Fixpoints for General Correctness

Walter Guttmann

Department of Computer Science, University of Sheffield, UK
walter.guttmann@uni-ulm.de

Abstract

We investigate various fixpoint operators in a semiring-based setting that models a general correctness semantics of programs. They arise as combinations of least/greatest (pre/post)fixpoints with respect to refinement/approximation. In particular, we show isotony of these operators and give representations of fixpoints in terms of other fixpoints. Some results require completeness of the Egli-Milner order, for which we provide conditions.

A new perspective is reached by exchanging the semirings with distributive lattices. They can be augmented in a natural way with a second order that is similar to the Egli-Milner order. We extend our discussion of fixpoint operators to this induced order. We show the impact on general correctness by connecting the lattice- and the semiring-based treatments to obtain results about the Egli-Milner order.

Keywords: distributive lattice, Egli-Milner order, fixpoint, general correctness, median, program semantics, recursion, semiring

1. Introduction

For providing a semantics of non-deterministic sequential programs there are different ways to represent terminating and non-terminating executions that start in the same state. In such a case, partial correctness ignores the non-terminating executions and total correctness ignores the terminating ones. General correctness [26] is finer by independently keeping terminating and non-terminating executions. The price for this precision is a more complex approximation order, the Egli-Milner order, to give a fixpoint semantics of recursion. Partial and total correctness just reuse the refinement order, respectively, its converse.

Recent progress in the algebraic treatment of general correctness is facilitated by expressing the Egli-Milner approximation order in terms of the refinement order, and least fixpoints with respect to Egli-Milner in terms of least and greatest fixpoints with respect to refinement [23, 24, 25]. This overcomes the complexity of the Egli-Milner order by reducing calculations to the simpler refinement order. The algebraic structures underlying these developments are variants of semirings and distributive lattices.

To calculate with fixpoints or to show their existence it is typical to assume that functions are isotone, although occasionally this proviso is not available as in [4, 5, 13, 7]. We have therefore shown that also in our algebraic setting basic programming constructs such as sequential composition, non-deterministic choice and while-loops are isotone with respect to the Egli-Milner order. The first goal of the present paper is to extend this result to full recursion.

This means that we need to show isotony of the fixpoint operator which gives the solution to a recursion. Unlike in partial and total correctness, we must care for two orders in general correctness: approximation and refinement. With either order, isotony of the fixpoint operator is needed to show isotony of functions describing nested recursions. Additionally, isotony of the fixpoint operator with respect to the refinement order is needed for refinements carried out within the body of a recursion. The situation is complicated further because the Egli-Milner fixpoint is expressed in terms of the two refinement fixpoints.

As a consequence, we investigate all three fixpoint operators mentioned above, each with respect to both the Egli-Milner and the refinement order. In particular, we show that the operator, which maps an isotone function to its Egli-Milner least fixpoint, is itself isotone with respect to the lifted Egli-Milner order. This

is necessary since general isotony results for fixpoint operators, such as [9, Rule 8.28], only apply to least prefixpoints, but our treatment just yields least fixpoints. We therefore give conditions under which the Egli-Milner order is complete, whence prefixpoints exist and coincide with fixpoints.

For many results, however, it is possible to avoid completeness, and thereby profit from the support by automated theorem provers such as Prover9. Since in the absence of completeness fixpoints and prefixpoints have quite different properties, we maintain this distinction throughout this paper, and similarly for postfixpoints in the dual case.

In addition to isotony of a fixpoint operator, we are interested in the location of the resulting fixpoints in the 'other' order. This issue arises, for example, in proving correctness of loop introduction rules [23] or of the unfold-fold method, as we do in the present paper. Moreover the case of Egli-Milner least fixpoints, which are derived from refinement fixpoints, shows that operators of one order can be combined to yield useful operators of the other order.

Insight into the relations between both orders is gained by turning to a variant of the Egli-Milner order that is intimately related to the refinement order; the background is as follows. Sets with two orders have been considered in the context of logic programming [20, 18] and domain theory [27, 28], under the name of bilattices and bitopologies, respectively. The two orders represent the information structure and the logical structure. The second goal of the present paper is to establish the connection of these works to general correctness.

To this end, we switch from the semiring-based setting to distributive lattices. As recalled by [27, 28], the median operation induces a second order in the lattice [3]; call it the 'cross' order. We investigate least (pre)fixpoints and greatest (post)fixpoints with respect to the cross order. In particular, we give conditions for their existence and represent them by (pre/post)fixpoints with respect to the original lattice order. The link to general correctness is provided as in [7], namely by showing that the cross order is a superset of the Egli-Milner order. This allows us to transfer a number of results, for example, about fixpoints, from the cross order to the Egli-Milner order, which is useful because the cross order is less complex.

In Section 2 we review a model of general correctness in which programs are represented by matrices over relations. We show the effect of program operations and several constructions, which are used throughout subsequent sections, in this particular instance. Because this model satisfies the axioms underlying the remainder of this paper, all results obtained there apply to general correctness.

Section 3 works in the semiring setting of [23, 24]. New results include the correctness of the unfold-fold method, another representation of Egli-Milner least fixpoints, isotony of (pre/post)fixpoint operators and conditions for completeness of the approximation order. We conclude with several properties of the Kleene star and omega operations with respect to the Egli-Milner order.

Section 4 works in distributive lattices. Some new results concern least (pre)fixpoints in the cross order: conditions for their existence, weaker isotony assumptions and more general representations. We also show isotony of (pre/post)fixpoint operators and conclude with greatest (post)fixpoints in the cross order.

The link between semirings and lattices is drawn in Section 5. We show algebraically that the Egli-Milner order is a subset of the cross order and exemplify the transfer of results between the two.

Related work is pointed out throughout the paper and discussed in the final section, which refers and translates to concrete models found in the literature.

2. Matrix Representation of General Correctness

To motivate the algebraic treatment carried out in subsequent sections, we discuss a particular model of general correctness. It is based on the 'prescriptions' of [14] and represents programs by 2×2 matrices. For the present purpose we assume that the entries of the matrices are relations, that is, subsets of $R =_{\text{def}} Q \times Q$ for a fixed base set Q; see [32, 23] for weaker settings. Denote by $+$, $\curlywedge$ and $^-$ the union, intersection and complement operations; by $\leq$ the subset relation; by $\cdot$ relational composition; by 0, 1 and $\top$ the empty, identity and universal relations, respectively. The composition $x \cdot y$ is abbreviated by xy.

In program semantics, Q is the state space given by the possible values of variables, R is the set of programs or specifications, $+$ models non-deterministic choice, $\leq$ refinement, $\cdot$ sequential composition and 1 the program with no effect on the state.

In general correctness it is necessary to represent non-terminating and terminating executions of a program independently. This is achieved by prescriptions. A prescription is a 2×2 matrix

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \in R^{2\times 2}$$

such that $w = w\top$. Elements of the form $w\top$, called vectors in [36], model subsets of Q or conditions on the state space; they are closed under the operations $+$, $\curlywedge$, $^-$ and $x\cdot$ for each $x \in R$.

The entry w of a prescription captures the set of states from which non-terminating executions exist. The entry x holds the state transitions caused by terminating executions. The entries in the top row are fixed so that sequential composition of prescriptions works appropriately for general correctness.

Let S be the set of all prescriptions. A number of special prescriptions known from [35, 13] are:

$$\mathsf{fail} = \begin{pmatrix} \top & 0 \\ 0 & 0 \end{pmatrix} \qquad \mathsf{loop} = \begin{pmatrix} \top & 0 \\ \top & 0 \end{pmatrix} \qquad \mathsf{havoc} = \begin{pmatrix} \top & 0 \\ 0 & \top \end{pmatrix} \qquad \mathsf{chaos} = \begin{pmatrix} \top & 0 \\ \top & \top \end{pmatrix} \qquad \mathsf{skip} = \begin{pmatrix} \top & 0 \\ 0 & 1 \end{pmatrix}$$

For instance, loop is the program that does not terminate: the vector $\top$ in its bottom-left entry states that there is a non-terminating execution from each state, while 0 at the bottom-right states that there are no terminating executions. Similarly, havoc is the program that terminates but has an arbitrary effect on the state, and skip is the program that terminates without changing the state.

Operations on the prescriptions S are obtained by lifting from the underlying set R. In particular, $+$ and $\curlywedge$ are applied componentwise, and $\cdot$ is given by the matrix product:

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} + \begin{pmatrix} \top & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} \top & 0 \\ w+y & x+z \end{pmatrix} \qquad \begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \cdot \begin{pmatrix} \top & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} \top & 0 \\ w+xy & xz \end{pmatrix}$$

Intuitively, the non-terminating executions $w+xy$ of a sequential composition mean the following: either the first program does not terminate because it starts from a state in w, or the first program takes a transition x to reach a state in y, from where the second program does not terminate. The terminating executions xz are obtained by composing the terminating executions x and z of both programs.

The elements fail, skip and chaos of S take the places of 0, 1 and $\top$ for the lifted operations. This way, we obtain an algebraic structure for S which is similar to the underlying relational structure of R. However, some differences remain: for example, $x \cdot 0 = 0$ holds for each $x \in R$, but the lifted $y \cdot \mathsf{fail} = \mathsf{fail}$ is not true for all $y \in S$ as witnessed by $y = \mathsf{loop}$ or $y = \mathsf{chaos}$. This shows that relations and prescriptions represent different models of computations: relations are adequate for partial correctness, prescriptions are adequate for general correctness.

Nevertheless the algebraic structure of prescriptions is rich. In particular, S forms a bounded distributive lattice and a semiring without the right zero law mentioned above, and S has a Kleene star, an omega and an antidomain operation. The axioms of these structures are given in Sections 3 and 4; the point here is that prescriptions satisfy all those axioms, whence the results established in this paper in particular apply to prescriptions.

The lifted operations $+$, $\curlywedge$ and $\cdot$ model non-deterministic choice, conjunction and sequential composition of programs. The Kleene star models finite iteration, the omega models infinite iteration and the antidomain models the set of states without outgoing transitions. On prescriptions they are obtained by lifting as follows:

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix}^* = \begin{pmatrix} \top & 0 \\ x^*w & x^* \end{pmatrix} \qquad \begin{pmatrix} \top & 0 \\ w & x \end{pmatrix}^\omega = \begin{pmatrix} \top & 0 \\ x^\omega + x^*w & x^\omega \end{pmatrix} \qquad a\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} = \begin{pmatrix} \top & 0 \\ 0 & a(w+x) \end{pmatrix}$$

Intuitively, x^*w represents those states from which after finitely many executions of x a state in w is reached, from where a non-terminating execution exists; x^ω is a vector representing the states from which x can be executed infinitely often; in relational terms $a(w+x) = \overline{(w+x)\cdot\top} \curlywedge 1$ holds, which represents the set of states from which neither non-terminating nor terminating executions exist.

Further structure is available through the prescriptions loop and havoc. They have no counterparts in the underlying set R, and therefore are represented by elements L and H with additional axioms in the

upcoming sections. For instance, prescriptions satisfy $\mathsf{chaos} \cdot \mathsf{fail} = \mathsf{loop}$ or, abstractly, $\top \cdot 0 = \mathsf{L}$. Using the domain operation $d(x) = a(a(x))$, another law is $d(\mathsf{loop}) = \mathsf{skip}$ or, abstractly, $d(\mathsf{L}) = 1$. Yet another property is that loop and havoc are complements, that is, $\mathsf{L} \curlywedge \mathsf{H} = 0$ and $\mathsf{L} + \mathsf{H} = \top$.

It is frequently helpful to decompose a prescription into its finite and infinite executions. In a semiring-based setting such as that of Section 3, the infinite executions are obtained by sequentially composing with fail. Subsequent application of domain brings this information to the bottom-right entry where it can act as a restriction in sequential compositions:

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \cdot \begin{pmatrix} \top & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \top & 0 \\ w & 0 \end{pmatrix} \qquad d\begin{pmatrix} \top & 0 \\ w & 0 \end{pmatrix} = \begin{pmatrix} \top & 0 \\ 0 & d(w) \end{pmatrix}$$

Abstractly, this is achieved by $y0$ and $d(y0)$ for an element $y \in S$. We have the law $d(y0)\mathsf{L} = y0$ for prescriptions, which serves as another axiom in the abstract setting. This construction is also used for representing the Egli-Milner order on prescriptions [35, 34, 17], namely

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \sqsubseteq \begin{pmatrix} \top & 0 \\ y & z \end{pmatrix} \Leftrightarrow y \leq w \wedge x \leq z \leq w + x \; .$$

Intuitively, we may remove non-terminating executions by $y \leq w$ and add terminating executions by $x \leq z$ provided there are non-terminating executions, that is, $z \leq w + x$. Precisely this is achieved by the abstract representation of the Egli-Milner order given in Section 3. Least fixpoints with respect to this order are taken as the semantics of recursive programs.

For prescriptions we have $x \curlywedge \mathsf{L} = x0$ as an alternative way to obtain the infinite executions, suitable for a lattice-based setting. The finite executions are similarly obtained by $x \curlywedge \mathsf{H}$:

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \curlywedge \begin{pmatrix} \top & 0 \\ 0 & \top \end{pmatrix} = \begin{pmatrix} \top & 0 \\ 0 & x \end{pmatrix} .$$

The same effect cannot be achieved using the operations $+$, $\cdot$ and a only, but additional axioms are necessary in a semiring-based setting.

In the lattice-based setting of Section 4 we are moreover concerned with the following operations, which mix the effects of $+$ and $\curlywedge$ and appear in [13, 15]:

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \sqcap \begin{pmatrix} \top & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} \top & 0 \\ w + y & x \curlywedge z \end{pmatrix} \qquad \begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \sqcup \begin{pmatrix} \top & 0 \\ y & z \end{pmatrix} = \begin{pmatrix} \top & 0 \\ w \curlywedge y & x + z \end{pmatrix}$$

They are abstractly represented by $x \sqcap y = (\mathsf{L} \curlywedge x) + (x \curlywedge y) + (y \curlywedge \mathsf{L})$ and $x \sqcup y = (\mathsf{H} \curlywedge x) + (x \curlywedge y) + (y \curlywedge \mathsf{H})$, two instances of the median operation which we discuss there. Furthermore, they induce the order

$$\begin{pmatrix} \top & 0 \\ w & x \end{pmatrix} \sqsubseteq \begin{pmatrix} \top & 0 \\ y & z \end{pmatrix} \Leftrightarrow y \leq w \wedge x \leq z \; ,$$

which is a superset of the Egli-Milner order [13, 7].

The development in the remainder of this paper abstracts from prescriptions as matrices to their algebraic structure. We do this to obtain a more general treatment, to exhibit their structure more clearly and to avoid unnecessary details which tend to obscure connections. Although the development is abstract, based on few axioms rather than rich models, the results apply to prescriptions and related general correctness models of programs [26, 35, 13, 14, 7, 34].

3. Fixpoints in Semirings

To investigate the isotony of fixpoint operators we abstract from the model discussed in Section 2. Programs are represented by elements of a bounded antidomain semiring $(S, +, 0, \cdot, 1, a, \top)$ without the

right zero law. The axioms are based on [33, 11, 12]:

$$\begin{array}{ccc} x+0=x & 1\cdot x=x & 0\cdot x=0 \\ x+x=x & x\cdot 1=x & \\ x+y=y+x & x\cdot(y\cdot z)=(x\cdot y)\cdot z & a(x)\cdot x=0 \\ x+(y+z)=(x+y)+z & x\cdot(y+z)=(x\cdot y)+(x\cdot z) & a^2(x)+a(x)=1 \\ x+\top=\top & (x+y)\cdot z=(x\cdot z)+(y\cdot z) & a(x\cdot a^2(y))=a(x\cdot y) \end{array}$$

We obtain the natural order $x \leq y \Leftrightarrow_{\text{def}} x+y=y$ and the domain operation $d(x) =_{\text{def}} a^2(x)$ based on the antidomain a. The elements 0 and $\top$ are the least and greatest ones with respect to the natural order. The operations $+$, $\cdot$ and d are $\leq$-isotone, while a is $\leq$-antitone. The operation $+$ has lower precedence than $\cdot$ which is again omitted by writing xy instead of $x \cdot y$.

In program semantics the operation $+$ represents non-deterministic choice and $\cdot$ sequential composition. The element 1 models the program skip which has no effect on the state, 0 models the program fail which has no transitions, and $\top$ models the program chaos which may perform anything. The domain $d(x)$ describes the set of states from which transitions under x are possible, the antidomain $a(x)$ those states from which no transitions under x exist.

It follows from the above axioms that the operation d is idempotent, whence the domain elements $d(S) = \{d(x) \mid x \in S\}$ are the fixpoints of d. They form a Boolean algebra $(d(S), +, 0, \cdot, 1, a)$ with join $+$, meet $\cdot$ and complement a. Every domain element is ≤ 1 and models a set of states; intuitively, the sequential composition px of the domain element $p \in d(S)$ with the program $x \in S$ restricts the transitions of x to those that start in the set p. Particular consequences about the domain operation are:

$$\begin{array}{cccc} d(x)x=x & d(x+y)=d(x)+d(y) & 1=d(\top) & d(x)\leq d(y) \Leftrightarrow x\leq d(y)x \\ d(xd(y))=d(xy) & d(a(x))=a(x) & x\leq d(x)\top & d(x)y=0 \Leftrightarrow d(x)d(y)=0 \\ d(d(x)y)=d(x)d(y) & a(d(x))=a(x) & xd(y)\top\leq d(xy)\top & d(x)y\leq z \Leftrightarrow y\leq z+a(x)\top \end{array}$$

In a bounded setting such as the one above the element $\mathsf{L} =_{\text{def}} \top \cdot 0$ exists. Observe that in general it is not 0 because the right zero law is omitted from the axioms. In program semantics the operation $(\cdot 0)$ intuitively cuts away all terminating executions of a program. In particular, L represents the program loop or the endless loop, whence we expect it to be the least element of the Egli-Milner order. To obtain this, we assume the following axioms about L:

$$\begin{array}{ll} (\mathsf{L1}) & d(x0)\mathsf{L}=x0 \\ (\mathsf{L2}) & d(\mathsf{L})=1 \end{array}$$

Intuitively, the axiom (L1) describes that the non-terminating executions of x are obtained by restricting the endless loop to the states from where x does not terminate. The axiom (L2) states that the endless loop L is total. We define the Egli-Milner order as in [24]:

$$x \sqsubseteq y \Leftrightarrow_{\text{def}} x \leq y + x0 \wedge y \leq x + d(x0)\top \,.$$

As discussed in Section 2, this gives the expected approximation order when instantiated in models of general correctness. An advantage of this definition over the previous one given in [23] is that it does not require the element H, which we discuss later.

The need for the specific axioms about L is apparent from the following consequence [24, Theorem 1], see also [23, Lemma 5].

Proposition 1. *The relation $\sqsubseteq$ is a partial order if and only if* (L1) *holds. It has the least element L if and only if* (L2) *holds. The operations $+$ and $\cdot$ are $\sqsubseteq$-isotone.*

Using sequential composition and non-deterministic choice we obtain the conditional statement according to if p then x else $y = d(p)x + a(p)y$. Then the semantics of the while-loop while p do y is given as the least fixpoint of the function $\lambda x.$if p then yx else 1 with respect to the Egli-Milner order. It can be represented using the Kleene star and omega operations, which are $\sqsubseteq$-isotone, too. We defer the discussion of this specific recursion to Section 3.6.

In general, recursion is modelled by the equation $x = f(x)$ using an arbitrary function $f : S \to S$. In this equation, $f(x)$ represents the body of the recursive program, possibly containing recursive calls to the program x being defined. For example, $f(x) = d(p)yx + a(p)$ characterises the while-loop described above. The semantics of the recursion $x = f(x)$ is the $\sqsubseteq$-least fixpoint of the function f.

For the reasons explained in the introduction, we are interested in this and other fixpoints of f: the $\sqsubseteq$-least fixpoint ξf and the $\sqsubseteq$-least prefixpoint $\hat{\xi} f$, the $\leq$-least fixpoint μf and the $\leq$-least prefixpoint $\hat{\mu} f$, the $\leq$-greatest fixpoint νf and the $\leq$-greatest postfixpoint $\hat{\nu} f$. They are elements of S satisfying the following properties:

$$\begin{array}{llll} f(\xi f) = \xi f & f(x) = x \Rightarrow \xi f \sqsubseteq x & f(\hat{\xi} f) \sqsubseteq \hat{\xi} f & f(x) \sqsubseteq x \Rightarrow \hat{\xi} f \sqsubseteq x \\ f(\mu f) = \mu f & f(x) = x \Rightarrow \mu f \leq x & f(\hat{\mu} f) \leq \hat{\mu} f & f(x) \leq x \Rightarrow \hat{\mu} f \leq x \\ f(\nu f) = \nu f & f(x) = x \Rightarrow \nu f \geq x & f(\hat{\nu} f) \geq \hat{\nu} f & f(x) \geq x \Rightarrow \hat{\nu} f \geq x \end{array}$$

If μf, νf and ξf exist, then clearly $\mu f \leq \xi f \leq \nu f$. Another simple consequence is that the least prefixpoint of an isotone function is the least fixpoint, and similarly for postfixpoints [10, Theorem 4.2]. The converse implication, however, does not necessarily hold: the existence of the least fixpoint does not imply the existence of the least prefixpoint, and similarly for postfixpoints. (A counterexample for partial orders is the function $\lambda x.2x$ on the integer numbers ordered by $\leq$ having the least and unique fixpoint 0 and all negative numbers as prefixpoints, hence no least prefixpoint.)

The following representation of the Egli-Milner least fixpoint ξf in terms of the $\leq$-least and $\leq$-greatest fixpoints μf and νf is obtained in [24, Corollary 3], see also [23, Corollary 13]. Its proof does not need (L2).

Proposition 2. *Let $f : S \to S$ be $\leq$- and $\sqsubseteq$-isotone and assume that μf and νf exist. Then ξf exists if and only if $\nu f \leq \mu f + d(\nu f 0)\top$ if and only if $\xi f = \nu f 0 + \mu f$.*

A benefit of the representation is that it replaces calculations using the complex Egli-Milner order $\sqsubseteq$, necessary for the general correctness semantics, by calculations using the simpler refinement order $\leq$. For example, Section 3.6 shows how to obtain the general correctness semantics of while-loops this way and Section 3.1 applies it to show correctness of the unfold-fold method.

The existing proof of Proposition 2, however, does not yield the $\sqsubseteq$-least prefixpoint $\hat{\xi} f$ even if $\hat{\mu} f$ and $\hat{\nu} f$ exist. This is unfortunate, because sometimes prefixpoints are necessary, for example, to show that a fixpoint operator is isotone. As remarked in the introduction, isotony of fixpoint operators is necessary for dealing with nested recursions. The following result is available [9, Rule 8.28] and stated here in terms of the order $\sqsubseteq$. Orders such as $\sqsubseteq$ and $\leq$ are lifted to functions pointwise.

Proposition 3. *Let $f, g : S \to S$ be such that $f \sqsubseteq g$. If $\hat{\xi} f$ and $\hat{\xi} g$ exist, then $\hat{\xi} f \sqsubseteq \hat{\xi} g$. If additionally f and g are $\sqsubseteq$-isotone, then $\xi f \sqsubseteq \xi g$.*

However, $\xi f \sqsubseteq \xi g$ cannot be obtained by assuming the existence of ξf and ξg only. (Continuing the above counterexample, take $\lambda x.2x$ and $\lambda x.2x + 2$ with the least fixpoints 0 and -2, respectively, despite $2x \leq 2x + 2$ for every integer number x.) This means we have to establish the existence of $\hat{\xi} f$ and $\hat{\xi} g$. By the following result [31, Theorem 9], it remains to show completeness with respect to the Egli-Milner order. A partially ordered set is chain-complete if every chain (possibly empty, totally ordered subset) has a supremum.

Proposition 4. *Let $f : S \to S$ be $\sqsubseteq$-isotone and assume that S is $\sqsubseteq$-chain-complete. Then $\hat{\xi} f$ exists.*

We give sufficient conditions in Section 3.4. Before that, we show that still many results about fixpoints can be derived without resorting to completeness. We prefer to avoid completeness and stay first-order whenever possible, because this enables the use of automated theorem provers such as Prover9. In particular, we look at the unfold-fold method, give another representation of ξf and investigate isotony of the fixpoint operators with respect to $\leq$ and of $\hat{\mu}$ with respect to $\sqsubseteq$.

3.1. Correctness of Unfold-Fold

As an example showing the usefulness of the representation granted by Proposition 2, we describe the unfold-fold method [6], which can be used to develop recursive programs from specifications. We are concerned with a generalisation given by [1] that allows the reduction of non-determinism in addition to meaning-preserving transformations. Its essence is captured in our algebraic setting as follows:

1. Start with a specification $x_0 \in S$.
2. Successively apply meaning-preserving or refining transformations (such as unfold and fold) to obtain a sequence of specifications $x_0, x_1, x_2, \ldots, x_n \in S$ where each step maintains or reduces non-determinism, that is, $x_i \geq x_{i+1}$.
3. Reach a specification x_n which is given in terms of the original x_0, that is, $x_n = f(x_0)$.
4. Turn it into the recursive program ξf.

In summary, we have $f(x_0) = x_n \leq x_{n-1} \leq \ldots \leq x_1 \leq x_0$, whence x_0 is a prefixpoint of f. This implies $\hat{\mu} f \leq x_0$, hence the method is valid in partial correctness, where recursions are solved by $\leq$-least fixpoints. The validity in general correctness, however, amounts to $\xi f \leq x_0$, which states that the recursively defined result ξf implements the original specification x_0. It is not clear that this holds, since x_0 is not necessarily a fixpoint of f, and even if $f(x_0) = x_0$ held, we could only conclude $\xi f \sqsubseteq x_0$.

A proof of the unfold-fold method in general correctness is given by [1] in a functional setting. We algebraically state and prove their result. Validity of unfold-fold in total correctness is addressed by [22, Theorem 4.5] in relation algebra.

Theorem 5. *Let $f : S \to S$ be $\leq$- and $\sqsubseteq$-isotone and assume that $\hat{\mu} f$, νf and ξf exist. Then*

1. $f(x) \leq x \Rightarrow \xi f \leq x + \mathsf{L}$.
2. $f(x) \leq x \wedge \xi f 0 \leq x 0 \Rightarrow \xi f \leq x$.

Proof. From $f(x) \leq x$ we obtain $\hat{\mu} f \leq x$, whence $\mu f = \hat{\mu} f \leq x$ since f is $\leq$-isotone. Claim (1) follows by $\xi f = \nu f 0 + \mu f \leq \top 0 + x = \mathsf{L} + x$ using Proposition 2. By the same proposition, we have $\xi f 0 = (\nu f 0 + \mu f)0 = \nu f 0$. Assuming $\xi f 0 \leq x 0$, we obtain claim (2) by $\xi f = \nu f 0 + \mu f = \xi f 0 + \mu f \leq x 0 + x = x$. □

Claim (1) corresponds to [1, Theorem 4.4] and claim (2) to [1, Corollary 4.5]; observe that our proof needs no induction. Intuitively, $\xi f 0 \leq x 0$ states that whenever x terminates, so does ξf.

Note that the main correctness claim $\xi f \leq x$ combines the natural order $\leq$ with the fixpoint ξf, which is essentially defined in terms of the Egli-Milner order $\sqsubseteq$. Another example for such a combination of the two orders is the general correctness loop refinement rule [23, Theorem 11].

3.2. Representing Egli-Milner Fixpoints

We extend Proposition 2 by further equivalent conditions and a representation in terms of the meet in the Egli-Milner order. More conditions and another representation can be added by additionally assuming that $(S, \leq)$ is a distributive lattice [25], see also Section 5.

The greatest lower bound of $x, y \in S$ with respect to $\sqsubseteq$ is denoted by $x \sqcap y$, provided it exists. Unless explicitly stated, existence is assumed for terms in the antecedent of a statement, but has to be established for terms in the consequent.

Theorem 6. *Let $f : S \to S$ be $\leq$- and $\sqsubseteq$-isotone and assume that μf and νf exist. Then the following are equivalent:*

1. *ξf exists.*
2. $\nu f \leq \mu f + d(\nu f 0)\top$.
3. $\xi f = \nu f 0 + \mu f$.
4. $\xi f = \mu f \sqcap \nu f$.
5. $\mu f \sqcap \nu f = \nu f 0 + \mu f$.
6. $\nu f 0 + \mu f \sqsubseteq \nu f$.

7. $\mu f \sqcap \nu f \leq \nu f$.

PROOF. Proposition 2 shows that (1), (2) and (3) are equivalent. We first add (4), (5) and (6) to this cycle, and then (7).

(1) $\Rightarrow$ (4): By definition, $\xi f \sqsubseteq \mu f$ and $\xi f \sqsubseteq \nu f$. Let $x \sqsubseteq \mu f$ and $x \sqsubseteq \nu f$, then $x \leq \mu f + x0 \leq \xi f + x0$ and $\xi f \leq \nu f \leq x + d(x0)\top$, whence $x \sqsubseteq \xi f$.

(4) $\Rightarrow$ (5): Clearly (4) implies (1), therefore apply (3).

(5) $\Rightarrow$ (6): This is immediate since $\mu f \sqcap \nu f \sqsubseteq \nu f$.

(6) $\Rightarrow$ (2): This holds by $\nu f \leq \nu f 0 + \mu f + d((\nu f 0 + \mu f)0)\top = \nu f 0 + \mu f + d(\nu f 0)\top = \mu f + d(\nu f 0)\top$.

(5) $\Rightarrow$ (7): This is immediate since $\nu f 0 + \mu f \leq \nu f$.

(7) $\Rightarrow$ (2): Let $m =_{\text{def}} \mu f \sqcap \nu f \leq \nu f$, then $m \sqsubseteq \mu f$ implies $m \leq \mu f + m0$, whence $m \sqsubseteq \nu f$ implies $\nu f \leq m + d(m0)\top \leq \mu f + m0 + d(m0)\top = \mu f + d(m0)\top \leq \mu f + d(\nu f 0)\top$. □

Half of statement (5) of the preceding theorem, namely $\mu f \sqcap \nu f \sqsubseteq \nu f 0 + \mu f$, holds provided $m = \mu f \sqcap \nu f$ exists. To see this, infer $m \leq \mu f + m0 \leq \nu f 0 + \mu f + m0$ from $m \sqsubseteq \mu f$, and $\nu f 0 + \mu f \leq \nu f \leq m + d(m0)\top$ from $m \sqsubseteq \nu f$.

3.3. Isotony without Completeness

We start investigating isotony of the (pre/post)fixpoint operators. Let us first collect the known cases and simple consequences. The following result covers $\leq$-isotony.

Theorem 7. *Let $f, g : S \to S$ be such that $f \leq g$.*

1. *If $\hat{\mu} f$ and $\hat{\mu} g$ exist, then $\hat{\mu} f \leq \hat{\mu} g$. If additionally f and g are $\leq$-isotone, then $\mu f \leq \mu g$.*
2. *If $\hat{\nu} f$ and $\hat{\nu} g$ exist, then $\hat{\nu} f \leq \hat{\nu} g$. If additionally f and g are $\leq$-isotone, then $\nu f \leq \nu g$.*
3. *If $\hat{\mu} f$, $\hat{\nu} f$, ξf, $\hat{\mu} g$, $\hat{\nu} g$ and ξg exist and f and g are $\leq$- and $\sqsubseteq$-isotone, then $\xi f \leq \xi g$. If additionally $\hat{\xi} f$ and $\hat{\xi} g$ exist, then $\hat{\xi} f \leq \hat{\xi} g$.*

PROOF.

1. $f(\hat{\mu} g) \leq g(\hat{\mu} g) \leq \hat{\mu} g$ implies $\hat{\mu} f \leq \hat{\mu} g$. By $\leq$-isotony, $\hat{\mu} f = \mu f$ and $\hat{\mu} g = \mu g$.
2. This follows dually.
3. By claims (1) and (2), $\mu f \leq \mu g$ and $\nu f \leq \nu g$. Thus $\xi f = \nu f 0 + \mu f \leq \nu g 0 + \mu g = \xi g$ by Proposition 2 and $\leq$-isotony of $\cdot$ and $+$. If $\hat{\xi} f$ exists, then $\hat{\xi} f = \xi f$ by $\sqsubseteq$-isotony of f, and similarly $\hat{\xi} g = \xi g$. □

For example, consider a recursive program $x = g(x)$ such that the body $g(x)$ contains non-determinism, that is, several possible executions starting in the same state. A step in program development might refine the body of the recursion $g(x)$ to $f(x)$ such that $f(x)$ is deterministic. Formally this means $f(x) \leq g(x)$ for each $x \in S$, that is, $f \leq g$. This results in the new recursive program $x = f(x)$. To show that it is a refinement of the original program, we apply claim (3) of the preceding theorem: provided the stated existence and isotony requirements are fulfilled, we obtain $\xi f \leq \xi g$.

We now turn to $\sqsubseteq$-isotony of the (pre/post)fixpoint operators. Proposition 3, which is proved just as claim (1) of Theorem 7, covers the Egli-Milner (pre)fixpoint up to the existence of $\hat{\xi} f$, which we discuss in Section 3.4. The $\leq$-greatest (post)fixpoint follows in Section 3.5. We begin with the $\leq$-least (pre)fixpoint. A preparatory lemma shows the effect of $f \sqsubseteq g$ in the order $\leq$.

Lemma 8. *Let $f, g : S \to S$ be such that f or g is $\sqsubseteq$-isotone and $f \sqsubseteq g$. Then $f(x+y0) \leq g(x) + f(x+y0)0$ and $g(x + d(x0)\top) \leq f(x) + d(f(x)0)\top$. In particular, $f(x + \mathsf{L}) \leq g(x) + \mathsf{L}$.*

PROOF. For every $\sqsubseteq$-isotone $h : S \to S$ we have $h(x + y0) \sqsubseteq h(x) \sqsubseteq h(x + d(x0)\top)$. Namely, by $\sqsubseteq$-isotony this reduces to $x + y0 \sqsubseteq x \sqsubseteq x + d(x0)\top$, which is immediate from the definition of $\sqsubseteq$. We remark that the consequence $h(x + \mathsf{L}) \leq h(x) + \mathsf{L}$ corresponds to [1, Lemma 4.3].

The claims $f(x+y0) \leq g(x)+f(x+y0)0$ and $g(x+d(x0)\top) \leq f(x)+d(f(x)0)\top$ follow from $f(x+y0) \sqsubseteq g(x)$ and $f(x) \sqsubseteq g(x + d(x0)\top)$, which are obtained according to

$$\begin{array}{ccccc} f(x + y0) & \sqsubseteq & f(x) & \sqsubseteq & f(x + d(x0)\top) \\ \sqcap\!| & & \sqcap\!| & & \sqcap\!| \\ g(x + y0) & \sqsubseteq & g(x) & \sqsubseteq & g(x + d(x0)\top) \end{array}$$

using $f \sqsubseteq g$ and $\sqsubseteq$-isotony of f or g. In particular, $f(x+\mathsf{L}) \leq g(x)+f(x+\top 0)0 \leq g(x)+\top 0 = g(x)+\mathsf{L}$. □

Theorem 9. *Let $f, g : S \to S$ be such that f is $\leq$- and $\sqsubseteq$-isotone and $f \sqsubseteq g$. If $\hat{\mu}f$ and $\hat{\mu}g$ exist, then $\hat{\mu}f \sqsubseteq \hat{\mu}g$. If additionally g is $\leq$-isotone, then $\mu f \sqsubseteq \mu g$.*

PROOF. We have $\hat{\mu}g \leq \hat{\mu}f + d(\hat{\mu}f0)\top$ since $g(\hat{\mu}f + d(\hat{\mu}f0)\top) \leq f(\hat{\mu}f) + d(f(\hat{\mu}f)0)\top \leq \hat{\mu}f + d(\hat{\mu}f0)\top$ by Lemma 8. Hence $f(\hat{\mu}g + \hat{\mu}f0) \leq f(\hat{\mu}f + d(\hat{\mu}f0)\top + \hat{\mu}f0) = f(\hat{\mu}f + d(\hat{\mu}f0)\top) \leq f(\hat{\mu}f) + d(f(\hat{\mu}f)0)\top \leq \hat{\mu}f + d(\hat{\mu}f0)\top$ by $\leq$-isotony of f and Lemma 8. This implies $f(\hat{\mu}g + \hat{\mu}f0)0 \leq (\hat{\mu}f + d(\hat{\mu}f0)\top)0 = \hat{\mu}f0 + d(\hat{\mu}f0)\mathsf{L} = \hat{\mu}f0$ by (L1). Therefore $f(\hat{\mu}g + \hat{\mu}f0) \leq g(\hat{\mu}g) + f(\hat{\mu}g + \hat{\mu}f0)0 \leq \hat{\mu}g + \hat{\mu}f0$ using Lemma 8 again. Thus $\hat{\mu}f \leq \hat{\mu}g + \hat{\mu}f0$, which gives $\hat{\mu}f \sqsubseteq \hat{\mu}g$ with our first observation. If both f and g are $\leq$-isotone, then $\hat{\mu}f = \mu f$ and $\hat{\mu}g = \mu g$. □

3.4. Completeness of the Egli-Milner Order

To obtain $\sqsubseteq$-isotony for ξ according to Proposition 3 we need the existence of $\hat{\xi}f$, which is not granted by Proposition 2, whence we use Proposition 4. But then we have to show that S is chain-complete with respect to $\sqsubseteq$, which we do in the following.

The supremum of the subset $D \subseteq S$ with respect to $\leq$ is denoted by $\sup_{\leq} D$, provided it exists; similarly $\inf_{\leq} D$ denotes the infimum and $x \curlywedge y =_{\text{def}} \inf_{\leq}\{x, y\}$ the $\leq$-meet of two elements $x, y \in S$. We start with a lemma about suprema of domain elements.

Lemma 10. *Let $D \subseteq d(S)$ be a set of domain elements and $x \in S$ such that $px = 0$ for each $p \in D$. If $\sup_{\leq} D$ exists, then $d(\sup_{\leq} D)x = 0$.*

PROOF. $px = 0 \Leftrightarrow pd(x) = 0 \Leftrightarrow p \leq a(d(x)) = a(x)$ for each $p \in D$ since $p = d(p)$, hence $\sup_{\leq} D \leq a(x)$, which implies $d(\sup_{\leq} D) \leq d(a(x)) = a(x) \Leftrightarrow d(\sup_{\leq} D)d(x) = 0 \Leftrightarrow d(\sup_{\leq} D)x = 0$. □

We cannot use [12, Proposition 5.2], which states $d(\sup_{\leq} D) = \sup_{\leq | d(S)} d(D)$ for an arbitrary $D \subseteq S$ with existing supremum $\sup_{\leq} D$. The reason is that the second supremum $\sup_{\leq | d(S)}$ is taken among the domain elements $d(S)$. In a domain semiring S this supremum is in general different from the supremum taken in S.

A partial order is complete if it has a least element and every directed subset of elements has a supremum. A subset D is directed if it is not empty and every pair of elements of D has an upper bound in D.

Assume that $(S, \leq)$ is a complete partial order. Consider the set $F =_{\text{def}} \{x \in S \mid x0 = 0\}$ of finite elements [33, Definition 4.6]: it is $\leq$-directed since $0 \in F$ and any $x, y \in F$ have the (least) upper bound $x + y \in F$. Hence $\mathsf{H} =_{\text{def}} \sup_{\leq} F$ exists; it corresponds to the program havoc. Intuitively, every element of F has only terminating executions. The next lemma extends this to H and asserts the existence of the function $(\curlywedge \mathsf{H})$ used subsequently.

Lemma 11. *Assume that $(S, \leq)$ is a complete partial order and $\cdot$ distributes over suprema of $\leq$-directed sets in its first argument. Then $\mathsf{H}0 = 0$ and $u \curlywedge \mathsf{H}$ exists for each $u \in S$.*

PROOF. First, $\mathsf{H}0 = (\sup_{\leq} F)0 = \sup_{\leq}\{x0 \mid x0 = 0\} = \sup_{\leq}\{0\} = 0$. Second, let $u \in S$ and consider the set $F_u =_{\text{def}} \{x \in S \mid x0 = 0 \wedge x \leq u\}$: as F it is $\leq$-directed with least upper bound $+$, whence $\sup_{\leq} F_u$ exists. We show $\sup_{\leq} F_u = u \curlywedge \mathsf{H}$. Clearly $\sup_{\leq} F_u \leq u$ since $x \leq u$ for each $x \in F_u$, and $\sup_{\leq} F_u \leq \mathsf{H}$ since $F_u \subseteq F$. Let $x \leq u$ and $x \leq \mathsf{H}$, then $x0 \leq \mathsf{H}0 = 0$, hence $x \in F_u$, thus $x \leq \sup_{\leq} F_u$. □

Intuitively, $x \leftthreetimes \mathsf{H}$ represents the finite executions of x. By definition, the functions $(\leftthreetimes \mathsf{H})$ and $(+\mathsf{L})$ form a Galois connection if $x \leftthreetimes \mathsf{H} \leq y \Leftrightarrow x \leq y + \mathsf{L}$ holds for each $x, y \in S$. Using this we can separate each element x into its infinite part $x0$ and its finite part $x \leftthreetimes \mathsf{H}$, see also [33].

Lemma 12. *Assume that the functions $(\leftthreetimes \mathsf{H})$ and $(+\mathsf{L})$ form a Galois connection. Then $x = x0 + (x \leftthreetimes \mathsf{H})$ and $x \leq y + \mathsf{L} \Leftrightarrow x \leq y + x0$ for each $x, y \in S$.*

Proof. The Galois connection gives $x \leq (x \leftthreetimes \mathsf{H}) + \mathsf{L}$, whence $d(x0)x \leq d(x0)((x \leftthreetimes \mathsf{H}) + \mathsf{L}) \leq (x \leftthreetimes \mathsf{H}) + d(x0)\mathsf{L} = (x \leftthreetimes \mathsf{H}) + x0$ by (L1). Moreover $a(x0)x \leq x \leftthreetimes \mathsf{H}$ because $a(x0)x \leq x$ and $a(x0)x0 = 0$ implies $a(x0)x \in F$ and hence $a(x0)x \leq \mathsf{H}$. Together $x = d(x0)x + a(x0)x \leq x0 + (x \leftthreetimes \mathsf{H}) \leq x$, showing the first claim.

The backward implication of the second claim is immediate by $x0 \leq \top 0 = \mathsf{L}$. For the forward implication assume $x \leq y + \mathsf{L}$, then $x \leftthreetimes \mathsf{H} \leq y$ by Galois, whence $x = x0 + (x \leftthreetimes \mathsf{H}) \leq x0 + y$ by the first claim. □

The existence of the Galois connection in the previous lemma is equivalent to the following conditions: $(\leftthreetimes \mathsf{H})$ distributes over $+$, $(+\mathsf{L})$ distributes over existing $\leftthreetimes$, $\mathsf{L} + \mathsf{H} = \top$ and $\mathsf{L} \leftthreetimes \mathsf{H} = 0$. As a consequence, we obtain the following equivalent representation of the Egli-Milner order: $x \sqsubseteq y \Leftrightarrow x \leq y + \mathsf{L} \wedge y \leq x + d(x0)\top$. We can now establish the main result, namely, completeness of the Egli-Milner order.

Theorem 13. *Assume that*

1. *$(S, \leq)$ is a complete partial order,*
2. *the function $\cdot$ distributes over suprema of $\leq$-directed sets in its first argument,*
3. *the supremum of a $\leq$-directed set of domain elements is a domain element, and*
4. *the functions $(\leftthreetimes \mathsf{H})$ and $(+\mathsf{L})$ form a Galois connection.*

Then $(S, \sqsubseteq)$ is a complete partial order.

Proof. By Proposition 1, S has the $\sqsubseteq$-least element L. Let $D \subseteq S$ be $\sqsubseteq$-directed.

Consider $D_H =_{\text{def}} \{u \leftthreetimes \mathsf{H} \mid u \in D\}$. To see that D_H is $\leq$-directed, let $u, v \in D$ and w some $\sqsubseteq$-upper bound, hence $u \sqsubseteq w$ and $v \sqsubseteq w$. Then $u \leq w + \mathsf{L}$, whence $u \leftthreetimes \mathsf{H} \leq w$ by the Galois connection, and clearly $u \leftthreetimes \mathsf{H} \leq \mathsf{H}$, thus $u \leftthreetimes \mathsf{H} \leq w \leftthreetimes \mathsf{H}$. Similarly $v \leftthreetimes \mathsf{H} \leq w \leftthreetimes \mathsf{H}$, and therefore $w \leftthreetimes \mathsf{H}$ is an upper bound in D_H.

Consider $D_L =_{\text{def}} \{x0 \mid x \in D\}$. To see that D_L is $\geq$-directed, let $u \sqsubseteq w$ and $v \sqsubseteq w$ for some $\sqsubseteq$-upper bound w of $u, v \in D$. Then $w \leq u + d(u0)\top$, whence $w0 \leq (u + d(u0)\top)0 = u0 + d(u0)\mathsf{L} = u0$ by (L1). Similarly $w0 \leq v0$, and therefore $w0$ is a lower bound in D_L.

To construct the $\leq$-infimum of D_L, consider $D_N =_{\text{def}} \{a(x0) \mid x \in D\}$: it is $\leq$-directed since the antidomain a is $\leq$-antitone and D_L is $\geq$-directed. Hence $\sup_{\leq} D_N$ exists.

We show $\inf_{\leq} D_L = a(\sup_{\leq} D_N)\mathsf{L}$. For each $x \in D$ we have $a(x0) \leq \sup_{\leq} D_N$, whence $a(\sup_{\leq} D_N)\mathsf{L} \leq a(a(x0))\mathsf{L} = d(x0)\mathsf{L} = x0$ by (L1), so $a(\sup_{\leq} D_N)\mathsf{L}$ is a lower bound of D_L. Let $z \leq x0$ for each $x \in D$, then $a(x0)z \leq a(x0)x0 = 0$, whence $d(\sup_{\leq} D_N)z = 0$ by Lemma 10. Thus $z = a(\sup_{\leq} D_N)z \leq a(\sup_{\leq} D_N)y0 \leq a(\sup_{\leq} D_N)\mathsf{L}$ using some $y \in D \neq \emptyset$.

We finally show $\sup_{\sqsubseteq} D = s =_{\text{def}} \inf_{\leq} D_L + \sup_{\leq} D_H$. To see that s is an $\sqsubseteq$-upper bound of D, let $x \in D$ and we show $x \sqsubseteq s$. First, $x \leftthreetimes \mathsf{H} \leq \sup_{\leq} D_H$, hence $x \leq \sup_{\leq} D_H + \mathsf{L} \leq s + \mathsf{L}$ by Galois. Second, $\inf_{\leq} D_L \leq x0 \leq d(x0)\top \leq x + d(x0)\top$, whence it remains to show $\sup_{\leq} D_H \leq x + d(x0)\top$, or $u \leftthreetimes \mathsf{H} \leq x + d(x0)\top$ for each $u \in D$. But this follows by the Galois connection using an $\sqsubseteq$-upper bound w of x and u, because $x \sqsubseteq w$ and $u \sqsubseteq w$ imply $u \leq w + \mathsf{L} \leq x + d(x0)\top + \mathsf{L}$.

To show that s is the least $\sqsubseteq$-upper bound, let $x \sqsubseteq z$ for each $x \in D$, hence $x \leq z + \mathsf{L}$ and $z \leq x + d(x0)\top$. Now $s \leq z + \mathsf{L}$ follows because $\inf_{\leq} D_L = a(\sup_{\leq} D_N)\mathsf{L} \leq \mathsf{L}$ and $\sup_{\leq} D_H \leq z$ since $x \leftthreetimes \mathsf{H} \leq z$ by Galois. So for $s \sqsubseteq z$ it remains to show $z \leq s + d(s0)\top$, which follows from $z \leq \sup_{\leq} D_H + d(\inf_{\leq} D_L \cdot 0)\top$. This is simplified using $\inf_{\leq} D_L \cdot 0 = a(\sup_{\leq} D_N)\mathsf{L}0 = a(\sup_{\leq} D_N)\mathsf{L}$ and $d(a(\sup_{\leq} D_N)\mathsf{L}) = d(a(\sup_{\leq} D_N)d(\mathsf{L})) = d(a(\sup_{\leq} D_N)) = a(\sup_{\leq} D_N)$ by (L2). Hence it suffices to show $z \leq \sup_{\leq} D_H + a(\sup_{\leq} D_N)\top$ or equivalently $d(\sup_{\leq} D_N)z \leq \sup_{\leq} D_H$. By the assumptions we can remove d and distribute $(\cdot z)$, so that we are left with $a(x0)z \leq \sup_{\leq} D_H$ for each $x \in D$. But this follows since $a(x0)z \leq x \leftthreetimes \mathsf{H}$: on the one hand $a(x0)z \leq a(x0)(x + d(x0)\top) = a(x0)x + 0 \leq x$; on the other hand this implies $a(x0)z0 \leq a(x0)x0 = 0$, whence $a(x0)z \leq \mathsf{H}$. □

Restricting the claim of the previous theorem to chain-completeness does not reduce the assumptions, since the definition of H and Lemma 11 are based on directed sets. A proof shortcut via a fixpoint theorem and its converse [31, Theorem 11] fails because Proposition 2 requires each function f to be both $\leq$- and $\sqsubseteq$-isotone and poses the additional constraint $\nu f \leq \mu f + d(\nu f 0)\top$.

By combining Theorem 13 with Propositions 3 and 4, we obtain $\sqsubseteq$-isotony for $\hat{\xi}$ and ξ.

Corollary 14. *Assume the conditions of Theorem 13 and let $f, g : S \to S$ be $\sqsubseteq$-isotone such that $f \sqsubseteq g$. Then $\hat{\xi} f \sqsubseteq \hat{\xi} g$ and $\xi f \sqsubseteq \xi g$.*

For example, consider two mutually recursive programs $x = tx + uy$ and $y = vx + wy$ using arbitrary programs $t, u, v, w \in S$. The semantics of the recursion x may be obtained as the prefixpoint $\hat{\xi} f$ of the function $f(x) = tx + u\hat{\xi} g_x$ using the nested prefixpoint of the parametric function $g_x(y) = vx + wy$. By Proposition 1 we know that g_x is $\sqsubseteq$-isotone for each $x \in S$. But to obtain that $\hat{\xi} f$ exists by Proposition 4, we need that f is $\sqsubseteq$-isotone. To show this, assume $x \sqsubseteq z$: then $g_x(y) = vx + wy \sqsubseteq vz + wy = g_z(y)$ for each $y \in S$ by Proposition 1, that is, $g_x \sqsubseteq g_z$; hence $\hat{\xi} g_x \sqsubseteq \hat{\xi} g_z$ by Corollary 14 assuming the conditions of Theorem 13; therefore $f(x) = tx + u\hat{\xi} g_x \sqsubseteq tx + u\hat{\xi} g_z = f(z)$ again by Proposition 1. Because f and g_x are $\sqsubseteq$-isotone, the prefixpoints are actually fixpoints.

3.5. Isotony of the Greatest Fixpoint Operator

It remains to investigate $\sqsubseteq$-isotony for the $\leq$-greatest (post)fixpoint operators. This case can be treated without completeness up to assuming $\xi g 0 \leq \xi f 0$ and the existence of $(\curlywedge \mathsf{H})$. We first recall the precise conditions of ν-fusion; the proof follows [9, Rule 8.30].

Lemma 15. *Let $(P, \leq_P)$ and $(Q, \leq_Q)$ be partial orders. Assume that $f^- : P \to Q$ and $f^+ : Q \to P$ form a Galois connection $f^-(x) \leq_Q y \Leftrightarrow x \leq_P f^+(y)$. Let $g : Q \to Q$ and $h : P \to P$ be such that h is $\leq_P$-isotone and $\hat{\nu} g$ and $\hat{\nu} h$ exist. If $h \circ f^+ \leq_P f^+ \circ g$ then $\nu h \leq_P f^+(\hat{\nu} g)$.*

Assume additionally that $h \circ f^+ = f^+ \circ g$. If g is $\leq_Q$-isotone then $\nu h = f^+(\hat{\nu} g) = f^+(\nu g)$. If $\hat{\nu} h$ exists then $\hat{\nu} h = \nu h = f^+(\hat{\nu} g)$.

Proof. $\nu h \leq_P f^+(f^-(\nu h))$ by Galois, hence $\nu h = h(\nu h) \leq_P h(f^+(f^-(\nu h))) \leq_P f^+(g(f^-(\nu h)))$ by $\leq_P$-isotony of h and $h \circ f^+ \leq_P f^+ \circ g$. Thus $f^-(\nu h) \leq_Q g(f^-(\nu h))$ by Galois, whence $f^-(\nu h) \leq_Q \hat{\nu} g$, which implies $\nu h \leq_P f^+(\hat{\nu} g)$ by Galois.

For the remaining claims, let $h \circ f^+ = f^+ \circ g$. If g is $\leq_Q$-isotone then $\hat{\nu} g = \nu g$, whence $f^+(\hat{\nu} g) = f^+(g(\hat{\nu} g)) = h(f^+(\hat{\nu} g))$, thus $f^+(\hat{\nu} g) \leq_P \nu h$. Finally $\hat{\nu} g \leq_Q g(\hat{\nu} g)$ implies $f^+(\hat{\nu} g) \leq_P f^+(g(\hat{\nu} g)) = h(f^+(\hat{\nu} g))$ since f^+ is order-preserving by Galois, whence if $\hat{\nu} h$ exists then $f^+(\hat{\nu} g) \leq_P \hat{\nu} h = \nu h$ by $\leq_P$-isotony of h. □

Theorem 16. *Let $f, g : S \to S$ be such that f and g are $\leq$-isotone, g is $\sqsubseteq$-isotone and $f \sqsubseteq g$. Assume that νf, ξf, $\hat{\mu} g$, $\hat{\nu} g$ and ξg exist and $\xi g 0 \leq \xi f 0$. Assume that the functions $(\curlywedge \mathsf{H})$ and $(+\mathsf{L})$ form a Galois connection. Then $\nu f \sqsubseteq \nu g$. If additionally $\hat{\nu} f$ exists, then $\hat{\nu} f \sqsubseteq \hat{\nu} g$.*

Proof. We obtain $f(x + \mathsf{L}) \leq g(x) + \mathsf{L}$ by Lemma 8 using $f \sqsubseteq g$ and $\sqsubseteq$-isotony of g. Hence $\nu f \leq \hat{\nu} g + \mathsf{L}$ by the ν-fusion of Lemma 15 using the Galois connection and $\leq$-isotony of f. Therefore $\nu f \leq \hat{\nu} g + \nu f 0$ by Lemma 12.

By $\leq$-isotony of g we get $\mu g = \hat{\mu} g$ and $\nu g = \hat{\nu} g$; moreover ξg exists. Hence Proposition 2 yields $\nu g \leq \mu g + d(\nu g 0)\top$ and $\xi g 0 = \nu g 0$ using $\leq$- and $\sqsubseteq$-isotony of g. Thus $\nu g 0 = \xi g 0 \leq \xi f 0 \leq \nu f 0$, while $\hat{\mu} g \leq \nu f + d(\nu f 0)\top$ follows since $g(\nu f + d(\nu f 0)\top) \leq f(\nu f) + d(f(\nu f)0)\top = \nu f + d(\nu f 0)\top$ by Lemma 8. Together $\nu g \leq \nu f + d(\nu f 0)\top$, whence $\nu f \sqsubseteq \nu g$.

If additionally $\hat{\nu} f$ exists, then $\hat{\nu} f = \nu f$, whence $\hat{\nu} f \sqsubseteq \hat{\nu} g$. □

To infer the missing $\xi g 0 \leq \xi f 0$ we use $\sqsubseteq$-isotony of ξ. We thus obtain $\sqsubseteq$-isotony for $\hat{\nu}$ and ν.

Corollary 17. *Assume the conditions of Theorem 13 and let $f, g : S \to S$ be $\leq$- and $\sqsubseteq$-isotone such that $f \sqsubseteq g$. Then $\hat{\nu} f \sqsubseteq \hat{\nu} g$ and $\nu f \sqsubseteq \nu g$.*

PROOF. Since $(S, \leq)$ is complete and f is $\leq$-isotone, $\hat{\mu}f = \mu f$ exists by Proposition 4 applied to the order $\leq$. Since $(S, \sqsubseteq)$ is complete by Theorem 13 and f is $\sqsubseteq$-isotone, $\hat{\xi}f = \xi f$ exists by Proposition 4. We now show that $\hat{\nu}f$ exists.

Let $D =_{\text{def}} \{x \mid x \leq f(x)\}$ be the set of postfixpoints of f: it is $\leq$-directed since $0 \in D$ and for $x, y \in D$ we have $x \leq f(x) \leq f(x+y)$ and $y \leq f(y) \leq f(x+y)$ by $\leq$-isotony of f, whence $x + y \leq f(x+y)$, thus $x + y \in D$ is the least upper bound of x and y in D. Hence $\sup_{\leq} D$ exists. For each $x \in D$ we obtain $x \leq f(x) \leq f(\sup_{\leq} D)$ by $\leq$-isotony of f, whence $\sup_{\leq} D \leq f(\sup_{\leq} D)$, thus $\sup_{\leq} D \in D$ is the greatest postfixpoint $\hat{\nu}f$ of f. By $\leq$-isotony of f, it is the greatest fixpoint, too.

In the same way we get that $\hat{\mu}g = \mu g$ and $\hat{\nu}g = \nu g$ and $\hat{\xi}g = \xi g$ exist. Moreover $\xi f \sqsubseteq \xi g$ by Corollary 14, hence $\xi g 0 \leq (\xi f + d(\xi f 0)\top)0 = \xi f 0 + d(\xi f 0)\mathsf{L} = \xi f 0$ by (L1). Thus $\nu f \sqsubseteq \nu g$ and $\hat{\nu}f \sqsubseteq \hat{\nu}g$ by Theorem 16. □

The existence of greatest postfixpoints in the previous result can also be obtained by [31, Corollary 5] if the Axiom of Choice is assumed.

3.6. While-Loops

We now look at the specific recursion describing while-loops: the semantics of $\mathsf{while}\ p\ \mathsf{do}\ y$ is the $\sqsubseteq$-least fixpoint of the function $\lambda x.d(p)yx + a(p)$. Consider the more general function $f : S \to S$ given by $f(x) = yx + z$ for arbitrary programs $y, z \in S$. The $\leq$-least and $\leq$-greatest fixpoints of f are represented using the Kleene star and omega operations [29, 8].

The omega operation describes infinite iterations. Together with the Kleene star for finite iterations it is axiomatised in [33] for semirings without the right zero law:

$$\begin{array}{ll} 1 + y^*y \leq y^* & z + xy \leq x \Rightarrow zy^* \leq x \\ 1 + yy^* \leq y^* & z + yx \leq x \Rightarrow y^*z \leq x \\ yy^\omega = y^\omega & x \leq yx + z \Rightarrow x \leq y^\omega + y^*z \end{array}$$

The operations * and $^\omega$ are $\leq$-isotone. Properties used below are $y^* = y^*y^* = (y^*y)^* = 1 + yy^*$ and $y^*0 \leq y^\omega 0$ and $y^\omega = y^*y^\omega = (y^*y)^\omega = y^\omega\top$ and $(x+y)^\omega = (x^*y)^\omega + (x^*y)^*x^\omega$.

A particular consequence of the above axioms is that $\mu f = \hat{\mu}f = y^*z$ and $\nu f = \hat{\nu}f = y^\omega + y^*z$. By Proposition 2 we have $\xi f = \nu f 0 + \mu f = y^\omega 0 + y^*z$. Using the combined iteration operation $y^\circ =_{\text{def}} y^\omega 0 + y^*$ we thus obtain the semantics of while-loops as $\xi f = y^\circ z$. The Kleene star and the combined iteration are $\sqsubseteq$-isotone [24, Theorem 6]. To show $\sqsubseteq$-isotony of omega, we can invoke Theorem 16 or Corollary 17 using the extra assumptions of a Galois connection or completeness, as required. However, a proof without these assumptions can be given, similarly to [25, Theorem 6].

Theorem 18. *Assume the above axioms hold in S and let $x, y \in S$ such that $x \sqsubseteq y$. Then $x^\omega \sqsubseteq y^\omega$.*

PROOF. From $x \sqsubseteq y$ we obtain $x \leq y + x0$ and $y \leq x + d(x0)\top$ and $x^* \sqsubseteq y^*$, whence $y^* \leq x^* + d(x^*0)\top$. The latter implies $y^*x0 \leq (x^* + d(x^*0)\top)x0 \leq x^*0 + d(x^*0)\mathsf{L} = x^*0$ by (L1). Therefore,

$$x^\omega \leq (y + x0)^\omega = (y^*x0)^\omega + (y^*x0)^*y^\omega = y^*x0 + y^\omega \leq y^\omega + x^*0 \leq y^\omega + x^\omega 0 \,.$$

Moreover,

$$\begin{array}{l} y^\omega \leq (x + d(x0)\top)^\omega = (x^*d(x0)\top)^\omega + (x^*d(x0)\top)^*x^\omega = x^*d(x0)\top(x^*d(x0)\top)^\omega + x^\omega + x^*d(x0)\top x^\omega \\ \quad \leq x^\omega + x^*d(x0)\top \leq x^\omega + d(x^*x0)\top \leq x^\omega + d(x^*0)\top \leq x^\omega + d(x^\omega 0)\top \,. \end{array}$$

Together we obtain $x^\omega \sqsubseteq y^\omega$. □

We conclude by several properties of these operators similar to the Kleene star axioms, but with respect to $\sqsubseteq$. From [24, Lemma 5] we know $1 + y^\circ y = 1 + yy^\circ = y^\circ$.

Theorem 19. *Assume the above axioms hold in S and let $x, y, z \in S$. Then*

$$\begin{aligned} xy \sqsubseteq x &\Rightarrow x(y+1) \sqsubseteq x \Rightarrow xy^\circ \sqsubseteq xy^* \sqsubseteq x \\ yx \sqsubseteq x &\Rightarrow (y+1)x \sqsubseteq x \Rightarrow y^\circ x \sqsubseteq y^* x \sqsubseteq x \\ z + yx \sqsubseteq x &\Rightarrow y^\circ z \sqsubseteq x \end{aligned}$$

Proof. Since $x \leq x(y+1)$ we obtain that $x(y+1) \sqsubseteq x$ is equivalent to $x(y+1) = xy+x \leq x+xy0$, and hence to $xy \leq x+xy0$. But this follows from $xy \sqsubseteq x$ and implies $x+(x+xy^*0)y = x+xy+xy^*0 = x+xy^*0$, thus $xy^* \leq x+xy^*0$ and $xy^\circ = xy^\omega 0+xy^* \leq xy^\circ 0+xy^*$. Moreover $x \leq xy^*+d(xy^*0)\top$ and $xy^* \leq xy^\circ+d(xy^\circ 0)\top$ since $1 \leq y^* \leq y^\circ$. Together we obtain $xy^\circ \sqsubseteq xy^* \sqsubseteq x$.

Symmetrically, $(y+1)x \sqsubseteq x$ is equivalent to $yx \leq x + yx0$, which follows from $yx \sqsubseteq x$ and implies $x+y(x+y^*x0) = x+yx+yy^*x0 \leq x+y^*x0$, thus $y^*x \leq x+y^*x0$ and $y^\circ x = y^\omega 0+y^*x \leq y^\circ x0+y^*x$. Again $x \leq y^*x + d(y^*x0)\top$ and $y^*x \leq y^\circ x + d(y^\circ x0)\top$ since $1 \leq y^* \leq y^\circ$. Together we obtain $y^\circ x \sqsubseteq y^*x \sqsubseteq x$.

For the final claim assume $z+yx \sqsubseteq x$. Then $x \leq z+yx+d((z+yx)0)\top = yx+z+d(z0+yx0)\top$, whence $x \leq y^\omega + y^*(z + d(z0+yx0)\top)$. But this implies $x0 \leq y^\omega 0 + y^*(z0 + d(z0+yx0)\mathsf{L}) = y^\omega 0 + y^*z0 + y^*yx0$ by (L1), whence $x0 \leq (y^*y)^\omega + (y^*y)^*(y^\omega 0 + y^*z0) = y^\omega + y^*y^\omega 0 + y^*y^*z0 = y^\omega + y^*z0$. Continuing the previous calculation,

$$\begin{aligned} x &\leq y^\omega + y^*(z + d(z0 + y(y^\omega + y^*z0))\top) = y^\omega + y^*z + y^*d(y^\omega + y^*z0)\top \\ &= y^\omega + y^*z + d(y^\omega)\top + d(y^*z0)\top = y^\omega 0 + y^*z + d(y^\omega 0)\top + d(y^*z0)\top = y^\circ z + d(y^\circ z0)\top \end{aligned}$$

since $y^*d(y^\omega + y^*z0)\top \leq d(y^*(y^\omega + y^*z0))\top = d(y^\omega + y^*z0)\top = d(y^\omega)\top + d(y^*z0)\top$ and $y^\omega + d(y^\omega)\top = d(y^\omega)\top = d(y^\omega d(\mathsf{L}))\top = d(y^\omega \mathsf{L})\top = d(y^\omega 0)\top = y^\omega 0 + d(y^\omega 0)\top$ by (L2).

Moreover $z+yx \leq x+(z+yx)0 = x+z0+y(x0)0 \leq x+z0+y(y^\omega+y^*z0)0 = x+y^\omega 0+y^*z0 = x+y^\circ z0$ by the assumption, whence also $z + y(x + y^\circ z0) = z + yx + yy^\circ z0 \leq x + y^\circ z0$. Therefore $y^*z \leq x + y^\circ z0$ and hence $y^\circ z \leq x + y^\circ z0$. Together, $y^\circ z \sqsubseteq x$. □

The last claim shows that $\hat{\xi} f = y^\circ z$ holds, too. On the other hand, $z + xy \sqsubseteq x$ implies neither $zy^* \sqsubseteq x$ nor $zy^\circ \sqsubseteq x$ in general, as the counterexample $x = y = 1$ and $z = 0$ shows, which also refutes $z + yx \sqsubseteq x \Rightarrow y^*z \sqsubseteq x$. Observe that again operations axiomatised with respect to the natural order $\leq$, namely $+$, $\cdot$, *, $^\omega$ and $^\circ$, are used in inequalities with respect to the other order $\sqsubseteq$.

4. Fixpoints in Distributive Lattices

In this section we investigate what can be derived about general correctness in a lattice-based setting, disregarding the operations of sequential composition $\cdot$ and (anti)domain. Hence we abandon the axioms of the previous section, and introduce new ones. Observe that also the new axioms abstract from the model discussed in Section 2.

A distributive lattice is a structure $(S, +, \curlywedge)$ satisfying the following axioms:

$$\begin{aligned} x + x &= x & x \curlywedge x &= x \\ x + y &= y + x & x \curlywedge y &= y \curlywedge x \\ x + (y + z) &= (x + y) + z & x \curlywedge (y \curlywedge z) &= (x \curlywedge y) \curlywedge z \\ x + (x \curlywedge y) &= x & x \curlywedge (x + y) &= x \\ x + (y \curlywedge z) &= (x + y) \curlywedge (x + z) & x \curlywedge (y + z) &= (x \curlywedge y) + (x \curlywedge z) \end{aligned}$$

Reduced axiom sets are discussed in [2]. As usual, the natural order is $x \leq y \Leftrightarrow_{\mathrm{def}} x + y = y$. It follows that $+$ and $\curlywedge$ are $\leq$-isotone. Again, the operation $+$ represents non-deterministic choice, $\curlywedge$ represents conjunction and $\leq$ refinement.

The ternary median operation is $(x, y, z) =_{\mathrm{def}} (x \curlywedge y) + (y \curlywedge z) + (z \curlywedge x)$, see [21, 3, 2]. It is self-dual and a collection of its symmetries is given in [28]. The median operation is relevant to program semantics because it induces an order that is a superset of the Egli-Milner order, as we show in Section 5. By investigating the median operation, we can thus obtain results about general correctness.

4.1. Pointed Distributive Lattices

We are interested in an instance of the median operation as [28]. Fix an element $\mathsf{L} \in S$, and define the operation $x \sqcap y =_{\text{def}} (\mathsf{L}, x, y) = (\mathsf{L} \curlywedge x) + (x \curlywedge y) + (y \curlywedge \mathsf{L})$ and the relation $x \sqsubseteq y \Leftrightarrow_{\text{def}} x = x \sqcap y$. The following properties can be derived automatically, for example, by using Prover9.

Proposition 20. *$(S, \sqcap, \mathsf{L})$ is a meet-semilattice (associative, commutative and idempotent) partially ordered by $\sqsubseteq$ with least element L. The operations $+$, $\curlywedge$ and $\sqcap$ distribute over each other. The two orders of S satisfy $x \leq y \Leftrightarrow x \curlywedge \mathsf{L} \leq y \wedge x \leq y + \mathsf{L}$ and $x \sqsubseteq y \Leftrightarrow y \curlywedge \mathsf{L} \leq x \leq y + \mathsf{L}$. If $x \leq y$ then $x \sqcap y = (y \curlywedge \mathsf{L}) + x = y \curlywedge (\mathsf{L} + x)$.*

We write $y \curlywedge \mathsf{L} + x$ whenever this is not ambiguous. The preceding characterisation of $\sqsubseteq$ is used frequently in this section. For the difference between a join- and a meet-semilattice, see [2]. In particular, $\sqsubseteq$ need not be uniquely characterised as a partial order with isotone operation $\sqcap$ and least element L.

The above construction works for an arbitrary element $\mathsf{L} \in S$. In Section 5 we establish the connection to general correctness by choosing L as in Section 3, representing the program that contains only non-terminating executions. This choice is evident because both the semiring- and the lattice-based settings are abstractions of the same model, as discussed in Section 2.

Several properties related to isotony are shown by the following lemma. In particular, they can be used to weaken the isotony requirements for showing the existence of fixpoints. Condition (8) also appears in the proof of Lemma 8.

Lemma 21. *Let $f : S \to S$ and consider the following statements, each universally quantified:*

$$\begin{array}{lll}
(1) & f(y) \curlywedge \mathsf{L} \leq f((y \curlywedge \mathsf{L}) + x) & f(x \curlywedge (y + \mathsf{L})) \leq f(y) + \mathsf{L} \quad (5) \\
(2) & f(y) \curlywedge \mathsf{L} \leq f((y \curlywedge \mathsf{L}) + (x \curlywedge (y + \mathsf{L}))) & f(((\mathsf{L} \curlywedge y) + x) \curlywedge (y + \mathsf{L})) \leq f(y) + \mathsf{L} \quad (6) \\
(3) & f(y) \curlywedge \mathsf{L} \leq f((y \curlywedge \mathsf{L}) + (x \curlywedge y)) & f((y + x) \curlywedge (y + \mathsf{L})) \leq f(y) + \mathsf{L} \quad (7) \\
(4) & f(y) \curlywedge \mathsf{L} \leq f(y \curlywedge \mathsf{L}) & f(y + \mathsf{L}) \leq f(y) + \mathsf{L} \quad (8)
\end{array}$$

Then (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) and (5) $\Rightarrow$ (6) $\Rightarrow$ (7) $\Rightarrow$ (8). If f is $\leq$-isotone, then (4) $\Rightarrow$ (1) and (8) $\Rightarrow$ (5). If (1) and (5) hold, then f is $\leq$-isotone. Finally, f is $\sqsubseteq$-isotone if and only if (2) and (6) hold.

Proof. The six implications of the first claim arise by substituting $x \curlywedge (y + \mathsf{L})$, $x \curlywedge y$, L, $(\mathsf{L} \curlywedge y) + x$, $x + y$ and L, respectively, for the unique occurrence of x in each antecedent. The second claim is immediate by $\leq$-isotony of f. For the third claim we use Proposition 20 to rewrite $\leq$-isotony of f, that is, $x \leq y \Rightarrow f(x) \leq f(y)$ as

$$x \curlywedge \mathsf{L} \leq y \wedge x \leq y + \mathsf{L} \Rightarrow f(x) \curlywedge \mathsf{L} \leq f(y) \wedge f(x) \leq f(y) + \mathsf{L} \,.$$

Separating the conjunctions, this clearly follows from the two implications

$$(x \curlywedge \mathsf{L} \leq y \Rightarrow f(x) \curlywedge \mathsf{L} \leq f(y)) \wedge (x \leq y + \mathsf{L} \Rightarrow f(x) \leq f(y) + \mathsf{L}) \,.$$

But these are recognised as instances of (1) and (5), respectively.

For the fourth claim observe that the arguments of f on the right hand side of (2) and on the left hand side of (6) are both $x \sqcap y$, the latter by self-duality of the median operation. Hence the conjunction of (2) and (6) is equivalent to $f(y) \curlywedge \mathsf{L} \leq f(x \sqcap y) \leq f(y) + \mathsf{L}$. By Proposition 20 this is equivalent to $f(x \sqcap y) \sqsubseteq f(y)$, which is a way to state $\sqsubseteq$-isotony of f. □

4.2. Fixpoints in Pointed Distributive Lattices

In the following we give representations of (pre)fixpoints in the above setting of a distributive lattice with a fixed element L. We reuse the notation for fixpoints introduced in Section 3:

$$\begin{array}{llll}
f(\xi f) = \xi f & f(x) = x \Rightarrow \xi f \sqsubseteq x & f(\hat{\xi} f) \sqsubseteq \hat{\xi} f & f(x) \sqsubseteq x \Rightarrow \hat{\xi} f \sqsubseteq x \\
f(\mu f) = \mu f & f(x) = x \Rightarrow \mu f \leq x & f(\hat{\mu} f) \leq \hat{\mu} f & f(x) \leq x \Rightarrow \hat{\mu} f \leq x \\
f(\nu f) = \nu f & f(x) = x \Rightarrow \nu f \geq x & f(\hat{\nu} f) \geq \hat{\nu} f & f(x) \geq x \Rightarrow \hat{\nu} f \geq x
\end{array}$$

If μf, νf and ξf exist, then clearly $\xi f \sqsubseteq \mu f$ and $\xi f \sqsubseteq \nu f$, whence $\xi f \sqsubseteq \mu f \sqcap \nu f$. The following result forces equality provided the fixpoints exist; a part of it is proved in the setting of bilattices in [19].

Lemma 22. *Let $f : S \to S$ and assume that μf and νf exist. Then $\mu f \sqcap \nu f = \nu f \curlywedge \mathsf{L} + \mu f \sqsubseteq x$ for every fixpoint $x = f(x) \in S$. Hence if ξf exists, then $\xi f = \mu f \sqcap \nu f = \nu f \curlywedge \mathsf{L} + \mu f$.*

Analogous statements hold with $\hat{\mu} f$ replacing μf, or $\hat{\nu} f$ replacing νf.

Proof. We only reason for the case that μf and νf exist; the same argument applies to the other three combinations. Let $f(x) = x$, then $\mu f \leq x \leq \nu f$, whence $x \curlywedge \mathsf{L} \leq \nu f \curlywedge \mathsf{L} \leq \nu f \curlywedge \mathsf{L} + \mu f \leq \mathsf{L} + \mu f \leq x + \mathsf{L}$ and therefore $\nu f \curlywedge \mathsf{L} + \mu f \sqsubseteq x$ by Proposition 20. Moreover $\mu f \sqcap \nu f = \nu f \curlywedge \mathsf{L} + \mu f$ by Proposition 20. □

We thus obtain a representation of $\sqsubseteq$-least fixpoints by fixpoints with respect to $\leq$. The following results extend this to $\sqsubseteq$-least prefixpoints and give conditions for the existence of the (pre)fixpoints. They should be compared with Theorem 6. As in the semiring-based setting, the representations are useful for general correctness because the refinement order $\leq$ is simpler.

Theorem 23. *Let $f : S \to S$ satisfy conditions* (3) *and* (7) *of Lemma 21. If $\hat{\mu} f \leq \hat{\nu} f$, then $\hat{\xi} f = \hat{\mu} f \sqcap \hat{\nu} f = \hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f$. If additionally f is $\sqsubseteq$-isotone and μf and νf exist, then $\xi f = \mu f \sqcap \nu f = \nu f \curlywedge \mathsf{L} + \mu f$.*

Proof. By Proposition 20 we obtain $\hat{\mu} f \sqcap \hat{\nu} f = \hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f$ since $\hat{\mu} f \leq \hat{\nu} f$. Using conditions (3) and (7) in the central steps we obtain

$$(\hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f) \curlywedge \mathsf{L} = \hat{\nu} f \curlywedge \mathsf{L} \leq f(\hat{\nu} f) \curlywedge \mathsf{L} \leq f(\hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f) \leq f(\hat{\mu} f) + \mathsf{L} \leq \hat{\mu} f + \mathsf{L} = (\hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f) + \mathsf{L}\,,$$

and hence $f(\hat{\mu} f \sqcap \hat{\nu} f) \sqsubseteq \hat{\mu} f \sqcap \hat{\nu} f$ by Proposition 20.

Let $f(x) \sqsubseteq x$, then $x \curlywedge \mathsf{L} \leq f(x) \leq x + \mathsf{L}$ by Proposition 20. By conditions (4) and (8) of Lemma 21 we obtain $x \curlywedge \mathsf{L} \leq f(x) \curlywedge \mathsf{L} \leq f(x \curlywedge \mathsf{L})$ and $f(x + \mathsf{L}) \leq f(x) + \mathsf{L} \leq x + \mathsf{L}$, hence $x \curlywedge \mathsf{L} \leq \hat{\nu} f$ and $\hat{\mu} f \leq x + \mathsf{L}$. But this implies $x \curlywedge \mathsf{L} \leq \hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f \leq x + \mathsf{L}$, whence $\hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f \sqsubseteq x$ by Proposition 20.

If f is $\sqsubseteq$-isotone, then $\xi f = \hat{\xi} f$, whence the remaining claim follows by Lemma 22. □

The assumption $\hat{\mu} f \leq \hat{\nu} f$ of the preceding theorem is in particular satisfied if $\hat{\mu} f$ and $\hat{\nu} f$ exist and f has a fixpoint. Without assuming the existence of $\hat{\mu} f$ and $\hat{\nu} f$ we have to use both $\leq$- and $\sqsubseteq$-isotony as the following result shows.

Theorem 24. *Let $f : S \to S$ be $\leq$- and $\sqsubseteq$-isotone. If μf and νf exist, then $\xi f = \mu f \sqcap \nu f = \nu f \curlywedge \mathsf{L} + \mu f$.*

Proof. Since $\mu f \leq \nu f$ we obtain $\mu f \sqcap \nu f = \nu f \curlywedge \mathsf{L} + \mu f$ by Proposition 20, and hence $\mu f \leq \mu f \sqcap \nu f \leq \nu f$. By $\sqsubseteq$-isotony of f we have $f(\mu f \sqcap \nu f) \sqsubseteq f(\mu f) = \mu f$ and $f(\mu f \sqcap \nu f) \sqsubseteq f(\nu f) = \nu f$, whence $f(\mu f \sqcap \nu f) \sqsubseteq \mu f \sqcap \nu f$. The converse inequality follows by Proposition 20 since

$$f(\mu f \sqcap \nu f) \curlywedge \mathsf{L} \leq f(\nu f) \curlywedge \mathsf{L} = \nu f \curlywedge \mathsf{L} \leq \nu f \curlywedge \mathsf{L} + \mu f \leq \mu f + \mathsf{L} = f(\mu f) + \mathsf{L} \leq f(\mu f \sqcap \nu f) + \mathsf{L}$$

using $\leq$-isotony of f. Thus $\mu f \sqcap \nu f$ is a fixpoint of f. Hence it is the $\sqsubseteq$-least by Lemma 22. □

The representation $\xi f = \mu f \sqcap \nu f$ is shown already in [18, Theorem 7.7] for finite distributive bilattices. A distributive bilattice is a set S with two partial orders that both induce a complete lattice on S in which all meets and joins distribute over each other. In other contexts related to logic programming, bilattices are assumed to have a negation operation [20]. By [28, Lemma 1.2] every bounded (and hence every complete or even finite) distributive bilattice arises via the construction of Section 4.1 using the median operation. Theorems 23 and 24 do not assume bounds on S or the existence of the $\sqsubseteq$-least (pre)fixpoints.

4.3. Bounded Distributive Lattices

Further structure is obtained by assuming bounds in $(S, \leq)$ and a complement of L, or one of the equivalent conditions of the following theorem. A lattice $(S, +, \curlywedge)$ is bounded if it has a least element 0 and a greatest element $\top$, equivalently $x + 0 = x = x \curlywedge \top$ for each $x \in S$. The least upper bound of $x, y \in S$ with respect to $\sqsubseteq$ is denoted by $x \sqcup y$, provided it exists.

Theorem 25. *The following are equivalent, and* H *is the same in all cases:*

1. $\forall x \in S : x \sqsubseteq \mathsf{H}$*, that is,* H *is the* $\sqsubseteq$*-greatest element.*
2. $\forall x \in S : 0 \leq x \leq \top \wedge \mathsf{H} = 0 \sqcup \top$*, that is,* $\leq$ *is bounded by* 0 *and* $\top$ *whose* $\sqsubseteq$*-join is* H*.*
3. $\forall x \in S : \mathsf{H} \curlywedge \mathsf{L} = 0 \leq x \leq \top = \mathsf{H} + \mathsf{L}$*, that is,* $\leq$ *is bounded by* 0 *and* $\top$*, and* H *and* L *are complements.*
4. $\forall x, y \in S : x \curlywedge \mathsf{L} \leq y \Leftrightarrow x \leq y + \mathsf{H}$*, that is, the functions* $(\curlywedge \mathsf{L})$ *and* $(+\mathsf{H})$ *form a Galois connection.*
5. $\forall x, y \in S : x \curlywedge \mathsf{H} \leq y \Leftrightarrow x \leq y + \mathsf{L}$*, that is, the functions* $(\curlywedge \mathsf{H})$ *and* $(+\mathsf{L})$ *form a Galois connection.*

Proof. We repeatedly apply Proposition 20 for the first two equivalences.

Thus $x \sqsubseteq \mathsf{H}$ is equivalent to $\mathsf{H} \curlywedge \mathsf{L} \leq x \leq \mathsf{H} + \mathsf{L}$, which shows (1) $\Leftrightarrow$ (3).

Assume (3), then $0 \sqsubseteq \mathsf{H}$ since $\mathsf{H} \curlywedge \mathsf{L} \leq 0 \leq \mathsf{H} + \mathsf{L}$, and $\top \sqsubseteq \mathsf{H}$ since $\mathsf{H} \curlywedge \mathsf{L} \leq \top \leq \mathsf{H} + \mathsf{L}$, and $0 \sqsubseteq x$ and $\top \sqsubseteq x$ imply $x \curlywedge \mathsf{L} \leq 0 \leq \mathsf{H} \leq \top \leq x + \mathsf{L}$ and hence $\mathsf{H} \sqsubseteq x$; thus $\mathsf{H} = 0 \sqcup \top$. On the other hand, (2) implies $0 \sqsubseteq \mathsf{H}$ and $\top \sqsubseteq \mathsf{H}$, whence $\mathsf{H} \curlywedge \mathsf{L} \leq 0$ and $\top \leq \mathsf{H} + \mathsf{L}$. Together we obtain (2) $\Leftrightarrow$ (3).

Assume (3), then $x \leq x + \mathsf{H} = (x + \mathsf{H}) \curlywedge (\mathsf{L} + \mathsf{H}) = (x \curlywedge \mathsf{L}) + \mathsf{H}$ and similarly $x \leq (x \curlywedge \mathsf{H}) + \mathsf{L}$, and $(y + \mathsf{H}) \curlywedge \mathsf{L} = (y \curlywedge \mathsf{L}) + (\mathsf{H} \curlywedge \mathsf{L}) = y \curlywedge \mathsf{L} \leq y$ and similarly $(y + \mathsf{L}) \curlywedge \mathsf{H} \leq y$. The Galois connections follow by [9, Lemma 7.26] using $\leq$-isotony of $\curlywedge$ and $+$.

On the other hand, $\mathsf{H} \curlywedge \mathsf{L} \leq y$ is implied by $\mathsf{H} \leq y + \mathsf{H}$ or $\mathsf{L} \leq y + \mathsf{L}$ using either Galois connection, and similarly $x \leq \mathsf{L} + \mathsf{H}$ is implied by $x \curlywedge \mathsf{L} \leq \mathsf{L}$ or $x \curlywedge \mathsf{H} \leq \mathsf{H}$. Together we obtain (4) $\Leftrightarrow$ (3) $\Leftrightarrow$ (5). □

The Galois connection (5) is used in Theorem 13.

If $(S, \leq)$ is bounded by 0 and $\top$ we obtain a number of connections between the available operations even without assuming the existence of H. Thus $(\sqcap 0) = (\curlywedge \mathsf{L})$ since $x \sqcap 0 = (\mathsf{L} \curlywedge x) + (x \curlywedge 0) + (0 \curlywedge \mathsf{L}) = \mathsf{L} \curlywedge x$, and $(\sqcap \top) = (+\mathsf{L})$ since $x \sqcap \top = (\mathsf{L} \curlywedge x) + (x \curlywedge \top) + (\top \curlywedge \mathsf{L}) = x + \mathsf{L}$. From either fact $\mathsf{L} = 0 \sqcap \top$ follows.

But much more can be said with H. The following result is mentioned by [3] and elaborated in [27, 28] based on condition (3) of Theorem 25.

Proposition 26. *Assume one of the conditions* (1)–(5) *stated in Theorem 25. Then* $(S, \sqcup, \mathsf{L}, \sqcap, \mathsf{H})$ *is a bounded distributive lattice where* $x \sqcup y = (\mathsf{H}, x, y) = (\mathsf{H} \curlywedge x) + (x \curlywedge y) + (y \curlywedge \mathsf{H})$*.*

Moreover [27, 28] add that 0 and $\top$ are complements in the induced lattice, the operations $+$, $\curlywedge$, $\sqcup$ and $\sqcap$ distribute over each other, and the original bounded distributive lattice is recovered by applying the same construction again. This shows a symmetry between the operations and orders, which is not available in the semiring-based setting. Particular results about the semantics of programs may thus be easier derived in the lattice-based setting and, using the link in Section 5, interpreted in a general correctness model based on the Egli-Milner order.

4.4. Isotony of Fixpoint Operators

Isotony of the pre- and postfixpoint operators is less difficult to establish in the present setting of bounded distributive lattices. The following result should be compared with Theorems 7 and 9 and Corollaries 14 and 17.

Theorem 27. *Let* $f, g : S \to S$*.*

1. *The operators* $\hat{\mu}$ *and* $\hat{\nu}$ *preserve* $\leq$ *and the operator* $\hat{\xi}$ *preserves* $\sqsubseteq$*.*
2. *If* $f \leq g$ *and* f *and* g *are* $\sqsubseteq$*-isotone and* $\hat{\mu} f \leq \hat{\nu} f$ *and* $\hat{\mu} g \leq \hat{\nu} g$*, then* $\hat{\xi} f \leq \hat{\xi} g$*.*
3. *Assume one of the conditions* (1)–(5) *stated in Theorem 25. Assume that* $f \sqsubseteq g$*, that* f *is* $\leq$*-isotone and that* f *or* g *is* $\sqsubseteq$*-isotone. If* $\hat{\mu} f$ *and* $\hat{\mu} g$ *exist, then* $\hat{\mu} f \sqsubseteq \hat{\mu} g$*. If* $\hat{\nu} f$ *and* $\hat{\nu} g$ *exist, then* $\hat{\nu} f \sqsubseteq \hat{\nu} g$*.*

Proof. Claim (1) is standard [9, Rule 8.28].

For claim (2) apply Theorem 23 to obtain $\hat{\xi} f = \hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f \leq \hat{\nu} g \curlywedge \mathsf{L} + \hat{\mu} g = \hat{\xi} g$ since $\hat{\mu} f \leq \hat{\mu} g$ and $\hat{\nu} f \leq \hat{\nu} g$ by claim (1).

For claim (3), let $f \sqsubseteq g$, whence $g(x) \curlywedge \mathsf{L} \leq f(x) \leq g(x) + \mathsf{L}$ for each $x \in S$ by Proposition 20. Then $g(x) \curlywedge \mathsf{L} \leq f(x \curlywedge \mathsf{L})$ and $f(x + \mathsf{L}) \leq g(x) + \mathsf{L}$ follow according to

$$\begin{array}{ccc} g(x) \curlywedge \mathsf{L} & \leq & g(x \curlywedge \mathsf{L}) \curlywedge \mathsf{L} \\ \mid\!\wedge & & \mid\!\wedge \\ f(x) \curlywedge \mathsf{L} & \leq & f(x \curlywedge \mathsf{L}) \end{array} \qquad \begin{array}{ccc} f(x + \mathsf{L}) & \leq & f(x) + \mathsf{L} \\ \mid\!\wedge & & \mid\!\wedge \\ g(x + \mathsf{L}) + \mathsf{L} & \leq & g(x) + \mathsf{L} \end{array}$$

by conditions (4) and (8) of Lemma 21 using $\sqsubseteq$-isotony of f or g. Thus $\hat{\nu}g \curlywedge \mathsf{L} \leq g(\hat{\nu}g) \curlywedge \mathsf{L} \leq f(\hat{\nu}g \curlywedge \mathsf{L})$, whence $\hat{\nu}g \curlywedge \mathsf{L} \leq \hat{\nu}f$. Moreover $\hat{\nu}f \leq \hat{\nu}g + \mathsf{L}$ by the ν-fusion of Lemma 15 using $\leq$-isotony of f and the Galois connection (5) of Theorem 25. Hence $\hat{\nu}f \sqsubseteq \hat{\nu}g$ by Proposition 20.

Furthermore $f(\hat{\mu}g + \mathsf{L}) \leq g(\hat{\mu}g) + \mathsf{L} \leq \hat{\mu}g + \mathsf{L}$, whence $\hat{\mu}f \leq \hat{\mu}g + \mathsf{L}$. Also $\hat{\mu}g \curlywedge \mathsf{L} \leq \hat{\mu}f$ by μ-fusion, that is, the dual of Lemma 15 using the Galois connection (4) of Theorem 25. Hence $\hat{\mu}f \sqsubseteq \hat{\mu}g$ by Proposition 20. □

Similar claims can be made for the fixpoint operators. A particular difference to Section 3 is that due to Theorems 23 and 24 it is not necessary to invoke completeness of $(S, \sqsubseteq)$. Conditions for completeness of this induced lattice are described in [28].

4.5. Greatest Fixpoints

Since the induced structure is a lattice, it makes sense to talk about $\sqsubseteq$-greatest (post)fixpoints, too. Let $f : S \to S$, then the $\sqsubseteq$-greatest fixpoint of and the $\sqsubseteq$-greatest postfixpoint $\hat{o}f$ are given by

$$f(of) = of \qquad f(x) = x \Rightarrow of \sqsupseteq x \qquad\qquad f(\hat{o}f) \sqsupseteq \hat{o}f \qquad f(x) \sqsupseteq x \Rightarrow \hat{o}f \sqsupseteq x$$

The following result corresponds to Theorem 23.

Corollary 28. *Assume one of the conditions* (1)–(5) *stated in Theorem 25. Let $f : S \to S$ satisfy conditions* (3) *and* (7) *of Lemma 21. If $\hat{\mu}f \leq \hat{\nu}f$, then $\hat{o}f = \hat{\mu}f \sqcup \hat{\nu}f = \hat{\nu}f \curlywedge \mathsf{H} + \hat{\mu}f$. If additionally f is $\sqsubseteq$-isotone and μf and νf exist, then $of = \mu f \sqcup \nu f = \nu f \curlywedge \mathsf{H} + \mu f$.*

Proof. According to Proposition 26 the $\sqcup$ operation is obtained by replacing L with H in the definition of $\sqcap$. Moreover the induced bounded distributive lattice satisfies $x = x \sqcap y \Leftrightarrow y = x \sqcup y$. Hence starting the construction of Section 4.1 with H instead of L and applying Proposition 26 gives the dual lattice, with swapped join and meet, and the converse order $\sqsupseteq$. But greatest (post)fixpoints in the dual lattice are least (pre)fixpoints in the original lattice. Therefore all claims follow by Theorem 23, provided we can adapt the conditions (3) and (7) of Lemma 21. Recall these conditions and replace L with H to obtain (3′) and (7′):

$$\begin{array}{lll} (3) & f(y) \curlywedge \mathsf{L} \leq f(y \curlywedge (\mathsf{L} + x)) & f(y + (x \curlywedge \mathsf{L})) \leq f(y) + \mathsf{L} \quad (7) \\ (3') & f(y) \curlywedge \mathsf{H} \leq f(y \curlywedge (\mathsf{H} + x)) & f(y + (x \curlywedge \mathsf{H})) \leq f(y) + \mathsf{H} \quad (7') \end{array}$$

Again, each statement is universally quantified. To show (3) $\Leftrightarrow$ (7′), consider the Galois connected version of (7′), namely $f(y + (x \curlywedge \mathsf{H})) \curlywedge \mathsf{L} \leq f(y)$. It follows from (3) by

$$f(y + (x \curlywedge \mathsf{H})) \curlywedge \mathsf{L} \leq f((y + (x \curlywedge \mathsf{H})) \curlywedge (\mathsf{L} + y)) = f(y + (x \curlywedge \mathsf{H} \curlywedge \mathsf{L})) = f(y + 0) = f(y) \,,$$

and it implies (3) by

$$f(y) \curlywedge \mathsf{L} = f(y \curlywedge \top) \curlywedge \mathsf{L} = f(y \curlywedge (\mathsf{L} + x + \mathsf{H})) \curlywedge \mathsf{L} = f((y \curlywedge (\mathsf{L} + x)) + (y \curlywedge \mathsf{H})) \curlywedge \mathsf{L} \leq f(y \curlywedge (\mathsf{L} + x)) \,.$$

Similarly (7) $\Leftrightarrow$ (3′) can be shown. □

On the other hand, analogous equivalences for the conditions (4) and (8) of Lemma 21 do not hold: for example, $\forall y : f(y) \curlywedge \mathsf{L} \leq f(y \curlywedge \mathsf{L})$ does not imply $\forall y : f(y + \mathsf{H}) \leq f(y) + \mathsf{H}$ as a counterexample generated by Mace4 shows. Note that also the preceding corollary does not rely on the existence of the $\sqsubseteq$-greatest (post)fixpoints; otherwise we find $of = \mu f \sqcup \nu f$ in the bilattice setting in [18, 19].

By the construction in the proof, also Theorems 24 and 27 can be extended to greatest (post)fixpoints. Moreover, since the original lattice is recovered by applying Proposition 26 again, we immediately obtain $\hat{\mu}f = \hat{\xi}f \curlywedge \hat{o}f$ and $\hat{\nu}f = \hat{\xi}f + \hat{o}f$. Both can also be shown directly by

$$\begin{aligned} \hat{\xi}f \curlywedge \hat{o}f &= (\hat{\nu}f \curlywedge \mathsf{L} + \hat{\mu}f) \curlywedge (\hat{\nu}f \curlywedge \mathsf{H} + \hat{\mu}f) = (\hat{\nu}f \curlywedge \mathsf{L} \curlywedge \hat{\nu}f \curlywedge \mathsf{H}) + \hat{\mu}f = 0 + \hat{\mu}f = \hat{\mu}f \,, \\ \hat{\xi}f + \hat{o}f &= (\hat{\nu}f \curlywedge \mathsf{L} + \hat{\mu}f) + (\hat{\nu}f \curlywedge \mathsf{H} + \hat{\mu}f) = (\hat{\nu}f \curlywedge (\mathsf{L} + \mathsf{H})) + \hat{\mu}f = \hat{\nu}f + \hat{\mu}f = \hat{\nu}f \,. \end{aligned}$$

5. Linking Semirings and Distributive Lattices

In this section we use a technique of [7] to apply the results obtained in the lattice-based setting to our theory of general correctness described in Section 3.

The following result to transfer fixpoints between partial orders is based on [7, Proposition 2]; we prove a generalisation that decouples the existence of the involved fixpoints and separates prefixpoints and fixpoints. Consider a set P with two partial orders $\leq_1$ and $\leq_2$, and a function $f : P \to P$. Denote the least fixpoints of f with respect to $\leq_1$ and $\leq_2$ by μ_1 and μ_2, the least prefixpoints by $\hat{\mu}_1$ and $\hat{\mu}_2$, respectively.

Lemma 29. *Assume $\leq_1 \subseteq \leq_2$. If μ_1 exists, then μ_2 exists and $\mu_1 = \mu_2$. If $\hat{\mu}_1$ and $\hat{\mu}_2 = \mu_2$ exist, then μ_1 exists and $\mu_1 = \hat{\mu}_1 = \hat{\mu}_2$.*

Proof. If μ_1 exists, then $f(\mu_1) = \mu_1$ and $f(x) = x \Rightarrow \mu_1 \leq_1 x \Rightarrow \mu_1 \leq_2 x$, thus μ_1 is the least fixpoint μ_2 of f with respect to $\leq_2$.

If $\hat{\mu}_1$ and $\hat{\mu}_2 = \mu_2$ exist, then $f(\hat{\mu}_2) = f(\mu_2) = \mu_2 = \hat{\mu}_2 \Rightarrow \hat{\mu}_1 \leq_1 \hat{\mu}_2 \Rightarrow \hat{\mu}_1 \leq_2 \hat{\mu}_2$. Furthermore $f(\hat{\mu}_1) \leq_1 \hat{\mu}_1 \Rightarrow f(\hat{\mu}_1) \leq_2 \hat{\mu}_1 \Rightarrow \hat{\mu}_2 \leq_2 \hat{\mu}_1$. Together $\hat{\mu}_1 = \hat{\mu}_2$, whence $f(\hat{\mu}_1) = f(\hat{\mu}_2) = \hat{\mu}_2 = \hat{\mu}_1$. But clearly $f(x) = x \Rightarrow \hat{\mu}_1 \leq_1 x$, thus $\hat{\mu}_1$ is the least fixpoint μ_1 of f with respect to $\leq_1$. □

To link the semiring- and the lattice-based settings, we denote by $\sqsubseteq'$ the Egli-Milner order of Section 3 and keep $\sqsubseteq$ for the order induced by Proposition 20 in Section 4. The following result shows that $\sqsubseteq'$ is a subset of $\sqsubseteq$, whence Lemma 29 applies.

Theorem 30. *Assume a structure S which is both a distributive lattice $(S, +, \curlywedge)$ and a bounded antidomain semiring $(S, +, 0, \cdot, 1, a, \top)$ without the right zero law. Let $\mathsf{L} = \top 0$ satisfy (L1). Then $\sqsubseteq' \subseteq \sqsubseteq$.*

Proof. We have $d(x0)\top \curlywedge \mathsf{L} = d(d(x0)\top \curlywedge \mathsf{L})(d(x0)\top \curlywedge \mathsf{L}) \leq d(d(x0)\top)\mathsf{L} = d(x0)d(\top)\mathsf{L} = d(x0)\mathsf{L} = x0$ by (L1). Let $x \sqsubseteq' y$, then $x \leq y + x0 \leq y + \mathsf{L}$ and $y \leq x + d(x0)\top$, which implies

$$y \curlywedge \mathsf{L} \leq (x + d(x0)\top) \curlywedge \mathsf{L} = (x \curlywedge \mathsf{L}) + (d(x0)\top \curlywedge \mathsf{L}) \leq x + x0 = x$$

by (L1). Together $y \curlywedge \mathsf{L} \leq x \leq y + \mathsf{L}$, whence $x \sqsubseteq y$ by Proposition 20. □

The following application of this result shows how the representations of (pre)fixpoints derived for the induced order $\sqsubseteq$ in the lattice-based setting can be transferred to the Egli-Milner order of the semiring-based setting. Denote by $\xi' f$ and $\hat{\xi}' f$ the $\sqsubseteq'$-least (pre)fixpoints of the function f.

Corollary 31. *Assume the conditions of Theorem 30 and let $f : S \to S$.*

1. *If f is $\leq$- and $\sqsubseteq'$-isotone and μf, νf and $\xi' f$ exist, then $\xi' f = \nu f 0 + \mu f = \nu f \curlywedge \mathsf{L} + \mu f$.*
2. *If f is $\sqsubseteq$-isotone and $\hat{\mu} f \leq \hat{\nu} f$ and $\hat{\xi}' f$ exists, then $\xi' f = \hat{\xi}' f = \hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f$.*

Proof. For the first claim, Lemma 29 yields $\xi' f = \xi f$ since $\sqsubseteq' \subseteq \sqsubseteq$ by Theorem 30. Hence $\xi f = \nu f \curlywedge \mathsf{L} + \mu f$ by Lemma 22. But $\xi' f = \nu f 0 + \mu f$ by Proposition 2.

For the second claim we get $\hat{\xi} f = \hat{\nu} f \curlywedge \mathsf{L} + \hat{\mu} f$ by Theorem 23. But $\hat{\xi} f = \xi f$ since f is $\sqsubseteq$-isotone, whence $\xi' f = \hat{\xi}' f = \hat{\xi} f$ by Lemma 29 again using Theorem 30. □

As regards the first claim we remark that while $x0 = x \curlywedge \mathsf{L}$ holds in the model of Section 2, it does not follow in the assumed structure as a counterexample generated by Mace4 shows. Note also that the decoupled existence of Lemma 29 spares us the use of Theorem 24 which would require $\sqsubseteq$-isotony, too.

Although $\sqsubseteq'$ and $\sqsubseteq$ are closely related, they are not identical: for example, $0 \sqsubseteq \mathsf{H}$ holds but $0 \sqsubseteq' \mathsf{H}$ does not hold. It can be shown that in the setting of Section 4 it is not possible to define the Egli-Milner order $x \sqsubseteq' y$ by a finite conjunction of inequalities $f_i(x, y) \leq g_i(x, y)$ with terms $f_i(x, y)$ and $g_i(x, y)$ composed only of the lattice operations $+$ and $\curlywedge$ and arbitrary constants.

6. Conclusion

We describe the relation to particular instances of the above structures found in the literature and translate between the used notations, and finally draw some conclusions. By $\sqcap$ the operator of Section 4 is meant, while $\sqsubseteq'$ again denotes the Egli-Milner order of Section 3.

Our orders $\leq$, $\sqsubseteq'$ and $\sqsubseteq$ correspond to the orders $\subseteq_1$, $\preceq$ and $\leq$ of [13]. That work proposes a semantics for recursive programs composed of operators which are not necessarily isotone with respect to the Egli-Milner order. Programs are described as pairs of relations describing state transition and termination information, see also [35, 30, 34]. To validate the semantics, it is then proved that for Egli-Milner-isotone constructs the result is in fact the least fixpoint with respect to both $\sqsubseteq$ and $\sqsubseteq'$. Our operations $\sqcap$, $\curlywedge$, $+$ and $\sqcup$ are listed in this sequence in [13, Section 4.4]. The first two are dismissed, $+$ is the usual non-deterministic choice, and $\sqcup$ is called 'fair choice' and further investigated; it motivates the above semantics because $\sqcup$ is not $\sqsubseteq'$-isotone. Our constants 0, L, H, $\top$, 1 and $\mathsf{L}+1$ are listed in this sequence in [13, Section 4.1] and in [35, Table II].

Our orders $\leq$, $\sqsubseteq'$ and $\sqsubseteq$ correspond to the orders $\subseteq$, $\sqsubseteq_\varepsilon$ and $\sqsubseteq_\pi$ of [7]. That work is also motivated by operations which are not Egli-Milner-isotone, in this case for parallel composition. A technique is devised to obtain least fixpoints with respect to another order $\sqsubseteq_\lambda$. It is the lexicographic order of the pairs of state transition and termination information and, being a superset of our $\sqsubseteq$ and hence $\sqsubseteq'$, motivates Lemma 29. Least fixpoints with respect to $\sqsubseteq_\lambda$ are reduced to $\leq$-least and $\leq$-greatest fixpoints as in our work, but the obtained representation nests these fixpoint operators. The assumptions made for this reduction [7, Theorem 4] are a complete lattice, $\leq$-isotony, complemented elements L and H, and condition (8) of Lemma 21. Our operations $+$ and $\curlywedge$ are considered, but not $\sqcap$ and $\sqcup$ since the focus is on the order $\sqsubseteq_\lambda$. Our constants 0, L, H and $\top$ are denoted by $\top$, $\lhd$, $\rhd$ and $\bot$ in [7].

Our operations $+$, $\sqcap$, $\curlywedge$ and $\sqcup$ correspond to demonic choice $[]$, fusion $\odot$, join $\Diamond$ and concert $\#$ of [15], which discusses their uses. The concert operator in particular also appears in [16, 17].

The first conclusion is that even beyond [23, 24] many properties of general correctness can be derived from a small basis of first-order axioms. On the other hand, Sections 3.4 and 3.5 provide two examples which apparently require completeness. We shall therefore inspect this boundary and see whether its interior can be enlarged by modifying the axiomatisation.

The second conclusion is that we can learn about general correctness by investigating orders related to the Egli-Milner order. This is in line with the results of [13, 7]. It is also worthwhile to look at the associated meet and join operations, as shown by the case of the fair choice/concert operator.

Acknowledgement

I thank Georg Struth for helpful discussions and the anonymous referees for valuable comments.

This work was supported by a fellowship within the Postdoc-Programme of the German Academic Exchange Service (DAAD).

References

[1] R. Berghammer, H. Ehler, and B. Möller. On the refinement of non-deterministic recursive routines by transformations. In M. Broy and C. B. Jones, editors, *Programming Concepts and Methods*, pages 53–71. North-Holland Publishing Company, 1990.

[2] G. Birkhoff. *Lattice Theory*, volume XXV of *Colloquium Publications*. American Mathematical Society, third edition, 1967.

[3] G. Birkhoff and S. A. Kiss. A ternary operation in distributive lattices. *Bulletin of the American Mathematical Society*, 53(8):749–752, 1947.

[4] M. Broy. A theory for nondeterminism, parallelism, communication, and concurrency. *Theoretical Computer Science*, 45:1–61, 1986.

[5] M. Broy and G. Nelson. Adding fair choice to Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems*, 16(3):924–938, May 1994.

[6] R. M. Burstall and J. Darlington. A transformation system for developing recursive programs. *Journal of the ACM*, 24(1):44–67, January 1977.

[7] Y. Chen. A fixpoint theory for non-monotonic parallelism. *Theoretical Computer Science*, 308(1–3):367–392, November 2003.

[8] E. Cohen. Separation and reduction. In R. Backhouse and J. N. Oliveira, editors, *Mathematics of Program Construction*, volume 1837 of *Lecture Notes in Computer Science*, pages 45–59. Springer-Verlag, 2000.
[9] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, second edition, 2002.
[10] J. Desharnais, B. Möller, and F. Tchier. Kleene under a modal demonic star. *Journal of Logic and Algebraic Programming*, 66(2):127–160, February–March 2006.
[11] J. Desharnais and G. Struth. Domain axioms for a family of near-semirings. In J. Meseguer and G. Roşu, editors, *Algebraic Methodology and Software Technology*, volume 5140 of *Lecture Notes in Computer Science*, pages 330–345. Springer-Verlag, 2008.
[12] J. Desharnais and G. Struth. Internal axioms for domain semirings. *Science of Computer Programming*, 76(3):181–203, March 2011.
[13] H. Doornbos. A relational model of programs without the restriction to Egli-Milner-monotone constructs. In E.-R. Olderog, editor, *Programming Concepts, Methods and Calculi*, pages 363–382. North-Holland Publishing Company, 1994.
[14] 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.
[15] S. Dunne. Junctive compositions of specifications in total and general correctness. In J. Derrick, E. Boiten, J. Woodcock, and J. von Wright, editors, *Proceedings of the BCS FACS Refinement Workshop REFINE 2002*, volume 70, Issue 3 of *Electronic Notes in Theoretical Computer Science*, pages 4–20. Elsevier B.V., November 2002.
[16] S. Dunne, A. Galloway, and W. Stoddart. Specification and refinement in general correctness. In A. Evans, D. Duke, and A. Clark, editors, *Proceedings of the 3rd BCS-FACS Northern Formal Methods Workshop*, Electronic Workshops in Computing. The British Computer Society, September 1998.
[17] S. Dunne, I. Hayes, and A. Galloway. Reasoning about loops in total and general correctness. In A. Butterfield, editor, *Second International Symposium on Unifying Theories of Programming*, volume 5713 of *Lecture Notes in Computer Science*, pages 62–81. Springer-Verlag, 2010.
[18] M. Fitting. Bilattices and the semantics of logic programming. *Journal of Logic Programming*, 11(2):91–116, August 1991.
[19] M. Fitting. Bilattices: A survey. Presentation given at the DIMACS Workshop on Applications of Lattices and Ordered Sets to Computer Science, available online at http://dimacs.rutgers.edu/Workshops/Lattices/slides/Fitting2.pdf, July 2003.
[20] M. L. Ginsberg. Multivalued logics: a uniform approach to reasoning in artificial intelligence. *Computational Intelligence*, 4(3):265–316, September 1988.
[21] A. A. Grau. Ternary Boolean algebra. *Bulletin of the American Mathematical Society*, 53(6):567–572, 1947.
[22] T. F. Gritzner and R. Berghammer. A relation algebraic model of robust correctness. *Theoretical Computer Science*, 159(2):245–270, June 1996.
[23] W. Guttmann. General correctness algebra. In R. Berghammer, A. M. Jaoua, and B. Möller, editors, *Relations and Kleene Algebra in Computer Science*, volume 5827 of *Lecture Notes in Computer Science*, pages 150–165. Springer-Verlag, 2009.
[24] W. Guttmann. Partial, total and general correctness. In C. Bolduc, J. Desharnais, and B. Ktari, editors, *Mathematics of Program Construction*, volume 6120 of *Lecture Notes in Computer Science*, pages 157–177. Springer-Verlag, 2010.
[25] W. Guttmann. Unifying recursion in partial, total and general correctness. In S. Qin, editor, *Unifying Theories of Programming, Third International Symposium, UTP 2010*, volume 6445 of *Lecture Notes in Computer Science*, pages 207–225. Springer-Verlag, 2010.
[26] D. Jacobs and D. Gries. General correctness: A unification of partial and total correctness. *Acta Informatica*, 22(1):67–83, April 1985.
[27] A. Jung and M. A. Moshier. A Hofmann-Mislove theorem for bitopological spaces. *Journal of Logic and Algebraic Programming*, 76(2):161–174, July–August 2008.
[28] O. Klinke. On the 90-degree-lemma. Technical report, University of Birmingham, October 2008. http://epapers.bham.ac.uk/53/.
[29] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, May 1994.
[30] R. D. Maddux. Relation-algebraic semantics. *Theoretical Computer Science*, 160(1–2):1–85, June 1996.
[31] G. Markowsky. Chain-complete posets and directed sets with applications. *Algebra Universalis*, 6(1):53–68, 1976.
[32] B. Möller. The linear algebra of UTP. In T. Uustalu, editor, *Mathematics of Program Construction*, volume 4014 of *Lecture Notes in Computer Science*, pages 338–358. Springer-Verlag, 2006.
[33] B. Möller. Kleene getting lazy. *Science of Computer Programming*, 65(2):195–214, March 2007.
[34] 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 *Lecture Notes in Computer Science*, pages 200–211. Springer-Verlag, 2006.
[35] G. Nelson. A generalization of Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems*, 11(4):517–561, October 1989.
[36] G. Schmidt and T. Ströhlein. *Relationen und Graphen*. Springer-Verlag, 1989.