leq \mu f + \mathsf{L} \leq x + \mathsf{L}$ and $x \leq \nu f \leq f(x) + {}^\ulcorner(f(x)0)\mathsf{H}$.

Hence $x = f(x)$ by Lemma 5. Let $y \in S$ such that $y = f(y)$, hence $\mu f \leq y \leq \nu f$. Then $x \sqsubseteq y$ since $x \leq \mu f + \mathsf{L} \leq y + \mathsf{L}$ and $y \leq \nu f \leq x + {}^\ulcorner(x0)\mathsf{H}$. □

As a consequence, we can give an explicit formula for ξf.

Corollary 13. *Assume ξf exists. Then $x = \xi f \Leftrightarrow x + \mathsf{L} = \mu f + \mathsf{L} \wedge x + \mathsf{H} = \nu f + \mathsf{H}$ and $\nu f \leq \mu f + {}^\ulcorner(\nu f 0)\mathsf{H} + \mathsf{L}$ and $\xi f = \nu f 0 + \mu f$.*

Proof. By Theorem 12 we obtain $\xi f \leq \mu f + \mathsf{L}$ and $\nu f \leq \xi f + {}^\ulcorner(\xi f 0)\mathsf{H} \leq \xi f + \mathsf{H}$, hence $\nu f \leq \mu f + \mathsf{L} + {}^\ulcorner(\nu f 0)\mathsf{H}$ using $\xi f \leq \nu f$. Let $x + \mathsf{L} = \mu f + \mathsf{L}$ and $x + \mathsf{H} = \nu f + \mathsf{H}$.

- $\mu f \leq x$ since $\mu f \leq x + \mathsf{L}$ and $\mu f \leq \nu f \leq x + \mathsf{H}$.
- $x \leq \nu f$ since $x \leq \nu f + \mathsf{H}$ and $x \leq \mu f + \mathsf{L} \leq \nu f + \mathsf{L}$.
- $\nu f \leq x + {}^\ulcorner(x0)\mathsf{H} + \mathsf{H}$, and $\nu f \leq x + {}^\ulcorner(x0)\mathsf{H} + \mathsf{L}$ since $\nu f 0 \leq (x + \mathsf{H})0 = x0$.

Hence $\mu f \leq \nu f \leq x + {}^\ulcorner(x0)\mathsf{H}$, yielding $x \sqsubseteq \mu f$ and $x \sqsubseteq \nu f$. The first claim follows by Theorem 12. It implies the third claim since $\nu f 0 + \mu f + \mathsf{L} = \mu f + \nu f 0 + \top 0 = \mu f + \top 0 = \mu f + \mathsf{L}$ and $\nu f + \mathsf{H} \leq \nu f 0 + \mathsf{H} \leq \nu f 0 + \mu f + \mathsf{H} \leq \nu f + \mathsf{H}$ by ($\mathsf{H2}$). □

Inspection of the proof reveals that ξf exists $\Leftrightarrow$ $\nu f \leq \mu f + {}^\ulcorner(\nu f 0)\mathsf{H} + \mathsf{L}$. In particular, we prove Theorem 6 by letting $f(x) = pax + q$. Then

$$\nu f = (pa)^\omega + (pa)^* q \leq \nabla(pa)\top + \mu f \leq \mu f + \nabla(pa)\mathsf{H} + \mathsf{L} = \mu f + {}^\ulcorner(\nu f 0)\mathsf{H} + \mathsf{L} \ ,$$

since ${}^\ulcorner(\nu f 0) = {}^\ulcorner((pa)^\omega 0 + (pa)^* q0) = \nabla(pa) + {}^\ulcorner((pa)^* 0) = \nabla(pa)$, and the least fixpoint is $\xi f = \nu f 0 + \mu f = (pa)^\omega 0 + (pa)^* q0 + (pa)^* q = \nabla(pa)\mathsf{L} + (pa)^* q$.

We have thus established $\nu f 0 + \mu f$ as the appropriate solution to recursion in general correctness. The same term is appropriate also in partial correctness, where $\nu f 0 = 0$ vanishes. It is not appropriate in total correctness, however, since it is not equal to νf in general.

Let us finally consider the instance of prescriptions again.

Corollary 14. *Assume that ξf exists and $\mu f = (t \Vdash a)$ and $\nu f = (u \Vdash b)$. Then $u \sqcap a = u \sqcap b$ and $\xi f = (u \Vdash a)$.*

Proof. We have $u \leq t$ since $\mu f \leq \nu f$, hence $\xi f = (u \Vdash b)(\top \Vdash 0) + (t \Vdash a) = (u \Vdash 0) + (t \Vdash a) = (u \sqcap t \Vdash a) = (u \Vdash a)$ by Corollary 13. The remaining claim follows since $(u \Vdash a) \sqsubseteq (u \Vdash b)$ is equivalent to $a \leq b \wedge b \leq a + \overline{u}$. □

A calculation shows that ξf exists $\Leftrightarrow b \leq a + \overline{u}$. It thus remains to calculate the least and greatest fixpoints for prescriptions. This can be done by the following result similar to those of [17, 15] for total correctness. We omit its proof.

Proposition 15. *Let $H(t \Vdash a) = F(t \Vdash a) \Vdash G(t \Vdash a)$ be isotone with respect to $\leq$. Then $\nu H = (P_\nu(Q_\nu) \Vdash Q_\nu)$ and $\mu H = (P_\mu(Q_\mu) \Vdash Q_\mu)$, where*

$$\begin{array}{lll} P_\nu(a) = \mu t.F(t \Vdash a) & R_\nu(a) = G(P_\nu(a) \Vdash a) & Q_\nu = \nu R_\nu \\ P_\mu(a) = \nu t.F(t \Vdash a) & R_\mu(a) = G(P_\mu(a) \Vdash a) & Q_\mu = \mu R_\mu \end{array}$$

7 Conclusion

Our work shows how to treat general correctness algebraically, despite its additional complexity caused by the Egli-Milner order and the finer termination information. We have thus extended the algebraic approach already available for partial and total correctness semantics.

Future work shall further investigate the calculus and refinement, and provide operators particularly suitable for general correctness, such as the 'concert' operator of [12]. Further applications arise in the area of hybrid systems [18]. We also observe that the assumption of a weak omega algebra in Sections 3–6 is only essential for $\top$ and the results concerning while loops.

Acknowledgement. I thank the anonymous referees for their valuable remarks and helpful suggestions.

References

1. C. J. Aarts. Galois connections presented calculationally. Master's thesis, Department of Mathematics and Computing Science, Eindhoven University of Technology, 1992.
2. J. W. de Bakker. Semantics and termination of nondeterministic recursive programs. In S. Michaelson and R. Milner, editors, *Automata, Languages and Programming: Third International Colloquium*, pages 435–477. Edinburgh University Press, 1976.
3. R. Berghammer and H. Zierer. Relational algebraic semantics of deterministic and nondeterministic programs. *Theoretical Computer Science*, 43:123–147, 1986.
4. M. Broy, R. Gnatz, and M. Wirsing. Semantics of nondeterministic and noncontinuous constructs. In F. L. Bauer and M. Broy, editors, *Program Construction*, volume 69 of *LNCS*, pages 553–592. Springer-Verlag, 1979.

5. J.-L. De Carufel and J. Desharnais. Demonic algebra with domain. In R. Schmidt, editor, *Relations and Kleene Algebra in Computer Science*, volume 4136 of *LNCS*, pages 120–134. Springer-Verlag, 2006.
6. E. Cohen. Separation and reduction. In R. Backhouse and J. N. Oliveira, editors, *Mathematics of Program Construction*, volume 1837 of *LNCS*, pages 45–59. Springer-Verlag, 2000.
7. J. Desharnais, B. Möller, and G. Struth. Algebraic notions of termination. Report 2006-23, Institut für Informatik, Universität Augsburg, October 2006.
8. J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM Transactions on Computational Logic*, 7(4):798–833, October 2006.
9. E. W. Dijkstra. *A Discipline of Programming.* Prentice Hall, 1976.
10. S. Dunne. Recasting Hoare and He's Unifying Theory of Programs in the context of general correctness. In A. Butterfield, G. Strong, and C. Pahl, editors, *5th Irish Workshop on Formal Methods*, Electronic Workshops in Computing. The British Computer Society, July 2001.
11. S. Dunne and A. Galloway. Lifting general correctness into partial correctness is *ok*. In J. Davies and J. Gibbons, editors, *Integrated Formal Methods*, volume 4591 of *LNCS*, pages 215–232. Springer-Verlag, 2007.
12. S. Dunne, I. Hayes, and A. Galloway. Reasoning about loops in total and general correctness. In A. Butterfield, editor, *Second International Symposium on the Unifying Theories of Programming*, LNCS. Springer-Verlag, to appear.
13. Z. Ésik and H. Leiß. Algebraically complete semirings and Greibach normal form. *Annals of Pure and Applied Logic*, 3(1–3):173–203, May 2005.
14. W. Guttmann and B. Möller. Modal design algebra. In S. Dunne and W. Stoddart, editors, *Unifying Theories of Programming*, volume 4010 of *LNCS*, pages 236–256. Springer-Verlag, 2006.
15. W. Guttmann and B. Möller. Normal design algebra. *Journal of Logic and Algebraic Programming*, to appear.
16. C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580/583, October 1969.
17. C. A. R. Hoare and J. He. *Unifying theories of programming.* Prentice Hall Europe, 1998.
18. P. Höfner and B. Möller. An algebra of hybrid systems. *Journal of Logic and Algebraic Programming*, 78(2):74–97, January 2009.
19. D. Jacobs and D. Gries. General correctness: A unification of partial and total correctness. *Acta Informatica*, 22(1):67–83, April 1985.
20. D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, May 1994.
21. D. Kozen. On Hoare logic and Kleene algebra with tests. *ACM Transactions on Computational Logic*, 1(1):60–76, July 2000.
22. B. Möller. Lazy Kleene algebra. In D. Kozen, editor, *Mathematics of Program Construction*, volume 3125 of *LNCS*, pages 252–273. Springer-Verlag, 2004.
23. B. Möller. The linear algebra of UTP. In T. Uustalu, editor, *Mathematics of Program Construction*, volume 4014 of *LNCS*, pages 338–358. Springer-Verlag, 2006.
24. B. Möller and G. Struth. WP is WLP. In W. MacCaull, M. Winter, and I. Düntsch, editors, *Relational Methods in Computer Science 2005*, volume 3929 of *LNCS*, pages 200–211. Springer-Verlag, 2006.
25. G. Nelson. A generalization of Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems*, 11(4):517–561, October 1989.
26. J. von Wright. Towards a refinement algebra. *Science of Computer Programming*, 51(1–2):23–45, May 2004.