Refining Ideal Behaviours

Bernhard Möller

Report Nr. 345 1995

Refining Ideal Behaviours[1]

Bernhard Möller

Institut für Mathematik, Universität Augsburg, D-86135 Augsburg, Germany,
e-mail: moeller@uni-augsburg.de

1 Introduction

1.1 Objectives

This paper provides some mathematical properties of *behaviours* of systems, where the individual elements of a behaviour are modeled by *ideals* of a suitable partial order. It is well-known that the associated ideal completion [8] provides a simple way of constructing algebraic cpos. An ideal can be viewed as a set of consistent finite or compact approximations of an object which itself may even be infinite.

We introduce a special way of characterising behaviours through sets of relevant approximations. This is a generalisation of the technique used in [12] for the case of streams. Given a set $P \subseteq M$ of a partial order $(M, \leq)$, we define

$$\mathsf{ide}\, P \overset{\text{def}}{=} \{Q^{\leq} : Q \subseteq P \text{ directed}\} ,$$

where $Q^{\leq} \overset{\text{def}}{=} \{x \in M : \exists\, y \in Q : x \leq y\}$ is the downward closure of Q. So $\mathsf{ide}\, P$ is the set of all ideals "spanned" by directed subsets of P. The elements in P may be regarded as finite "snapshots" of computations; the ideals in $\mathsf{ide}\, P$ are then the limits of such computations. They form the behaviour finitely described by P. Of course, other notions of finitary description would be possible, but we have found this one particularly useful.

Of particular interest are sets of infinite ideals (in a suitable sense of "infinite"), since they model non-terminating systems. These are singled out by the operator inf . The combination $\mathsf{inf}\,\mathsf{ide}\, P$ therefore describes the infinite computations characterized by "snapshots" in P. It is a generalization of the lim -operation

$$\mathsf{lim}\, W \overset{\text{def}}{=} \{x \in A^{\omega} : \mathrm{FP}(x) \cap W \text{ infinite}\}$$

that is used in the theory of ω-languages (see e.g. [21, 25, 26]) and was introduced in [9]. Here, $\mathrm{FP}(x)$ denotes the set of finite prefixes of x.

The context of this work is deductive program design, in which implementations are derived from specifications by semantics-preserving deduction rules. Examples of this paradigm are transformational program development (see e.g. [19, 4]) and the refinement calculus (see e.g. [2, 14, 15]). There is a growing conviction that this paradigm is most efficient when based on algebraic rather than purely logical frameworks. For sequential programs this is demonstrated in [4]. In the parallel case, to some extent the work reported in [18, 6] can be viewed as falling into the algebraic realm; purely algebraic approaches are presented in [11, 22]. All these are based on the particular domain of streams. The present paper abstracts from that and contributes

[1] This research was partially sponsored by Esprit Working Group 8533 NADA — New Hardware Design Methods

a number of distributivity and monotonicity laws for operators like ide and inf in general domains; these laws are useful in correct refinement of specifications into implementations.

It should be noted, however, that the use of these operators has its place more at the level of specifications; we are not defining semantics for an implementation language. For that reason we can afford to work with operators that have a strongly angelic aspect and, to some extent, abstract from the possibilities of deadlock or failure. We think that this is justified, because from the user's point of view a system "just should work"; it is the duty of the implementor to avoid deadlocks and failures.

1.2 A Small Example

As an example of the use of these constructs, we give a specification of a bounded buffer module in the particular domain $A^\infty = A^* \cup A^\omega$ of finite and infinite streams over a set A of atomic actions. The finite approximations there are the finite words, so $M = A^*$, and the approximation order $\leq$ is the prefix order. Then A^∞ is the ideal completion of M. In this particular domain, for a set $P \subseteq M = A^*$ of finite approximations, $\mathsf{ide}\, P$ is the set of finite and infinite streams that satisfy P in a relevant subset of their finite prefixes.

The buffer module has one input and one output port. In describing such modules, we choose the letters a for the action of inputting and b for outputting and set $A \stackrel{\text{def}}{=} \{a, b\}$. Boundedness of a module can be enforced by requiring the number of input actions to exceed the number of output actions by at most some $n \in \mathbb{N}$ which then is the capacity of the device. We denote by s_c the number of occurrences of $c \in A$ in $s \in A^*$. Generalising the above informal description slightly, we define, for $n \in \mathbb{Z}$ and $a, b \in A$, the set

$$\mathrm{X}^{ab}_n \stackrel{\text{def}}{=} \{s \in A^* : s_a \leq s_b + n\}$$

of finite approximations. Then $s \in \mathrm{X}^{ab}_n$ may be pronounced "a exceeds b by at most n in s". The specification is, however, very loose in that the balance between as and bs might be struck only at the very end of a word. For instance, $a^{k+n}b^k \in \mathrm{X}^n_{ab}$. So the restriction may be violated in prefixes and only established in the end. For bounded devices, this is not possible. They need a stronger specification. Therefore we define

$$\mathrm{B}^{ab}_n \stackrel{\text{def}}{=} \mathsf{saf}\, \mathrm{X}^{ab}_n$$

where $s \in \mathsf{saf}\, P$ means that P holds for all prefixes of s, too, i.e., enforces P as a safety condition.

Now $\mathsf{ide}\, \mathrm{B}^{ab}_n$ is the set of all finite and infinite streams that satisfy X^{ab}_n in all prefixes. However, we are interested in devices that work for an unbounded time. This is specified by taking as overall behaviour of such a device the set

$$\mathcal{B}^{ab}_n \stackrel{\text{def}}{=} \mathsf{inf}\, \mathsf{ide}\, \mathrm{B}^{ab}_n \ ,$$

where inf selects from a set of streams the infinite ones.

A buffer is a device in which the number of outputs must not exceed the number of inputs. Hence we define

$$\mathcal{BF}^{ab} \stackrel{\text{def}}{=} \mathcal{B}^{ba}_0 \ .$$

Note the reversal of the arguments in the superscript. The finitary property B^{ba}_0 spells out to $s_b \leq s_a$, as required. This describes an unbounded buffer. A bounded buffer of capacity n then is described by

$$\mathcal{BB}_n^{ab} \overset{\text{def}}{=} \mathcal{BF}^{ab} \cap \mathcal{B}_n^{ab} \ .$$

This specifies the set of all infinite streams for which in all finite prefixes, the number of outputs does not exceed the number of inputs and the number of inputs may exceed the number of outputs by at most n.

The example will be resumed briefly at the end of the paper to show how a calculation of an implementation from the specification using our laws proceeds.

1.3 Overview

Section 2 gives some order-theoretic definitions and properties. Then Section 3 lists some properties of directed sets. The central Section 4 then gives the relevant definitions for ideals and proves the algebraic laws. It turns out that a special property we call max-determinedness is an essential prerequisite for many of the laws. We give a brief characterization of domains that fulfill it; a consequence of it is that the base set over which the ideals are formed consists of compact elements only. This is, for instance, the case for the domain of finite and infinite words or streams, and Section 5 discusses that particular domain further in the light of the general results. Finally, in Section 6 the buffer example is resumed to sketch the actual use of the refinement laws.

2 Order-Theoretic Preliminaries

In this section we repeat some basic notions from the theory of partial orders and state some new algebraic properties. The proofs for this section are deferred to the Appendix.

For preordered set $(M, \leq)$ and $N \subseteq M$ we define the proper and improper downward closure by

$$N^< \overset{\text{def}}{=} \{y \in M : \exists\, x \in N : y < x\}$$
$$N^\leq \overset{\text{def}}{=} N \cup N^<$$

where $y < x \Leftrightarrow y \leq x \wedge \neg\, x \leq y$. If $\leq$ is even an order, then $N^\leq = \{y \in M : \exists\, x \in N : y \leq x\}$. We list some useful properties of these operations:

Lemma 2.1 *Consider $N, P \subseteq M$. Then*

1. $N \subseteq N^\leq \wedge (N^<)^< \subseteq N^<$.
2. $(N \cup P)^< = N^< \cup P^< \wedge (N \cup P)^\leq = N^\leq \cup P^\leq$ *(distributivity).*
3. $N \subseteq P \Rightarrow N^\leq \subseteq P^\leq \wedge N^< \subseteq P^<$ *(monotonicity).*
4. $(N^\leq)^< = N^< \wedge (N^\leq)^\leq = N^\leq$.

The set of **maximal** elements of $N \subseteq M$ is defined by

$$\mathsf{max}\, N \overset{\text{def}}{=} N \backslash N^< \ .$$

Again, we give some useful properties:

Lemma 2.2 *Consider $N, P \subseteq M$. Then*

1. $\mathsf{max}\, N = N^{\leq} \backslash N^{<}$.
2. $\mathsf{max}\, N = \mathsf{max}\, N^{\leq}$.
3. $N \subseteq P \Rightarrow N \cap \mathsf{max}\, P \subseteq \mathsf{max}\, N$.
4. $\mathsf{max}\,(N \cup P) = (\mathsf{max}\, N)\backslash P^{<} \cup (\mathsf{max}\, P)\backslash N^{<}$
5. $\mathsf{max}\, N \cap P^{<} = \emptyset \Rightarrow \mathsf{max}\,(N \cup P) = \mathsf{max}\, N \cup (\mathsf{max}\, P)\backslash N^{<}$.
6. $N \cap P^{<} = \emptyset \Rightarrow \mathsf{max}\,(N \cup P) = \mathsf{max}\, N \cup (\mathsf{max}\, P)\backslash N^{<}$.

We now extend the order $\leq$ to a relation on subsets of M by

$$N \leq P \overset{\text{def}}{\Leftrightarrow} N \subseteq P^{\leq} .$$

This is the angelic half of the Egli-Milner preorder [20]. In particular, $N^{\leq} \leq N$. Some further useful properties are

Lemma 2.3 *Consider $N, P \subseteq M$. Then*

1. $N \leq P \Leftrightarrow N \leq P^{\leq}$.
2. $L \subseteq N \wedge N \leq P \wedge P \subseteq Q \Rightarrow L \leq Q$.
3. $N \leq P \Leftrightarrow N^{\leq} \subseteq P^{\leq}$.
4. $N \leq P \Rightarrow N^{<} \subseteq P^{<}$.
5. $N \leq P \Rightarrow (N \cup P)^{\leq} = P^{\leq} \;\wedge\; (N \cup P)^{<} = P^{<}$.
6. $N \leq P \Rightarrow \mathsf{max}\,(N \cup P) = \mathsf{max}\, P$.
7. $N \leq P \wedge P \leq N \Rightarrow \mathsf{max}\, N = \mathsf{max}\, P$.
8. $N \leq P \wedge \mathsf{max}\, P = \emptyset \Rightarrow \mathsf{max}\,(N \cup P) = \emptyset$.

Since $\leq$ generally is only a preorder between sets, we are interested in the induced equivalence relation

$$N \sim P \overset{\text{def}}{\Leftrightarrow} N \leq P \wedge P \leq N .$$

For this we have

Lemma 2.4 *Consider $N, P \subseteq M$. Then $N \sim P \Leftrightarrow N^{\leq} = P^{\leq}$.*

Proof: Immediate from Lemma 2.3.3. □

A subset $N \subseteq M$ is a **cone** if it is downward closed, i.e., if $N^{\leq} \subseteq N$. Hence on cones $\leq$ and $\subseteq$ coincide; in particular, $\leq$ is a partial order on cones.

Since M is a cone and the intersection of cones is a cone again, the set of all cones forms a complete lattice under inclusion. It is isomorphic to the angelic or Hoare power domain [23] over $(M, \leq)$. However, we are not going to use that domain.

In the sequel we will define many functions on single points of M and lift them to subsets of M by *pointwise extension*, i.e., by setting, for $f : M \to M$ and $N \subseteq M$,

$$f(N) \overset{\text{def}}{=} \{f(x) : x \in N\} \ .$$

These pointwise extended functions distribute through arbitrary unions and hence are monotonic w.r.t. inclusion and strict w.r.t. $\emptyset$. We will also use this mechanism to lift these functions a further level to sets of subsets of M.

3 Directed Sets

A subset $N \subseteq M$ is **directed** if every finite subset of N has an upper bound in N. Equivalently, N is directed if $N \neq \emptyset$ and any two elements in N have a common upper bound in N. For $P \subseteq M$ we denote by $\mathsf{dir}\, P$ the set of all directed subsets of P. Note that the operation dir is monotonic w.r.t. inclusion.

We now study how directedness behaves under union and intersection.

Lemma 3.1 *Consider $N, P \subseteq M$. Then*

1. $N \cup P \in \mathsf{dir}\, M \ \Rightarrow\ N \leq P \ \vee\ P \leq N$.
2. $N \cup P \in \mathsf{dir}\, M \ \wedge\ N \leq P \ \Rightarrow\ P \in \mathsf{dir}\, M$.
3. $Q^{\leq} \in \mathsf{dir}\, M \ \Rightarrow\ Q \in \mathsf{dir}\, M$.
4. $N \cup P \in \mathsf{dir}\, M \ \wedge\ P = P^{\leq} \ \wedge\ N \cap P \ = \ \emptyset \ \Rightarrow\ P \leq N \ \wedge\ N \in \mathsf{dir}\, M$.
5. $N \cup P \in \mathsf{dir}\, M \ \Rightarrow\ N \in \mathsf{dir}\, M \ \vee\ P \in \mathsf{dir}\, M$.
6. $N \leq P \ \wedge\ P \in \mathsf{dir}\, M \ \Rightarrow\ N \cup P \in \mathsf{dir}\, M$.
7. $$\begin{aligned}\mathsf{dir}\,(N \cup P) \ = \ & \{K \cup L : (K \in \mathsf{dir}\, N \ \wedge\ L \subseteq P \ \wedge\ L \leq K)\} \ \cup \\ & \{K \cup L : (L \in \mathsf{dir}\, P \ \wedge\ K \subseteq N \ \wedge\ K \leq L)\} \ .\end{aligned}$$
8. $\mathsf{dir}\,(N \cup P) \ \supseteq\ \mathsf{dir}\, N \ \cup\ \mathsf{dir}\, P$.
9. $\mathsf{dir}\,(N \cap P) \ = \ \mathsf{dir}\, N \ \cap\ \mathsf{dir}\, P$.

Proof:

1. For $N = \emptyset$ or $P = \emptyset$ the claim is trivial. So consider $N, P \neq \emptyset$ and suppose $N \not\leq P$. Then there is $x \in N$ with $x \not\leq P$. Assume now $y \in P$. By directedness of $N \cup P$ there is a $z \in N \cup P$ with $x, y \leq z$. Since $x \not\leq P$, it follows that $z \in N \backslash P \subseteq N$. Since y was arbitrary, we have shown $P \leq N$.
2. Assume $x, y \in P$. By directedness of $N \cup P$ there is a $z \in N \cup P$ with $x \leq z$ and $y \leq z$. If $z \in P$, we are done. Otherwise, by $N \leq P$ there is a $u \in P$ with $z \leq u$ so that by transitivity also $x \leq u$ and $y \leq u$.
3. is immediate from 2 by setting $N = Q^{\leq}$, $P = Q$ and using $Q^{\leq} \leq Q$.
4. By $\emptyset = N \cap P = N \cap P^{\leq}$ we know $\neg\ N \leq P$, so that we may infer from 1 that $P \leq N$. Now 2 shows the claim.
5. is immediate from 1 and 2.

6. Assume $x, y \in N \cup P$. By $N \leq P$ and $P \leq P$ there are $u, v \in P$ with $x \leq u \wedge y \leq v$. Since P is directed, there is $z \in P$ with $u \leq z$ and $v \leq z$. Hence also $x \leq z$ and $y \leq z$ by transitivity.
7. We show ($\subseteq$); the reverse inclusion is immediate from 6.
   Consider $Q \in \mathsf{dir}\,(N \cup P)$. We have $Q = K \cup L$ where $K \overset{\text{def}}{=} Q \cap N$ and $L \overset{\text{def}}{=} Q \cap P$. By 1 we know $K \leq L \vee L \leq K$. If $K \leq L$ then $L \in \mathsf{dir}\, P$ by 2. If $L \leq K$ then $K \in \mathsf{dir}\, N$ by 2. This shows the claim.
8. is immediate both from the definition and monotonicity, but also follows by setting $L = \emptyset$ in the first summand and $K = \emptyset$ in the second one in 7.
9. We only need to show ($\supseteq$), since the reverse inclusion follows from monotonicity of dir . Assume $D \in \mathsf{dir}\, N \cap \mathsf{dir}\, P$. Then $D \subseteq N \wedge D \subseteq P$ and hence $D \subseteq N \cap P$. Since D is directed, also $D \in \mathsf{dir}\,(N \cap P)$.

□

4 Ideals and Behaviours

4.1 Ideals

An **ideal** of a partial order $(M, \leq)$ is a directed cone, i.e., a subset $Q \in \mathsf{dir}\, M$ with $Q^{\leq} \subseteq Q$. A **principal ideal** is an ideal of the form $x^{\leq}$ for some $x \in M$. By $I(M)$ we denote the set of all ideals of M.

To tie this in with domain-theoretic notions we recall the ideal completion (cf. e.g. [3, 8]). Consider an arbitrary ordered set $(M, \leq)$. By $\sqcup N$ we denote the set of least upper bounds of a subset $N \subseteq M$ in M; in case $\sqcup N$ is non-empty we identify it with its only element. Then $(M, \leq)$ is called **dir-complete** iff for every set $D \in \mathsf{dir}\, M$ we have $\sqcup D \neq \emptyset$. An element x of M is **compact** iff for every $D \in \mathsf{dir}\, M$ with $x \leq \sqcup D$ we have also $x \leq z$ for some $z \in D$. Equivalently, x is compact iff for every $I \in I(M)$ with $x \leq \sqcup I$ we have $x \in I$. $(M, \leq)$ is **algebraic** iff every element of M is the supremum of a directed set of compact elements. A non-compact element of M is then called a **limit point** or an **infinite element**. With these notions one has (see e.g. [8])

Theorem 4.1 *Let $(M, \leq)$ be an ordered set.*

1. *The set $(I(M), \subseteq)$ ordered by set inclusion is dir -complete and inductive, the compact elements being the ideals $x^{\leq}$ for $x \in M$. The mapping $\iota : x \mapsto x^{\leq}$ is an embedding of M into $I(M)$. In particular,*
$$x \leq y \Leftrightarrow x^{\leq} \subseteq y^{\leq} .$$
2. *For every monotonic mapping $h : M \to P$ into a dir -complete set $(P, \leq)$ there is a unique continuous mapping $\overline{h} : I(M) \to P$ extending h, i.e., with $\overline{h}(x^{\leq}) = h(x)$. $\overline{h}$ is given by $\overline{h}(I) = \sqcup\, h(I)$ for $I \in I(M)$; hence $\overline{h}(D^{\leq}) = \sqcup\, h(D)$ for $D \in \mathsf{dir}\, M$.*

The order $(I(M), \subseteq)$ is called the **ideal completion** of $(M, \leq)$.

4.2 Describing Ideals by Properties

We want to characterise ideals by certain sets of "relevant" approximations. Such a set, i.e., a subset of our overall partially ordered set M, is called a **property** in this connection.

For property $P \subseteq M$ we now define by

$$\mathsf{ide}\, P \overset{\text{def}}{=} \{D^{\leq} : D \in \mathsf{dir}\, P\}$$

the set of all ideals "spanned" by directed subsets of P. Note that $\mathsf{ide}\, M = I(M)$. For the case of finite and infinite sequences over some alphabet a related notion occurs in [9]; the connection will be made precise in Section 4.6. Note that ide is monotonic w.r.t. inclusion. A different characterisation of ide is given by

Lemma 4.2 *For $I \in I(M)$ and $Q \subseteq M$ the following statements are equivalent:*

1. $I \in \mathsf{ide}\, Q$.
2. $I \subseteq (I \cap Q)^{\leq}$.
3. $I = (I \cap Q)^{\leq}$.

Proof: The equivalence of 2 and 3 is obvious by monotonicity of $^{\leq}$ and downward closedness of I.
(1 ⇒ 2) Suppose $I = D^{\leq}$ for $D \in \mathsf{dir}\, Q$.

$$\begin{array}{ll} & I \\ = & \quad \{\!\![\text{ assumption }]\!\!\} \\ & D^{\leq} \\ = & \quad \{\!\![\text{ since } D \subseteq Q \ ]\!\!\} \\ & (D \cap Q)^{\leq} \\ \subseteq & \quad \{\!\![\text{ monotonicity }]\!\!\} \\ & (D^{\leq} \cap Q)^{\leq} \\ = & \quad \{\!\![\text{ assumption }]\!\!\} \\ & (I \cap Q)^{\leq} \ . \end{array}$$

(3 ⇒ 1) Since I is directed, so is $(I \cap Q)^{\leq}$. By Lemma 3.1.3 also $I \cap Q$ is directed and the claim follows. □

We say that an ideal $I \in I(M)$ **satisfies** property $P \subseteq M$ and write $I \models P$ iff $I \in \mathsf{ide}\, P$.

We have

Lemma 4.3 *1. $S \models Q \Rightarrow S \models Q^{\leq}$. The reverse implication is not valid.*

2. $S \models Q \wedge S \models P \Rightarrow S \models Q^{\leq} \cap P^{\leq}$.

Proof:
1. is immediate from $Q \subseteq Q^{\leq}$ and monotonicity of ide. For a counterexample to the reverse implication see Example 5.3.
2. immediate from 1.

□

4.3 Safety and Deadlock-Freedom

Two important correctness notions for parallel systems are safety and liveness [1, 10]. We want to show how they can be expressed algebraically.

Informally, a property P is called a safety property iff the following two conditions hold:

1. Whenever P is satisfied by some object then it also holds for all finite approximations of that object.
2. If P holds for all elements of a directed set of finite approximations then it also holds for their supremum.

Since the supremum of (the images of) a directed set of finite approximations in the ideal completion is that set, in our terminology $P \subseteq M$ is a **safety property** iff P is a cone in M. In this case

$$I \models P \Leftrightarrow I \subseteq P \; .$$

A property $\mathcal{Q} \subseteq I(M)$ is informally called a liveness property iff every finite approximation can be extended to an infinite one in $\mathcal{Q}$ [1]. We are in this paper interested in a more liberal form of liveness: we stay purely at the level of finite approximations and consider properties $Q \subseteq M$ such that every finite approximation in Q can be extended into an infinite object that satisfies Q. We call such properties **deadlock-free**. This definition reflects an angelic view: whenever there is a possibility to extend a finite behaviour, the overall behaviour will have the opportunity to choose it. Let us now give an algebraic characterisation.

Lemma 4.4 *Let $Q \subseteq M$ be a property with $Q \neq \emptyset$. Then every principal ideal in $\mathsf{ide}\, Q$ is contained in a non-compact ideal in $\mathsf{ide}\, Q$ iff $\mathsf{max}\, Q = \emptyset$.*

Proof: ($\Rightarrow$) Assume $x \in \mathsf{max}\, Q$. By assumption there is some non-compact ideal $I \in \mathsf{ide}\, Q$ with $x^{\leq} \subseteq I$. Consider an arbitrary $y \in I$. By directedness of I there is $z \in I$ with $x, y \leq z$. Since $I \in \mathsf{ide}\, Q$ there is $u \in Q$ with $z \leq u$. But maximality of x in Q implies $u = x$. This shows $I \leq x$ and hence $I = x^{\leq}$, so that I is compact. Contradiction!

($\Leftarrow$) Consider $x \in Q$ and $\mathcal{I} \overset{\text{def}}{=} \{I \in \mathsf{ide}\, Q : x^{\leq} \subseteq I\}$. Then $\mathcal{I}$ is non-empty. Moreover, every chain $\mathcal{C} \subseteq \mathcal{I}$ has an upper bound in $\mathcal{I}$, viz. $\bigcup \mathcal{C}$. By Zorn's Lemma therefore $\mathcal{I}$ contains a maximal element J. Suppose J is compact. Then $J = y^{\leq}$ for some $y \in M$. We show that y then is maximal in Q, a contradiction. Consider $z \in Q$ with $y \leq z$. Then $z^{\leq} \in \mathsf{ide}\, Q$ and $J \subseteq z^{\leq}$. By maximality of J we get $J = z^{\leq}$ and hence also $z = y$. □

Therefore we call Q **deadlock-free** iff $Q \neq \emptyset \wedge \mathsf{max}\, Q = \emptyset$. This property will be the premise for a number of the laws to come. An investigation of the general notion of liveness in order-theoretic terms will be the subject of subsequent papers.

4.4 Continual Satisfaction

In connection with safety issues one is interested in the set of all objects that satisfy a property also in all their finite approximations. Given a property $P \subseteq M$ we define the property $\mathsf{saf}\, P$ by

$$\mathsf{saf}\, P \overset{\text{def}}{=} \{x \in M : x^{\leq} \subseteq P\} \; .$$

Lemma 4.5 *1.* $\mathsf{saf}\,P \subseteq P$.

2. $\mathsf{saf}\,P = P$ *iff* P *is a safety property.*

3. $\mathsf{saf}\,P$ *is the greatest safety property contained in* P.

4. saf *is monotonic and strict w.r.t.* $\emptyset$.

5. $\mathsf{saf}\,(P \cap Q) = \mathsf{saf}\,P \cap \mathsf{saf}\,Q$.

Proof: 1.

$$\begin{array}{ll} & x \in \mathsf{saf}\,P \\ \Leftrightarrow & \quad \{[\ \text{definition}\ ]\} \\ & x^{\leq} \subseteq P \\ \Rightarrow & \quad \{[\ x \in x^{\leq}\ ]\} \\ & x \in P\ . \end{array}$$

2. $(\Rightarrow)$

$$\begin{array}{ll} & x \in P \\ \Leftrightarrow & \quad \{[\ \text{assumption}\ ]\} \\ & x \in \mathsf{saf}\,P \\ \Leftrightarrow & \quad \{[\ \text{definition}\ ]\} \\ & x^{\leq} \subseteq P\ . \end{array}$$

$(\Leftarrow)$

$$\begin{array}{ll} & x \in P \\ \Rightarrow & \quad \{[\ \text{assumption}\ ]\} \\ & x^{\leq} \subseteq P \\ \Leftrightarrow & \quad \{[\ \text{definition}\ ]\} \\ & x \in \mathsf{saf}\,P \end{array}$$

so $P \subseteq \mathsf{saf}\,P$; the reverse inclusion was shown in 1.

3. It is obvious that $\mathsf{saf}\,P$ is a safety property. Let $Q \subseteq P$ be a safety property and $x \in Q$. By definition then $x^{\leq} \subseteq Q \subseteq P$ and hence $x \in \mathsf{saf}\,P$.

4. is immediate from the definition.

5.

$$\begin{array}{ll} & x \in \mathsf{saf}\,(P \cap Q) \\ \Leftrightarrow & \quad \{[\ \text{definition}\ ]\} \\ & x^{\leq} \subseteq P \cap Q \\ \Leftrightarrow & \quad \{[\ \text{infimum property of intersection}\ ]\} \\ & x^{\leq} \subseteq P \wedge x^{\leq} \subseteq Q \\ \Leftrightarrow & \quad \{[\ \text{definition}\ ]\} \\ & x \in \mathsf{saf}\,P \wedge x \in \mathsf{saf}\,Q\ . \end{array}$$

□

Note that saf does not distribute through union. We can now state two distributivity properties for ide:

Lemma 4.6 *Consider $N, P \subseteq M$. Then*

1. $\mathsf{ide}\,(N \cup P) = \mathsf{ide}\,N \cup \mathsf{ide}\,P$.
2. $N = \mathsf{saf}\,N \Rightarrow \mathsf{ide}\,(N \cap P) = \mathsf{ide}\,N \cap \mathsf{ide}\,P$.

Proof: 1.

$$\begin{array}{ll} & I \in \mathsf{ide}\,(N \cup P) \\ \Leftrightarrow & \quad \{\!\![\text{ by Lemma 4.2 }]\!\!\} \\ & I = (S \cap (N \cup P))^{\le} \\ \Leftrightarrow & \quad \{\!\![\text{ distributivity of } \cap \text{ over } \cup \text{ and Lemma 2.1.2 }]\!\!\} \\ & I = (S \cap N)^{\le} \cup (S \cap P)^{\le} \\ \Rightarrow & \quad \{\!\![\text{ by directedness of } I\text{, Lemma 3.1.1 and Lemma 2.3.3 }]\!\!\} \\ & I = (S \cap N)^{\le} \vee I = (S \cap P)^{\le} \\ \Leftrightarrow & \quad \{\!\![\text{ by Lemma 4.2 }]\!\!\} \\ & I \in \mathsf{ide}\,N \vee I \in \mathsf{ide}\,P \ . \end{array}$$

The reverse inclusion follows by monotonicity of ide.
Another proof can be given using Lemma 3.1.7.

2. We only need to show ($\supseteq$), since the reverse inclusion follows from monotonicity of ide.
Assume $S \in \mathsf{ide}\,N \cap \mathsf{ide}\,P$, say $S = D^{\le} = E^{\le}$ with $D \in \mathsf{dir}\,N \wedge E \in \mathsf{dir}\,P$. By Lemma 2.4 then $E \le D$, and by Lemma 2.3.2 we get $E \le N$, since $D \subseteq N$. Now $N = N^{\le}$ shows $E \subseteq N$. Since $E \subseteq P$ we get $E \subseteq N \cap P$ and, since E is directed, even $E \in \mathsf{dir}\,(N \cap P)$. This shows $S = E^{\le} \in \mathsf{ide}\,(N \cap P)$.

□

This also shows once again the monotonicity of ide. However, we have even

Corollary 4.7 $N \subseteq P \Leftrightarrow \mathsf{ide}\,N \subseteq \mathsf{ide}\,P$.

Proof: The inclusion from right to left is part of Theorem 4.1.1. □

We can restate 1 and 2 in terms of the satisfaction relation:

$$\begin{array}{rcl} & & I \models (N \cup P) \ \Leftrightarrow \ I \models N \vee I \models P \ , \\ N = \mathsf{saf}\,N & \Rightarrow & I \models (N \cap P) \ \Leftrightarrow \ I \models N \wedge I \models P \ . \end{array}$$

It should be noted, however, that ide only distributes through finite unions and hence is not "continuous". For an instance of this see Example 5.4.

4.5 Behaviours and Refinement

Our application of ideals will be the description of systems. To model non-determinacy, we define a **behaviour** to be a set of ideals. As our refinement relation we choose inclusion, i.e., behaviour $\mathcal{T}$ **refines** behaviour $\mathcal{S}$ if $\mathcal{T} \subseteq \mathcal{S}$. For instance, given a property $P \subseteq M$, the set $\mathsf{ide}\,P$ of ideals satisfying P, is a behaviour. To allow correct local refinements one therefore has to ensure monotonicity of all operations w.r.t. inclusion.

For comparing behaviours, however, we also use a second relation which, contrary to the "global" view of inclusion allows a "local" view of the ideals involved. We define, more generally, for sets $\mathcal{S}, \mathcal{T} \subseteq \mathsf{dir}\, M$,

$$\mathcal{S} \leq \mathcal{T} \overset{\text{def}}{\Leftrightarrow} \mathcal{S} \subseteq \mathcal{T}^{\leq}$$

with

$$\begin{array}{rcl} \mathcal{T}^{<} & \overset{\text{def}}{=} & \{D \in \mathsf{dir}\, M : \exists\, E \in \mathcal{T} : D < E\} \ , \\ \mathcal{T}^{\leq} & \overset{\text{def}}{=} & \mathcal{T} \cup \mathcal{T}^{<} \ , \\ D < E & \overset{\text{def}}{\Leftrightarrow} & D \leq E \wedge \neg\, E \leq D \ . \end{array}$$

So $\leq$ is the extension of the preorder $\leq$ between directed sets to sets of directed sets in the sense of Section 2. Recall that between cones and hence ideals $\leq$ coincides with $\subseteq$.

4.6 Maximal and Infinite Ideals

Frequently one is interested in processes that continue as long as possible. These are modeled by ideals which are maximal w.r.t. $\leq$ or, equivalently, w.r.t. inclusion. We therefore give a characterisation of maximal ideals. For a behaviour $\mathcal{B}$ we denote the subset of maximal ideals by max; this agrees with the definition in Section 2, and hence all our laws there apply.

Lemma 4.8 *Suppose $I \in I(M)$ and $N \subseteq M$. Then*

1. $x \in \mathsf{max}\, I \ \Leftrightarrow\ I = x^{\leq}$.
2. $\mathsf{max}\, I = \emptyset \ \Rightarrow\ I$ *infinite.*
3. $\mathsf{max}\, N = \emptyset \wedge I \in \mathsf{max}\, \mathsf{ide}\, N \ \Rightarrow\ \mathsf{max}\, I = \emptyset$.

Proof: 1. ($\Rightarrow$) We only need to show $I \subseteq x^{\leq}$; the other inclusion follows from downward closure of I. Suppose $y \in I$. By directedness of I there is $z \in I$ with $x \leq z$ and $y \leq z$. Maximality of x implies $z = x$ and hence $y \leq x$.
($\Leftarrow$)

$$\begin{array}{cl} & \mathsf{max}\, I \\ = & \quad \{\!\![\ \text{by assumption}\ ]\!\!\} \\ & \mathsf{max}\, x^{\leq} \\ = & \quad \{\!\![\ \text{by Lemma 2.2.1}\ ]\!\!\} \\ & (x^{\leq})^{\leq} \backslash (x^{\leq})^{<} \\ = & \quad \{\!\![\ \text{by Lemma 2.1.4}\ ]\!\!\} \\ & x^{\leq} \backslash x^{<} \\ = & \quad \{\!\![\ \text{by Lemma 2.2.1}\ ]\!\!\} \\ & \mathsf{max}\, x \\ = & \quad \{\!\![\ \text{irreflexivity of} <]\!\!\} \\ & \{x\} \ . \end{array}$$

2. Every non-empty finite set has a maximal element.

3. Suppose $\mathsf{max}\, I \neq \emptyset$, say $x \in \mathsf{max}\, I$. By 1 then $I = x^{\leq}$ and by $I \in \mathsf{ide}\, N$ we get $x \in N$. Since $\mathsf{max}\, N = \emptyset$, there is $y \in N$ with $x \leq y$ and $y \neq x$. But then $y^{\leq} \in \mathsf{ide}\, N$ and hence, by Theorem 4.1.1, we have $x^{\leq} \subseteq y^{\leq} \wedge x^{\leq} \neq y^{\leq}$. This is a contradiction to $I \in \mathsf{max}\,\mathsf{ide}\, N$.

□

Motivated by 2 we define, for a behaviour $\mathcal{B}$, the set of its infinite ideals as

$$\mathsf{inf}\, \mathcal{B} \overset{\text{def}}{=} \{I \in \mathcal{B} : \mathsf{max}\, I = \emptyset\} .$$

For general domains, this is a bit of a misnomer, since there may well be infinite ideals *with* maximal elements. However, we will single out a particular class of domains where this cannot occur and work mostly with these, so that the terminology will be justified. Clearly, inf distributes through arbitrary union and intersection:

$$\mathsf{inf}\,(\bigcup_{i \in I} \mathcal{B}_i) = \bigcup_{i \in I} \mathsf{inf}\, \mathcal{B}_i , \tag{1}$$

$$\mathsf{inf}\,(\bigcap_{i \in I} \mathcal{B}_i) = \bigcap_{i \in I} \mathsf{inf}\, \mathcal{B}_i . \tag{2}$$

Now Lemma 4.8.3 can be restated as

$$\mathsf{max}\, N = \emptyset \Rightarrow \mathsf{max}\,\mathsf{ide}\, N \subseteq \mathsf{inf}\,\mathsf{ide}\, N .$$

The reverse inclusion is generally not valid. For a counterexample choose $M = \mathbb{N} \cup \{\infty\}$ with the usual ordering and consider the ideal $\mathbb{N} \in I(M)$. We have $\mathsf{max}\, \mathbb{N} = \emptyset$, but $\mathbb{N} \notin \mathsf{max}\, I(M)$, since $\mathbb{N} \subseteq M \in I(M)$ and $\mathbb{N} \neq M$.

We call a partial order $(M, \leq)$ max**-determined** if

$$\mathsf{inf}\, I(M) \subseteq \mathsf{max}\, I(M) .$$

Now we clarify the relation between $\mathsf{inf}\,\mathsf{ide}$ and $\mathsf{max}\,\mathsf{ide}$ and investigate monotonicity and distributivity of the $\mathsf{max}\,\mathsf{ide}$ and $\mathsf{max}\,\mathsf{inf}$ operation, which is important for refinement.

Lemma 4.9 *Let $(M, \leq)$ be max-determined. Then, for $N, P \subseteq M$,*

1. $\mathsf{inf}\,\mathsf{ide}\, N \subseteq \mathsf{ide}\, N \cap \mathsf{max}\, I(M) \subseteq \mathsf{max}\,\mathsf{ide}\, N$.
2. $\mathsf{max}\,\mathsf{ide}\, N = \mathsf{inf}\,\mathsf{ide}\, N \cup \mathsf{ide}\,\mathsf{max}\, N$.
3. $\mathsf{max}\, N = \emptyset \Rightarrow \mathsf{inf}\,\mathsf{ide}\, N = \mathsf{ide}\, N \cap \mathsf{max}\, I(M) = \mathsf{max}\,\mathsf{ide}\, N$.
4. $\mathsf{inf}\,\mathsf{ide}\, N \cup P = \mathsf{inf}\,\mathsf{ide}\, N \cup \mathsf{inf}\,\mathsf{ide}\, P$.
   In particular, $\mathsf{inf}\,\mathsf{ide}$ *is monotonic w.r.t. inclusion.*
5. $N = \mathsf{saf}\, N \Rightarrow \mathsf{inf}\,\mathsf{ide}\,(N \cap P) = \mathsf{inf}\,\mathsf{ide}\, N \cap \mathsf{inf}\,\mathsf{ide}\, P$.
6. $\mathsf{max}\, N = \emptyset \wedge N \subseteq P \Rightarrow \mathsf{max}\,\mathsf{ide}\, N \subseteq \mathsf{max}\,\mathsf{ide}\, P$.
7. $\mathsf{max}\, N = \mathsf{max}\, P = \emptyset \Rightarrow \mathsf{max}\,\mathsf{ide}\,(N \cup P) = \mathsf{max}\,\mathsf{ide}\, N \cup \mathsf{max}\,\mathsf{ide}\, P$.
8. *If N and P are cones with* $\mathsf{max}\, N = \mathsf{max}\, P = \mathsf{max}\,(N \cap P) = \emptyset$ *then* $\mathsf{max}\,\mathsf{ide}\,(N \cap P) = \mathsf{max}\,\mathsf{ide}\, N \cap \mathsf{max}\,\mathsf{ide}\, P$.

Proof: 1.

$$\begin{array}{ll} & I \in \mathsf{inf}\,\mathsf{ide}\,N \\ \Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\ & I \in \mathsf{ide}\,N \ \wedge\ \mathsf{max}\,I \ = \ \emptyset \\ \Rightarrow & \quad \{\![\text{ since } (M, \leq) \text{ is } \mathsf{max}\text{-determined }]\!\} \\ & I \in \mathsf{ide}\,N \ \wedge\ I \in \mathsf{max}\,I(M) \\ \Rightarrow & \quad \{\![\text{ by Lemma 2.2.3, since } \mathsf{ide}\,N \ \subseteq\ I(M) \ ]\!\} \\ & I \in \mathsf{max}\,\mathsf{ide}\,N \ . \end{array}$$

2. ($\subseteq$) Suppose $I \in \mathsf{max}\,\mathsf{ide}\,N$. If $\mathsf{max}\,I = \emptyset$, then $I \in \mathsf{inf}\,\mathsf{ide}\,N$ by definition. Otherwise $\mathsf{max}\,I$ is a singleton, say $\mathsf{max}\,I = \{x\}$, and $I = x^{\leq}$. It follows that $x \in N$. For $y \in N$ with $x \leq y$ we have $x^{\leq} \subseteq y^{\leq} \in \mathsf{ide}\,N$, so that $x^{\leq} = y^{\leq}$ by maximality of $I = x^{\leq}$. Hence also $x = y$. This shows $x \in \mathsf{max}\,N$, so that $I = x^{\leq} \in \mathsf{ide}\,\mathsf{max}\,N$.
($\supseteq$) $\mathsf{inf}\,\mathsf{ide}\,N \subseteq \mathsf{max}\,\mathsf{ide}\,N$ was shown in 1. Suppose now $I \in \mathsf{ide}\,\mathsf{max}\,N$, say $I = x^{\leq}$ with $x \in \mathsf{max}\,N$, and $I \subseteq J \in \mathsf{ide}\,N$, say $J = D^{\leq}$ for $D \in \mathsf{dir}\,N$. Consider $y \in J$. By directedness of J there is a $z \in J$ with $x, y \leq z$. By $J = D^{\leq}$ there is a $u \in D$ with $z \leq u$. Hence also $x, y \leq u$. By $D \subseteq N$ and $x \in \mathsf{max}\,N$ we get $x = u$. So $y \leq x$ and hence $y \in x^{\leq} = I$. Altogether, $J \subseteq I$ and hence $J = I$. So $I \in \mathsf{max}\,\mathsf{ide}\,N$.

3. Assume $\mathsf{max}\,N = \emptyset$. Then Lemma 4.8.3 shows $\mathsf{max}\,\mathsf{ide}\,N \subseteq \mathsf{inf}\,\mathsf{ide}\,N$ and the equalities follow from 1.

4. immediate from Lemma 4.6.1 and equation (1).

5. immediate from Lemma 4.6.2 and equation (2).

6.

$$\begin{array}{ll} & \mathsf{max}\,\mathsf{ide}\,N \\ = & \quad \{\![\text{ by 3 }]\!\} \\ & \mathsf{ide}\,N \ \cap\ \mathsf{max}\,I(M) \\ \subseteq & \quad \{\![\text{ by assumption } N \subseteq P \text{ and monotonicity of } \mathsf{ide} \ ]\!\} \\ & \mathsf{ide}\,P \ \cap\ \mathsf{max}\,I(M) \\ \subseteq & \quad \{\![\text{ by 3 }]\!\} \\ & \mathsf{max}\,\mathsf{ide}\,P \ . \end{array}$$

7. We aim at an application of Lemma 2.2.5. Suppose therefore that $I \in \mathsf{max}\,\mathsf{ide}\,N \cap (\mathsf{ide}\,P)^{<}$. By 3 we have $I \in \mathsf{max}\,I(M)$. But by $I \in (\mathsf{ide}\,P)^{<}$ there is $J \in \mathsf{ide}\,P$ with $I \subset J$, a contradiction to maximality of I. Hence $\mathsf{max}\,\mathsf{ide}\,N \cap (\mathsf{ide}\,P)^{<} = \emptyset$. By symmetry, also $\mathsf{max}\,\mathsf{ide}\,P \cap (\mathsf{ide}\,N)^{<} = \emptyset$. Now the claim is immediate from Lemma 2.2.5.

8. ($\subseteq$) follows from 6.
($\supseteq$) Assume $I \in \mathsf{max}\,\mathsf{ide}\,N \cap \mathsf{max}\,\mathsf{ide}\,P$. Then by 3 we have $I \in \mathsf{max}\,I(M)$. Hence, again by 3, we only need to show $I \in \mathsf{ide}\,(N \cap P)$. Since N and P are cones we get $I \subseteq N$ and $I \subseteq P$ and hence $I \subseteq N \cap P$ as well, showing the claim.

□

The next lemma allows simplification of the defining property of a behaviour.

Lemma 4.10 *Consider $N, P \subseteq M$. Then*

$$\mathsf{max}\,\mathsf{ide}\,(N \cup P) \ = \ \mathsf{max}\,\mathsf{ide}\,P \ \Leftrightarrow\ \mathsf{ide}\,N \leq \mathsf{ide}\,P \ .$$

Proof: (⇐)

$$\begin{array}{ll} & \mathsf{ide}\,N \leq \mathsf{ide}\,P \\ \Rightarrow & \quad \{\![\text{ by Lemma 2.3.6 }]\!\} \\ & \mathsf{max}\,(\mathsf{ide}\,N \cup \mathsf{ide}\,P) \ = \ \mathsf{max}\,\mathsf{ide}\,P \\ \Leftrightarrow & \quad \{\![\text{ by Lemma 4.6.1 }]\!\} \\ & \mathsf{max}\,\mathsf{ide}\,(N \cup P) \ = \ \mathsf{max}\,\mathsf{ide}\,P \ . \end{array}$$

(⇒) If $N = \emptyset$, the claim holds trivially, since $\mathsf{ide}\,\emptyset = \emptyset$. Hence we now assume $N \neq \emptyset$. We now need the so-called *Maximal Principle* (see e.g. [8]): *Assume a partial order in which every non-empty chain has an upper bound. Then every element has a maximal element above it.*
We apply this to the partial order $(\mathsf{ide}\,N, \subseteq)$. It satisfies the assumption, since $\mathsf{ide}\,N$ is closed under directed unions and hence, in particular, under unions of chains of directed sets. Consider now $I \in \mathsf{ide}\,N \subseteq \mathsf{ide}\,(N \cup P)$. By the maximal principle there is a $J \in \mathsf{max}\,\mathsf{ide}\,(N \cup P) = \mathsf{max}\,\mathsf{ide}\,P$ with $I \leq J$. □

Under additional assumptions we can simplify the property:

Lemma 4.11 *Assume* $P \in \mathsf{dir}\,M$. *Then*

$$\mathsf{max}\,\mathsf{ide}\,(N \cup P) \ = \ \mathsf{max}\,\mathsf{ide}\,P \ \Leftrightarrow \ N \leq P \ .$$

Proof: To apply Lemma 4.10 we show that $P \in \mathsf{dir}\,M$ implies

$$\mathsf{ide}\,N \leq \mathsf{ide}\,P \ \Leftrightarrow \ N \leq P \ .$$

(⇒) Assume $x \in N$. Then $\{x\}^{\leq} \in \mathsf{ide}\,N$ and so there is $I \in \mathsf{ide}\,P$, say $I = D^{\leq}$ for $D \in \mathsf{dir}\,P$, with $\{x\}^{\leq} \leq I$. By Lemma 2.3.1-2 we get $\{x\} \leq P$.
(⇐) For $I \in \mathsf{ide}\,N$ we have $I \leq P \in \mathsf{dir}\,P$ and hence, by Lemma 2.3.1, also $I \leq P^{\leq} \in \mathsf{ide}\,P$. □

For a counterexample when P is not directed see Example 5.6 in connection with Corollary 4.12.2 below.

Recalling the equivalence $\sim$ associated with the preorder $\leq$, we obtain from the previous two lemmata

Corollary 4.12 *Consider* $N, P \subseteq M$. *Then*

1. $\mathsf{ide}\,N \sim \mathsf{ide}\,P \Rightarrow \mathsf{max}\,\mathsf{ide}\,N = \mathsf{max}\,\mathsf{ide}\,P$.
2. *If* $N, P \in \mathsf{dir}\,M$ *then*
$$N \sim P \ \Rightarrow \ \mathsf{max}\,\mathsf{ide}\,N \ = \ \mathsf{max}\,\mathsf{ide}\,P \ .$$

We conclude this section by an alternative characterization of the set $\mathsf{inf}\,\mathsf{ide}\,P$ for property $P \subseteq M$. First we define

$$\mathsf{lim}\,P \ \overset{\text{def}}{=} \ \{I \in I(M) : I \cap P \in \mathsf{dir}\,M \ \wedge \ \mathsf{max}\,(I \cap P) \ = \ \emptyset\} \ .$$

This generalizes the corresponding definition for infinite words or streams in [21, 25, 26] (to cite just a few), which is based on [9]. Other notations for $\mathsf{lim}\,P$ found in the literature are P^{δ} or $\vec{P}$. We can then show

Lemma 4.13 *1.* $\mathsf{inf\,ide}\,P \subseteq \mathsf{lim}\,P$.

2. If $(M, \leq)$ is max-determined then the reverse inclusion holds as well.

Proof: We first note that

$$\begin{array}{ll}
 & I \in \mathsf{inf\,ide}\,P \\
\Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\
 & I \in \mathsf{ide}\,P \wedge \mathsf{max}\,I = \emptyset \\
\Leftrightarrow & \quad \{\![\text{ by Lemma 4.2 }]\!\} \\
 & I = (I \cap P)^{\leq} \wedge \mathsf{max}\,I = \emptyset \\
\Leftrightarrow & \quad \{\![\text{ equality }]\!\} \\
 & I = (I \cap P)^{\leq} \wedge \mathsf{max}\,(I \cap P)^{\leq} = \emptyset \\
\Leftrightarrow & \quad \{\![\text{ Lemma 2.2.2 }]\!\} \\
 & I = (I \cap P)^{\leq} \wedge \mathsf{max}\,(I \cap P) = \emptyset \; . \qquad\qquad (*)
\end{array}$$

Now we prove our claims as follows:

1. $$\begin{array}{ll}
 & (*) \\
\Rightarrow & \quad \{\![\text{ by Lemma 3.1.3 }]\!\} \\
 & I \cap P \in \mathsf{dir}\,M \wedge \mathsf{max}\,(I \cap P) = \emptyset \\
\Leftrightarrow & \quad \{\![\text{ definition }]\!\} \\
 & I \in \mathsf{lim}\,P \; .
\end{array}$$

2. Let $(M, \leq)$ be max-determined and assume $I \in \mathsf{lim}\,P$. By $(*)$ it remains to show $I = (I \cap P)^{\leq}$. First, by monotonicity of downward closure we have $(I \cap P)^{\leq} \subseteq I^{\leq} = I$. Using Lemma 2.2.2 we obtain $\mathsf{max}\,(I \cap P)^{\leq} = \mathsf{max}\,(I \cap P) = \emptyset$, so that by max-determinedness $(I \cap P)^{\leq} \in \mathsf{max}\,I(M)$ and hence $(I \cap P)^{\leq} = I$.

□

4.7 About max-Determinedness

It remains to investigate under which conditions a partial order is max-determined. To this end we introduce some auxiliary notions. Let $F : \mathcal{P}(M) \to \mathcal{P}(M)$ be some function, such as dir or ide. We say that $N \subseteq M$ **has F-maxima** if every set in $F(N)$ has a maximal element. In addition to the functions mentioned we shall use

$$\begin{array}{rcl}
\mathsf{ne}\,N & \overset{\text{def}}{=} & \{C \subseteq N : C \neq \emptyset\} \; , \\
\mathsf{chai}\,N & \overset{\text{def}}{=} & \{C \subseteq N : C \text{ non-empty chain}\} \; .
\end{array}$$

Lemma 4.14 *If $N \subseteq M$ has chai-maxima, then it also has ne-maxima.*

Proof: Assume $\emptyset \neq D \subseteq N$ and $\mathsf{max}\,D = \emptyset$. Construct a chain $C \subseteq N$ as follows: Choose $x_0 \in D$ arbitrarily. Assume now that x_i has been found. Since $x_i \notin \emptyset = \mathsf{max}\,D$, there is $x_{i+1} \in D$ with $x_i < x_{i+1}$. Now for $C \overset{\text{def}}{=} \{x_i : i \in \mathbb{N}\}$ we have $\mathsf{max}\,C = \emptyset$, a contradiction. □

Corollary 4.15 *If $N \subseteq M$ has chai-maxima, then it also has dir-maxima.*

Proof: Every directed set is non-empty. □

We say that $(M, \leq)$ **separates ideals** if for all $I, J \in I(M)$ with $I \neq J$ the intersection $I \cap J$ has chai-maxima. The connection with max-determinedness is given by

Theorem 4.16 *$(M, \leq)$ is max-determined iff $(M, \leq)$ separates ideals.*

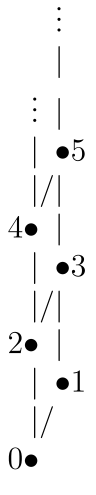
Proof: ($\Rightarrow$) Suppose $I \neq J$ and $C \in \mathsf{chai}\,(I \cap J)$, but $\mathsf{max}\, C = \emptyset$. Then $C^{\leq}$ is an ideal with $\mathsf{max}\, C^{\leq} = \emptyset$. By max-determinedness then $C^{\leq} \in \mathsf{max}\,\mathsf{ide}\, M$. Since by downward closedness of I and J we have $C^{\leq} \subseteq I$ and $C^{\leq} \subseteq J$ it follows that $I = C^{\leq} = J$, a contradiction.
($\Leftarrow$) Assume $\mathsf{max}\, I = \emptyset$ and $I \notin \mathsf{max}\,\mathsf{ide}\, M$. Then there is $J \neq I$ with $I \subseteq J$. Since $(M, \leq)$ separates ideals and by Corollary 4.15 then $I = I \cap J$ has dir-maxima. In particular, $\mathsf{max}\, I \neq \emptyset$, a contradiction. □

This has the following surprising consequence:

Corollary 4.17 *Let $(M, \leq)$ be max-determined. Then all elements of M are compact.*

Proof: By the previous theorem, $(M, \leq)$ separates ideals.
We now first show $\sqcup I \subseteq I$ for all $I \in I(M)$. Assume $y \in \sqcup I$ and set $J \overset{\text{def}}{=} \{y\}^{\leq}$. We have $I \subseteq J$. If $I \neq J$ then $I = I \cap J$ has a maximal and hence, by directedness, greatest element z. But then $z = \sqcup I = y$ so that $J = I$, a contradiction.
Consider now $x \in M$ and $I \in I(M)$ such that $x \leq \sqcup I \in I$. By downward closedness of I we get $x \in I$ and x is compact. □

The reverse implication is not valid as the following example shows: Consider



in which all elements are compact. However, for $I \overset{\text{def}}{=} \{0, 2, 4, \ldots\}$ we have $\mathsf{max}\, I = \emptyset$ and $I \subset J \overset{\text{def}}{=} \{0, 1, 2, 3, 4, \ldots\}$, i.e., I is not maximal. Concerning separation of ideals, $I = I \cap J$ doesn't have a maximal element.

It will be interesting to find further, more "manageable" characterisations of max-determinedness.

5 A Particular Case: Streams

We now specialise to a particular partial order. We shall represent streams using sets of finite traces. These are finite words over an alphabet A of atomic actions; they are ordered by the prefix relation.

5.1 Prefix Order and Streams

As usual, A^* is the set of all finite words over alphabet A. By ε we denote the empty word over A, whereas concatenation is denoted by $\bullet$.

A word u is a **prefix** of a word v, written $u \sqsubseteq v$, iff there is a word w such that $u \bullet w = v$, or, in other words, if v is an extension of u. It is well-known that this defines a partial order on words which is even well-founded. Moreover, ε is the least element in this order. The corresponding strict-order is denoted by $\sqsubset$. A cone of $(A^*, \sqsubseteq)$ is then a prefix-closed language. Note that every non-empty cone contains ε.

A few properties we shall use are the following (where $x, y, u, v, w \in A^*$ and $U, V \subseteq A^*$):

$$\begin{aligned} v \sqsubseteq w \quad &\Leftrightarrow \quad u \bullet v \sqsubseteq u \bullet w \ , & (3) \\ u \sqsubseteq w \wedge v \sqsubseteq w \quad &\Rightarrow \quad u \sqsubseteq v \vee v \sqsubseteq u \ , & (4) \\ V \neq \emptyset \quad &\Rightarrow \quad (U \bullet V)^{\sqsubseteq} = U^{\sqsubseteq} \cup U \bullet V^{\sqsubseteq} \ . & (5) \end{aligned}$$

Poperty (4) is also called **local linearity**. Because of it, the following special property of directedness over $(A^*, \sqsubseteq)$ is immediate:

Lemma 5.1 *$D \subseteq A^*$ is directed w.r.t. $\sqsubseteq$ iff D is linearly ordered by $\sqsubseteq$.*

Thus, by prefix-closedness, an ideal is a set of words of increasing length "growing at the right end". This set may be finite or infinite. A simple example is, for $a \in A$, the infinite ideal

$$a^* = \{\varepsilon,\ a,\ a \bullet a,\ a \bullet a \bullet a,\ a \bullet a \bullet a \bullet a,\ \ldots\} \ .$$

For the special case of words under the prefix ordering, we therefore call the elements of $I(A^*)$ **streams** over A. The compact elements of $I(A^*)$ correspond to the elements of A^*, whereas the non-compact elements are precisely the (cardinally) infinite ideals. Hence, for countable A, the set $(I(A), \subseteq)$ has a countable basis of compact elements and therefore is countably algebraic.

Let us give another characterization of infinite streams:

Lemma 5.2 *A stream S is infinite iff $\mathsf{max}\, S = \emptyset$.*

Proof: First, by linearity of the prefix order on a stream and by its well-foundedness, an infinite stream cannot have a maximal element. By Lemma 4.8.2 we have also the reverse implication. □

5.2 Streams and Properties

The set of streams satisfying a property $P \subseteq A^*$ is

$$\mathsf{str}\, P \overset{\text{def}}{=} \mathsf{ide}\, P \ .$$

Note that it would not be adequate to work with the set $\mathsf{str}\,(P^{\sqsubseteq})$, the so-called *adherence* of P (see e.g. [17, 25]), instead of $\mathsf{str}\,P$. The reason is that by prefix-closure infinite substreams may "sneak" into a cone although it results from a language of mutually $\sqsubseteq$-incomparable words which represent systems with finite behaviour only.

Example 5.3 The language $0^* \bullet 1$ represents a behaviour with arbitrarily long but finite sequences of 0s terminated by the "explicit endmarker" 1. However, its prefix closure $(0^* \bullet 1)^{\sqsubseteq}$ contains the infinite ideal 0^* representing an infinite stream of 0s. □

Using König's Lemma one can even show that for finite A *every* infinite cone contains an infinite stream. This is also the reason why the Hoare power domain is "too angelic". The general definition of ide omits these undesired streams.

Safety properties are in our special case simply prefix-closed subsets of A^*. To see an example of a deadlock-free property, we first note that if $U \cap \varepsilon = \emptyset$ then $\mathsf{max}\,U^* = \emptyset$. Hence, for $A = \{0, 1\}$ the language $(0^* \bullet 1)^*$ is deadlock-free.

We want to show now that str (and hence ide) does not distribute through general union:

Example 5.4 Take $U = 0^*$. Then $U = \bigcup\limits_{i \in \mathbb{N}} 0^i$. However, $\mathsf{str}\,U = \{0^*\} \cup \{(0^i)^{\sqsubseteq} : i \in \mathbb{N}\}$, whereas $\bigcup\limits_{i \in \mathbb{N}} \mathsf{str}\,0^i = \{(0^i)^{\sqsubseteq} : i \in \mathbb{N}\}$. □

5.3 Maximal and Infinite Streams

As already mentioned, maximal ideals model processes that go on as long as possible. For streams we have a more pleasant situation than for general ideals:

Lemma 5.5 $(A^*, \sqsubseteq)$ *is* max*-determined.*

Proof: Assume $I \in \mathsf{ide}\,A^* \wedge \mathsf{max}\,I = \emptyset$ and consider $J \in \mathsf{ide}\,A^*$ with $I \subseteq J$. By Lemma 2.4 and downward closure of I, J it suffices to show $J \leq I$. Consider $y \in J$. Since $\mathsf{max}\,I = \emptyset$ there is some $x \in I \subseteq J$ with $||y|| \leq ||x||$, where $||u||$ denotes the length of word u. Moreover, by directedness of J, there is $z \in J$ with $x \sqsubseteq z \wedge y \sqsubseteq z$. From linearity of $z^{\sqsubseteq}$ it therefore follows that $x \sqsubseteq y \vee y \sqsubseteq x$. However, since $||y|| \leq ||x||$, we must have $y \sqsubseteq x$. □

This allows us to use all laws from Section 4.6 for streams. At this point it is also convenient to give the counterexample to Corollary 4.12.2 and hence also to Lemma 4.11 when non-directed sets are involved:

Example 5.6 Set $U \overset{\text{def}}{=} 0^* \bullet 1$ and $V \overset{\text{def}}{=} U \cup 0^* = U^{\sqsubseteq}$ by (5). Then $U \sim V$, but $\mathsf{max}\,\mathsf{str}\,U \neq \mathsf{max}\,\mathsf{str}\,V$, since $0^* \in (\mathsf{max}\,\mathsf{str}\,V) \backslash (\mathsf{max}\,\mathsf{str}\,U)$. Note, however, that neither U nor V is directed. □

Now we turn to infinite streams. We note that by Lemma 5.2 we have

$$\mathsf{inf}\,\mathsf{ide}\,P = \{I \in \mathsf{ide}\,P : I \text{ infinite}\} .$$

To establish the relation with [25] we also show

Lemma 5.7 *For* $P \subseteq A^*$ *we have*

$$\mathsf{lim}\,P = \{I \in I(A^*) : I \cap P \textit{ infinite}\} .$$

Proof:

$$\begin{array}{ll} & I \in \mathsf{lim}\, P \\ \Leftrightarrow & \quad \{\!\![\text{ definition }]\!\!\} \\ & I \cap P \in \mathsf{dir}\, M \ \wedge\ \mathsf{max}\,(I \cap P) \ = \ \emptyset \\ \Leftrightarrow & \quad \{\!\![\text{ by } I \cap P \ \subseteq\ I \text{ and Lemma 5.1 }]\!\!\} \\ & I \cap P \neq \emptyset \wedge \mathsf{max}\,(I \cap P) \ = \ \emptyset \ . \end{array}$$

We show now that, for linearly ordered $L \ \subseteq\ A^*$,

$$L \text{ infinite } \ \Leftrightarrow\ L \neq \emptyset \wedge \mathsf{max}\, L \ = \ \emptyset \ .$$

($\Rightarrow$) $L \ \neq\ \emptyset$ is immediate. Suppose $x \in \mathsf{max}\, L$. By linearity then $L \ \subseteq\ x^{\sqsubseteq}$. But then $|L| \leq ||x|| + 1$, a contradiction.
($\Leftarrow$) Every non-empty finite set has a maximal element. □

5.4 Stream Concatenation

As a prerequisite for defining infinite repetition we need stream concatenation which, for streams S, T is defined by

$$S \circ T \stackrel{\text{def}}{=} S \cup (\mathsf{max}\, S) \bullet T \ .$$

Let us explain this definition. If S is finite then $\mathsf{max}\, S$ is a singleton. This part of the overall behaviour then is prefixed to all traces in T to represent the concatenated behaviour. If S is infinite then $\mathsf{max}\, S \ = \ \emptyset$ and hence, by strictness of $\circ$, we get $S \circ T \ = \ S$, as is intuitively expected.

It is straightforward to show that $S \circ T$ is indeed a stream and that $(I(A^*), \circ, \varepsilon)$ is a monoid. Moreover one has

$$\mathsf{max}\,(S \circ T) \ = \ (\mathsf{max}\, S) \bullet (\mathsf{max}\, T) \ . \tag{6}$$

As a shorthand notation we shall also allow words as first argument of $\circ$. This is made precise by setting

$$u \circ T \ \stackrel{\text{def}}{=} \ u^{\sqsubseteq} \circ T \ = \ u^{\sqsubseteq} \cup u \bullet T \ .$$

Again, $\circ$ is extended pointwise to behaviours and, in the case of the above shorthand, to languages.

5.5 Infinite Repetition

We now give the usual greatest fixpoint definition of the set U^ω of streams that result from infinite repetition of words from a language $U \ \subseteq\ A^*$:

$$\mathcal{X} \ \subseteq\ U^\omega \stackrel{\text{def}}{\Leftrightarrow} \mathcal{X} \ = \ U \circ \mathcal{X} \ .$$

This is well-defined by monotonicity of $\circ$. Note that by this definition $\emptyset^\omega = \emptyset$. However, if $\varepsilon \in U$ then $U^\omega \ = \ I(A^*)$. For that reason, U^ω is usually considered only for $\varepsilon \notin U$.

It should be noted that for $|U| \geq 2$ and $U \cap \varepsilon \ = \ \emptyset$ there are nontrivial solutions of $\mathcal{X} \ = \ U \circ \mathcal{X}$ properly less than U^ω. As an example consider the behaviour $U^* \circ \bigcup\limits_{u \in U} u^\omega$ of all eventually periodic streams.

To tie this in with the str-operation, we quote [25], p. 433:

$$\varepsilon \notin U \;\Rightarrow\; \mathsf{lim}\, U^* \;=\; U^\omega \,\cup\, U^* \circ \mathsf{lim}\, U \ ,$$

or, using Lemma 4.13 and max-determinedness,

$$\varepsilon \notin U \;\Rightarrow\; \mathsf{inf}\,\mathsf{str}\, U^* \;=\; U^\omega \,\cup\, U^* \circ \mathsf{inf}\,\mathsf{str}\, U \ .$$

From this it is immediate that

$$\varepsilon \notin U \,\wedge\, \mathcal{X} \;=\; U \circ \mathcal{X} \;\Rightarrow\; \mathcal{X} \;\subseteq\; \mathsf{inf}\,\mathsf{str}\, U^* \ . \tag{7}$$

Moreover, by strictness of $\circ$ it follows that

$$\varepsilon \notin U \;\Rightarrow\; \mathsf{inf}\,\mathsf{str}\, U \;=\; \emptyset \;\Rightarrow\; U^\omega \;=\; \mathsf{inf}\,\mathsf{str}\, U^* \ . \tag{8}$$

A sufficient condition to establish the premise is given by

Lemma 5.8 *If $U \subseteq A^*\backslash\varepsilon$ satisfies the Fano condition, i.e., the words in U are mutually incomparable w.r.t. $\sqsubseteq$, then*

$$U^\omega \;=\; \mathsf{inf}\,\mathsf{str}\, U^* \ .$$

Proof: By the Fano condition, all directed subsets of U are singletons. Hence $\mathsf{str}\, U \;=\; \{u^{\leq} : u \in U\}$ consists of finite streams only. □

Note that if $\varepsilon \in U$ then U satisfies the Fano condition iff $U \;=\; \varepsilon$; for this case the above equation doesn't hold, since then $\mathsf{inf}\,\mathsf{str}\, U^* \;=\; \emptyset$. It should also be mentioned that U satisfies the Fano condition iff $U \;=\; \mathsf{max}\, U$. To see what happens if the Fano condition is not satisfied, consider

Example 5.9 Let $A = \{a, b\}$ and $U \overset{\text{def}}{=} \{a{\bullet}b^n : n \in \mathbb{N}\} \subseteq A^*$. Then $U \in \mathsf{dir}\, U^*$, since $U \subseteq U^*$ and U is directed. Hence $U^{\sqsubseteq} = \varepsilon \cup U \in \mathsf{str}\, U^*$ and, since $U^{\sqsubseteq}$ is infinite, even $U^{\sqsubseteq} \in \mathsf{inf}\,\mathsf{str}\, U^*$. Now, $U^{\sqsubseteq}$ represents an a followed by infinitely many bs; but this behaviour clearly does not arise from repeated concatenation of words in U. It is "sneaked in" by the fact that simply considering directed subsets of U^* throws away too much structural information. □

To allow a characterization of U^ω for languages that do not satisfy the Fano condition, one can artificially enforce it by attaching a special endmarker to all words in U and remove it after singling out the infinite streams. Let $\# \notin A$ be a new letter and consider streams over the extended alphabet $A \cup \#$. Moreover, denote by $A \lhd u$ the word that results from u by removing all occurrences of $\#$ and extend the operation $A\lhd$ pointwise to languages and behaviours. Some useful properties are

$$\begin{aligned} A \lhd (u \bullet v) \;&=\; (A \lhd u) \bullet (A \lhd v) \ , && (9)\\ A \lhd (U \circ T) \;&=\; (A \lhd U) \circ (A \lhd T) \ . && (10) \end{aligned}$$

Then we have

Lemma 5.10 *For $U \subseteq A^*\backslash\varepsilon$,*

$$U^\omega \;=\; A \lhd \mathsf{inf}\,\mathsf{str}\,(U \bullet \#)^* \ .$$

The proof will be given below. The streams in $\mathsf{str}\,(U \bullet \#)^*$ correspond to finite and infinite sequences that result from concatenating arbitrary elements of U with the separator $\#$ in between. The operation max then selects the prefix-maximal ones of these; if $\varepsilon \notin U$ these are precisely the infinite words resulting from repeatedly concatenating words from U. The separators are used to record the "construction history" of the streams; they are finally thrown away again by the filter $A\lhd$. In this way subsets of U^* which are directed "by accident" are ignored. A similar mechanism for defining iteration is employed in [18] in the finite case and in [5] in the infinite case. To prove Lemma 5.10 we need the auxiliary

Lemma 5.11 *If $\# \notin A$ then*

1. $\mathsf{dir}\,(U \bullet \# \bullet V) \;=\; \{u \bullet \# \bullet E : u \in U \;\wedge\; E \in \mathsf{dir}\,V\}$.
2. $\mathsf{str}\,(U \bullet \# \bullet V) \;=\; (U \bullet \#) \circ \mathsf{str}\,V$.
3. $\mathsf{inf}\,\mathsf{str}\,(U \bullet \# \bullet V) \;=\; (U \bullet \#) \circ \mathsf{inf}\,\mathsf{str}\,V$.

Proof: 1. ($\subseteq$) Assume $D \in \mathsf{dir}\,(U \bullet \# \bullet V)$ and consider $x_i \;=\; u_i \bullet \# \bullet v_i \in D$ with $i \in \{1,2\}$ and $u_i \in U$ and $v_i \in V$. By directedness of D we may w.l.o.g. assume $x_1 \sqsubseteq x_2$, say $x_1 \bullet w = x_2$. So $u_1 \bullet \# \bullet v_1 \bullet w = u_2 \bullet \# \bullet v_2$. Since $\#$ doesn't occur in u_i and v_i, it follows that $u_1 = u_2$ and $v_1 \sqsubseteq v_2$, as required.
($\supseteq$) is immediate from (3).

2.
$$
\begin{array}{ll}
 & \mathsf{str}\,(U \bullet \# \bullet V) \\
= & \quad \{\!\![\text{ definition }]\!\!\} \\
 & \{D^{\sqsubseteq} : D \in \mathsf{dir}\,(U \bullet \# \bullet V)\} \\
= & \quad \{\!\![\text{ by 1 }]\!\!\} \\
 & \{(u \bullet \# \bullet E)^{\sqsubseteq} : u \in U \;\wedge\; E \in \mathsf{dir}\,V\} \\
= & \quad \{\!\![\text{ by equation (5) and non-emptiness of directed sets }]\!\!\} \\
 & \{(u \bullet \#)^{\sqsubseteq} \cup (u \bullet \#) \bullet E^{\sqsubseteq} : u \in U \;\wedge\; E \in \mathsf{dir}\,V\} \\
= & \quad \{\!\![\text{ definition of } \circ \;]\!\!\} \\
 & \{(u \bullet \#) \circ E^{\sqsubseteq} : u \in U \;\wedge\; E \in \mathsf{dir}\,V\} \\
= & \quad \{\!\![\text{ pointwise extension }]\!\!\} \\
 & (U \bullet \#) \circ \mathsf{str}\,V \;.
\end{array}
$$

3.
$$
\begin{array}{ll}
 & S \in \mathsf{inf}\,\mathsf{str}\,(U \bullet \# \bullet V) \\
\Leftrightarrow & \quad \{\!\![\text{ definition }]\!\!\} \\
 & S \in \mathsf{str}\,(U \bullet \# \bullet V) \;\wedge\; \mathsf{max}\,S \;=\; \emptyset \\
\Leftrightarrow & \quad \{\!\![\text{ by 2 }]\!\!\} \\
 & S \in (U \bullet \#) \circ \mathsf{str}\,V \;\wedge\; \mathsf{max}\,S \;=\; \emptyset \\
\Leftrightarrow & \quad \{\!\![\text{ pointwise extension }]\!\!\} \\
 & \exists\, u \in U : \exists\, T \in \mathsf{str}\,V : S \;=\; (u \bullet \#) \circ T \;\wedge\; \mathsf{max}\,S \;=\; \emptyset \\
\Leftrightarrow & \quad \{\!\![\text{ by equation (6) }]\!\!\} \\
 & \exists\, u \in U : \exists\, T \in \mathsf{str}\,V : S \;=\; (u \bullet \#) \circ T \;\wedge\; u \bullet \# \bullet \mathsf{max}\,T \;=\; \emptyset \\
\Leftrightarrow & \quad \{\!\![\text{ totality of } \bullet \;]\!\!\} \\
 & \exists\, u \in U : \exists\, T \in \mathsf{str}\,V : S \;=\; (u \bullet \#) \circ T \;\wedge\; \mathsf{max}\,T \;=\; \emptyset
\end{array}
$$

$$
\begin{array}{ll}
\Leftrightarrow & \quad \{\![\ \text{definition of } \mathsf{inf}\ ]\!\} \\
 & \exists\, u \in U : \exists\, T \in \mathsf{inf}\,\mathsf{str}\, V : S \;=\; (u \bullet \#) \circ T \\
\Leftrightarrow & \quad \{\![\ \text{pointwise extension}\ ]\!\} \\
 & S \in (U \bullet \#) \circ \mathsf{inf}\,\mathsf{str}\, V \ .
\end{array}
$$

□

Now we are ready to give the

Proof of Lemma 5.10:
We first show that $\mathcal{B} \overset{\text{def}}{=} A \lhd \mathsf{inf}\,\mathsf{str}\,(U \bullet \#)^*$ is a fixpoint:

$$
\begin{array}{ll}
 & \mathcal{B} \\
= & \quad \{\![\ \text{definition}\ ]\!\} \\
 & A \lhd \mathsf{inf}\,\mathsf{str}\,(U \bullet \#)^* \\
= & \quad \{\![\ \text{recursion for } {}^*\ ]\!\} \\
 & A \lhd \mathsf{inf}\,\mathsf{str}\,(\varepsilon \,\cup\, U \bullet \# \bullet (U \bullet \#)^*) \\
= & \quad \{\![\ \text{by Lemma 4.10}\ ]\!\} \\
 & A \lhd \mathsf{inf}\,\mathsf{str}\,(U \bullet \# \bullet (U \bullet \#)^*) \\
= & \quad \{\![\ \text{by Lemma 5.11.3}\ ]\!\} \\
 & A \lhd (U \bullet \#) \circ \mathsf{inf}\,\mathsf{str}\,(U \bullet \#)^* \\
= & \quad \{\![\ \text{by (9) and (10)}\ ]\!\} \\
 & ((A \lhd U) \bullet (A \lhd \#)) \circ (A \lhd \mathsf{inf}\,\mathsf{str}\,(U \bullet \#)^*) \\
= & \quad \{\![\ \text{definition of } \lhd \text{ and } \mathcal{B}\ ]\!\} \\
 & U \circ \mathcal{B} \ .
\end{array}
$$

Hence $\mathcal{B} \;\subseteq\; U^\omega$. For the reverse inclusion assume $S \in U^\omega$. We construct sequences $(u_i)_{i\in\mathbb{N}}$ and $(S_i)_{i\in\mathbb{N}}$ with $u_i \in U$ and $S_i \in U^\omega$ as follows: By $S \in U^\omega \;=\; U \circ U^\omega$ there are $u_0 \in U$ and $S_0 \in U^\omega$ with $S \;=\; u_0 \circ S_0$. Given $S_i \in U^\omega \;=\; U \circ U^\omega$, there are $u_{i+1} \in U$ and $S_{i+1} \in U^\omega$ with $S_i \;=\; u_{i+1} \circ S_{i+1}$.
Set now

$$
\begin{array}{llllll}
v_i & \overset{\text{def}}{=} & \underset{j<i}{\bullet}\, u_j \ , & w_i & \overset{\text{def}}{=} & \underset{j<i}{\bullet}\, (u_j \bullet \#) \qquad (i \in \mathbb{N}) \ , \\
D & \overset{\text{def}}{=} & \{v_i : i \in \mathbb{N}\} \ , & E & \overset{\text{def}}{=} & \{w_i : i \in \mathbb{N}\} \ .
\end{array}
$$

Then by construction $\forall \ \in \mathbb{N} : S = v_i \circ S_i$ so that $D \;\subseteq\; S$ and hence $D \;\sqsubseteq\; S$. Consider $s \in S$ and set $n \overset{\text{def}}{=} ||s||$. By $\varepsilon \notin U$ then $||v_n|| \geq ||s||$ so that $s \in S \;=\; v_n \circ S_n$ shows $s \;\sqsubseteq\; v_n \in D$. Therefore $S \;\sqsubseteq\; D$ and hence by downward closure of S even $S = D^{\sqsubseteq}$. However, $D^{\sqsubseteq} \;=\; A \lhd E^{\sqsubseteq}$ and $E \in \mathsf{dir}\,(U \bullet \#)^*$. By construction and $\varepsilon \notin U$ we have $w_i \;\sqsubset\; w_{i+1}$ for all $i \in \mathbb{N}$, so that additionally $\mathsf{max}\, E^{\sqsubseteq} \;=\; \mathsf{max}\, E \;=\; \emptyset$. This means $E^{\sqsubseteq} \in \mathsf{inf}\,\mathsf{str}\,(U \bullet \#)^*$. Altogether, we have shown $S \in \mathcal{B}$ as required. □

6 The Bounded Buffer Example Revisited

We consider again the buffer example in the introduction. We recall the family of properties

$$\mathrm{X}_n^{ab} \overset{\text{def}}{=} \{s \in A^* : s_a \leq s_b + n\} \ ,$$

where $n \in \mathbb{Z}$ and $A = \{a, b\}$. From this predicative, implicit definition we want to calculate a more explicit description corresponding to a generating grammar or accepting automaton. This can be done by a simple unfold/fold transformation using induction on the words in A^*. We obtain, for $c \in A$ and $U \subseteq A^*$,

$$\begin{array}{rcl} \varepsilon \in \mathrm{X}_n^{ab} & \Leftrightarrow & 0 \leq n \ , \\ c \bullet U \subseteq \mathrm{X}_n^{ab} & \Leftrightarrow & U \subseteq \mathrm{X}_{n+\delta_{cb}-\delta_{ca}}^{ab} \ , \end{array}$$

where δ is the Kronecker symbol. This corresponds to an infinite grammar with nonterminals X_n^{ab} or an infinite automaton with states X_n^{ab} $(n \in \mathbb{Z})$. Next we want a similar representation for

$$\mathrm{B}_n^{ab} \overset{\text{def}}{=} \mathsf{saf}\,\mathrm{X}_n^{ab} \ .$$

This can be done quite systematically, cf. [13], yielding

$$\begin{array}{rcll} \varepsilon \in \mathrm{B}_n^{ab} & \Leftrightarrow & 0 \leq n \ , & \\ a \bullet U \subseteq \mathrm{B}_n^{ab} & \Leftrightarrow & 0 \leq n-1 & \wedge \quad U \subseteq \mathrm{B}_{n-1}^{ab} \ , \\ b \bullet U \subseteq \mathrm{B}_n^{ab} & \Leftrightarrow & 0 \leq n & \wedge \quad U \subseteq \mathrm{B}_{n+1}^{ab} \ . \end{array}$$

In particular, $\mathrm{B}_n^{ab} = \emptyset$ for $n < 0$. Now we consider the bounded buffer behaviour. We calculate:

$$\begin{array}{ll} & \mathcal{BB}_n^{ab} \\ = & \quad \{\!\![\text{ definition }]\!\!\} \\ & \mathcal{BF}^{ab} \cap \mathcal{B}_n^{ab} \\ = & \quad \{\!\![\text{ definition }]\!\!\} \\ & \mathcal{B}_0^{ba} \cap \mathcal{B}_n^{ab} \\ = & \quad \{\!\![\text{ definition }]\!\!\} \\ & \mathsf{inf\,str}\,\mathrm{B}_0^{ba} \cap \mathsf{inf\,str}\,\mathrm{B}_n^{ab} \\ = & \quad \{\!\![\text{ by Lemma 4.9.5, since by definition the B sets are safety properties }]\!\!\} \\ & \mathsf{inf\,str}\,(\mathrm{B}_0^{ba} \cap \mathrm{B}_n^{ab}) \ . \end{array}$$

So the problem has been reduced to finding an explicit representation for $\mathrm{B}_0^{ba} \cap \mathrm{B}_n^{ab}$, which is a simple product automaton construction. It is a special case of the automaton for

$$\mathrm{G}_{mn} \overset{\text{def}}{=} \mathrm{B}_m^{ba} \cap \mathrm{B}_n^{ab} \ .$$

With a suitable definition of parallel composition one has the usual lemma that a buffer of capacity n can be implemented by a parallel composition of n buffers of capacity 1 (see again [13] for details). For the special case of $n = 1$ we have

$$\mathrm{BB}_1^{ab} = \mathrm{G}_{01} \ ,$$

where

$$\begin{array}{rcl} \varepsilon \in \mathrm{G}_{01} \Leftrightarrow \mathrm{TRUE} \ , & \qquad & \varepsilon \in \mathrm{G}_{10} \Leftrightarrow \mathrm{TRUE} \ , \\ a \bullet U \subseteq \mathrm{G}_{01} \Leftrightarrow U \subseteq \mathrm{G}_{10} \ , & & a \bullet U \subseteq \mathrm{G}_{10} \Leftrightarrow \mathrm{FALSE} \ , \\ b \bullet U \subseteq \mathrm{G}_{01} \Leftrightarrow \mathrm{FALSE} \ , & & b \bullet U \subseteq \mathrm{G}_{10} \Leftrightarrow U \subseteq \mathrm{G}_{01} \ . \end{array}$$

This corresponds to a two-state accepting automaton for the bounded buffer property, which is sufficient for purposes of implementation. However, the above can also be seen as a regular grammar or system of equations for languages. If desired, we can calculate from it a regular expression for $\mathrm{BB}_1^{ab} = \mathrm{G}_{01}$ using twice

$$\textbf{(Arden's Rule)} \quad \frac{U \cap \varepsilon = \emptyset, \; X = V \cup U \bullet X}{X = U^* \bullet V \; .}$$

This gives

$$\mathrm{BB}_1^{ab} = (a \bullet b)^* \bullet (\varepsilon \cup a) \; .$$

Using

$$(a \bullet b)^* \bullet a \;\sim\; (a \bullet b)^* \; ,$$

directedness of these two languages and Corollary 4.12.2, which applies, since BB_1^{ab} is deadlock-free and so $\mathsf{inf}\,\mathsf{str}\,\mathrm{BB}_1^{ab} = \mathsf{max}\,\mathsf{str}\,\mathrm{BB}_1^{ab}$ by Lemma 4.9.3, we obtain

$$\mathcal{BB}_1^{ab} = \mathsf{inf}\,\mathsf{str}\,(a \bullet b)^* \; .$$

Finally we use the fact that the language $a{\bullet}b$ as a singleton trivially satisfies the Fano condition, so that Lemma 5.8 gives

$$\mathcal{BB}_1^{ab} = (a \bullet b)^\omega \; ,$$

as expected.

7 Conclusion

We have introduced some algebraic operators and laws that can be used in the specification and derivation of systems. By abstracting from the domain of streams for which most of the notions were coined originally, we have obtained a rich set of laws which hold for a wide variety of domains. The order-theoretic approach lends itself well to an algebraictreatment. The point-free formulation eases and compactifies specifications,proofs of the basic properties and the actual derivations. Further research along these lines should search for similar algebraic characterisations of other important notions about systems and to explore their algebraic properties.

Concerning the underlying theory, our domain-thoretic notions should be tied in with the topological view (see e.g. [21, 24]). Moreover, in the stream domain there obviously is a close connection with temporal operators: $\mathsf{str}\,P$ is related to intermittent assertions [7], $\mathsf{inf}\,\mathsf{str}\,P$ can be read as $\Box\Diamond P$ (always eventually P) and $\mathsf{saf}\,P$ as $\boxed{\mathrm{i}}\,P$ (P holds in all initial subintervals [16]). These connections need to be made precise and carried over to arbitrary domains.

Acknowledgements

I gratefully acknowledge helpful remarks from J. Desharnais, W. Dosch, and M. Russling.

Appendix: Deferred Proofs

It turns out that all proofs for Section 2 can be given in a point-free, strongly algebraic proof style.

Proof of Lemma 2.1

1. The first property is immediate from the definition, whereas the second follows from the transitivity of $<$.
2. The first conjunct is a general property of inverse images of relations. The second one follows easily from it.
3. is immediate from 2.
4. First,

$$\begin{array}{ll}
 & (N^{\leq})^{<} \\
= & \quad \{\![\ \text{definition of } N^{\leq}\ ]\!\} \\
 & (N \cup N^{<})^{<} \\
= & \quad \{\![\ \text{by } 2\ ]\!\} \\
 & N^{<} \cup (N^{<})^{<} \\
= & \quad \{\![\ \text{by } 1\ ]\!\} \\
 & N^{<}\ .
\end{array}$$

Second,

$$\begin{array}{ll}
 & (N^{\leq})^{\leq} \\
= & \quad \{\![\ \text{definition of } {}^{\leq}\ ]\!\} \\
 & N^{\leq} \cup (N^{\leq})^{<} \\
= & \quad \{\![\ \text{by previous property}\ ]\!\} \\
 & N^{\leq} \cup N^{<} \\
= & \quad \{\![\ \text{since } N^{<} \subseteq N^{\leq} \text{ by definition}\ ]\!\} \\
 & N^{\leq}\ .
\end{array}$$

Proof of Lemma 2.2

1.

$$\begin{array}{ll}
 & N^{\leq} \backslash N^{<} \\
= & \quad \{\![\ \text{definition}\ ]\!\} \\
 & (N \cup N^{<}) \backslash N^{<} \\
= & \quad \{\![\ \text{distributivity}\ ]\!\} \\
 & N \backslash N^{<} \cup N^{<} \backslash N^{<} \\
= & \quad \{\![\ \text{set theory}\ ]\!\} \\
 & N \backslash N^{<} \\
= & \quad \{\![\ \text{definition}\ ]\!\} \\
 & \mathsf{max}\, N\ .
\end{array}$$

2.

$$\begin{array}{ll}
 & \mathsf{max}\, N^{\leq} \\
= & \quad \{\![\ \text{definition}\ ]\!\} \\
 & N^{\leq} \backslash (N^{\leq})^{<} \\
= & \quad \{\![\ \text{by Lemma 2.1.4}\ ]\!\} \\
 & N^{\leq} \backslash N^{<}
\end{array}$$

$=$ $\quad\{\![$ by 1 $]\!\}$

$\mathsf{max}\, N$.

3. $N \cap \mathsf{max}\, P$

$=$ $\quad\{\![$ definition $]\!\}$

$N \cap (P \backslash P^{<})$

$=$ $\quad\{\![$ set theory $]\!\}$

$(N \cap P) \backslash P^{<}$

$=$ $\quad\{\![$ by assumption $N \subseteq P$ $]\!\}$

$N \backslash P^{<}$

$\subseteq$ $\quad\{\![$ monotonicity of $^{<}$ and antitonicity of $\backslash$ in its right argument $]\!\}$

$N \backslash N^{<}$

$=$ $\quad\{\![$ definition $]\!\}$

$\mathsf{max}\, N$

4. $\mathsf{max}\,(N \cup P)$

$=$ $\quad\{\![$ definition $]\!\}$

$(N \cup P) \backslash (N \cup P)^{<}$

$=$ $\quad\{\![$ distributivity $]\!\}$

$(N \cup P) \backslash (N^{<} \cup P^{<})$

$=$ $\quad\{\![$ set theory $]\!\}$

$(N \backslash N^{<} \backslash P^{<}) \cup (P \backslash P^{<} \backslash N^{<})$

$=$ $\quad\{\![$ definition $]\!\}$

$(\mathsf{max}\, N) \backslash P^{<} \cup (\mathsf{max}\, P) \backslash N^{<}$.

5. immediate from 4.
6. immediate from 5 by $\mathsf{max}\, N \subseteq N$.

Proof of Lemma 2.3

1. is immediate from the definition and Lemma 2.1.4.
2. is immediate from monotonicity of $^{\leq}$.
3. $(\Leftarrow)$ is immediate from the definition and $N \subseteq N^{\leq}$. For $(\Rightarrow)$ we reason

$N \leq P$

$\Leftrightarrow$ $\quad\{\![$ definition $]\!\}$

$N \subseteq P^{\leq}$

$\Rightarrow$ $\quad\{\![$ by Lemma 2.1.3 $]\!\}$

$N^{\leq} \subseteq (P^{\leq})^{\leq}$

$\Leftrightarrow$ $\quad\{\![$ Lemma 2.1.4 $]\!\}$

$N^{\leq} \subseteq P^{\leq}$.

4. $N \leq P$

$\Leftrightarrow$ $\quad\{\![$ definition $]\!\}$

$$\begin{array}{ll} & N \subseteq P^{\leq} \\ \Rightarrow & \{\![\ \text{monotonicity}\ ]\!\} \\ & N^{<} \subseteq (P^{\leq})^{<} \\ \Leftrightarrow & \{\![\ \text{by Lemma 2.1.4}\ ]\!\} \\ & N^{<} \subseteq P^{<}\ . \end{array}$$

5. immediate from 3,4 and distributivity of $^{\leq}$.
6. $$\begin{array}{ll} & \mathsf{max}\,(N \cup P) \\ = & \{\![\ \text{by Lemma 2.2.1}\ ]\!\} \\ & (N \cup P)^{\leq} \backslash (N \cup P)^{<} \\ = & \{\![\ \text{by assumption } N \leq P \text{ and 5}\ ]\!\} \\ & P^{\leq} \backslash P^{<} \\ = & \{\![\ \text{definition}\ ]\!\} \\ & \mathsf{max}\, P\ . \end{array}$$
7. immediate from 6.
8. immediate from 6.

References

[1] B. Alpern, F.B. Schneider: Defining liveness. Information Processing Letters **21**, 181–185 (1985)

[2] R.-J.R. Back: A calculus of refinements for program derivations. Acta Informatica **25**, 593–624 (1988)

[3] G. Birkhoff: Lattice theory, 3rd edition. American Mathematical Society Colloquium Publications, Vol. XXV. Providence, R.I.: AMS 1967

[4] R.S. Bird, O. de Moor: The algebra of programs. Prentice-Hall 1996 (to appear)

[5] M. Broy: Functional specification of time sensitive communicating systems. In: M. Broy (ed.): Programming and mathematical method. NATO ASI Series, Series F: Computer and Systems Sciences, Vol. **88**. Berlin: Springer 1992, 325–367

[6] M. Broy, K. Stølen: Specification and refinement of finite dataflow networks — a relational approach. In: H. Langmaack, W.-P. de Roever, J. Vytopil (eds.): Formal techniques in real-time and fault-tolerant computing. Lecture Notes in Computer Science **863**. Berlin: Springer 1994, 247–267

[7] R.M. Burstall: Program proving as hand simulation with a little induction. Proc. IFIP Congress 1974. Amsterdam: North-Holland1974, 308–312

[8] B.A. Davey, H.A. Priestley: Introduction to lattices and order. Cambridge: Cambridge University Press 1990

[9] M. Davis: Infinitary games of perfect information. In: M. Dresher, L.S. Shapley, A.W. Tucker (eds.): Advances in game theory. Princeton, N.J.: Princeton University Press 1964, 89–101

[10] F. Dederichs, R. Weber: Safety and liveness from a methodological point of view. Information Processing Letters **36**, 25–30 (1990)

[11] B. Von Karger, C.A.R. Hoare: Sequential calculus. Information Processing Letters **53**, 123–130 (1995)

[12] B. Möller: Ideal streams. In: E.-R. Olderog (ed.): Programming concepts, methods and calculi. IFIP Transactions A-56. Amsterdam: North-Holland 1994, 39–58

[13] B. Möller: Calculating a bounded queue (forthcoming)

[14] C.C. Morgan: Programming from Specifications. Prentice-Hall, 1990.

[15] J.M. Morris: A theoretical basis for stepwise refinement and the programming calculus. Science of Computer Programming **9**, 287–306 (1987)

[16] B. Moszkowski: Some very compositional temporal properties. In: E.-R. Olderog (ed.): Programming concepts, methods and calculi. IFIP Transactions A-56. Amsterdam: North-Holland 1994, 307–326

[17] M. Nivat: Behaviors of processes and synchronized systems of processes. In: M. Broy, G. Schmidt (eds.): Theoretical foundations of programming methodology. Dordrecht: Reidel 1982, 473–551

[18] E.-R. Olderog: Nets, terms and formulas. Cambridge: Cambridge University Press 1991

[19] H.A. Partsch: Specification and transformation of programs — A formal approach to software development. Berlin: Springer 1990

[20] G.D. Plotkin: A powerdomain construction. SIAM J. Computing **5**, 452-487 (1976)

[21] R. Redziejowski: Infinite-word languages and continuous mappings. Theoretical Computer Science **43**, 59–79 (1986)

[22] F.J. Rietman: A relational calculus for the design of distributed algorithms. Dissertation, University of Utrecht, 1995

[23] M.B. Smyth: Power domains. J. Computer Syst. Sciences **16**, 23–36 (1978)

[24] M.B. Smyth: Topology. In: S. Abramsky, D.M. Gabbay, T.S.E. Maibaum (eds.): Handbook of logic in computer science. Vol. 1, Background: Mathematical structures. Oxford: Clarendon Press 1992, 641–761

[25] L. Staiger: Research in the theory of ω-languages. J. Inf. Process. Cybern. EIK **23**, 415–439 (1987)

[26] W. Thomas: Automata on infinite objects. In: J. van Leeuwen (ed.): Handbook of theoretical computer science. Vol. B: Formal models and semantics. Amsterdam: Elsevier 1990, 133–191