A Constructive Theory of Continuous Domains Suitable for Implementation

Andrej Bauer[*] Iztok Kavkler[†]

January 31, 2008

Abstract

We formulate a predicative, constructive theory of continuous domains whose realizability interpretation gives a practical implementation of continuous ω-chain complete posets and continuous maps between them. We apply the theory to implementation of the interval domain and exact real numbers.

1 Introduction

In computation with exact real numbers, and in computable analysis generally, we usually use sequences or streams of approximations to represent reals, or points of a space. We order approximations according to their quality, which leads to order-theoretic constructions of spaces. We took this approach in our implementation of intervals and real numbers *Era* [3], which uses the tool *RZ* [4] to derive specifications (program templates) from axiomatizations of constructive mathematical theories. Therefore, we first looked for a suitable axiomatization of the space of approximations of real numbers. This is a subject studied by domain theory [1, 15]. It turned out that the usual formulations of domains did not quite serve our purposes because their RZ translations were impractical. In this paper we present a predicative constructive theory of continuous predomains whose realizability interpretation allows an efficient implementation of the interval domain, and consequently exact real numbers.

From other implementers of exact real arithmetic, most notably Norbert Müller with iRRAM [13] and Branimir Lambov with RealLib [12, 11], we learned how an efficient implementation of reals should work:

[*]Faculty of Mathematics and Physics, University of Ljubljana, and Institute of mathematics, physics and mechanics, Slovenia. E-mail: `Andrej.Bauer@andrej.com`.

[†]Faculty of Mathematics and Physics, University of Ljubljana, Slovenia. E-mail: `Iztok.Kavkler@fmf.uni-lj.si`.

1. Reals should be represented by sequences of dyadic intervals, i.e., those whose endpoints are rationals of the form $n/2^k$. This allows us to use high-performance numerical libraries such as Numerix [14] and MPFR [9] for low-level calculations.

2. As few conditions as possible should be imposed on the approximating sequences. For example, they should not have a prescribed rate of convergence, and we should not require that each next approximation makes definite progress.[1]

3. Computation is performed in *stages*, where at stage n we compute only with n-th approximations, if possible. This helps curb memory consumption, as we do not have to store information about previous or future approximations.

While other design choices are possible, these ideas have turned out to be successful in practice. They suggest what kind of domain theoretic model we should look at. For example, because elements are represented as sequences of approximations, we should look at posets closed under suprema of chains, rather than arbitrary directed sets. There are many other considerations that one has to take into account to get just the right kind of theory that is suitable for an actual implementation. The main contribution of this paper is to show that theories of constructive mathematics can be "logically engineered" in such a way that their realizability interpretations directly correspond to the practical implementations.

The paper is organized as follows. In Section 2 we discuss constructive logic and our choice of axioms. In Sections 3 and 4 we develop basic constructive theory of predomains and continuous maps, which we apply to the interval domain and real numbers in Section 7. In Section 8 we prove extension theorems for the interval domain, while in the final section we discuss possible improvements to our approach.

2 Predicative constructive logic

We assume familiarity with Bishop style constructive mathematics [6, 7] and the realizability interpretation of constructive logic in a category of modest sets, see e.g. [16, 2, 4].

Our choice of logic and axioms is dictated by the fact that we actually want to implement (the realizability interpretations of) the theories we develop. For example, we reject the general Law of Excluded Middle because it would have to be implemented by (non-existent) Halting Oracle, while powersets are not allowed because they cannot be represented by realizability relations on datatypes.

[1] By requiring definite progress at each step we are forced to artificially represent dyadic intervals by *inexact* approximations.

The realizability interpretation validates the extra-logical principles Number Choice, Dependent Choice, and Markov Principle[2]. Throughout we use Number Choice to choose sequences of representatives from sequences of equivalence classes. Computationally speaking, this is a harmless application of Choice because equivalence classes are represented by their members, anyhow, so there is nothing to choose. We use the closely related Dependent Choice once in Section 3.

We crucially rely on Markov Principle which states that a binary sequence whose terms are not all 0 contains a 1. Again, this is not a matter of taste but a choice that leads to more efficient implementation. As stated in the introduction, we want to represent a real number as a chain of nested intervals $[p_0, q_0] \supseteq [p_1, q_1] \supseteq \cdots$ with rational endpoints whose widths converge to 0. But how do we state the convergence? Unfortunately, the constructively acceptable condition

$$\forall\, k \in \mathbb{N} \,.\, \exists\, n \in \mathbb{N} \,.\, q_n - p_n < 2^{-k} \tag{1}$$

would force us to represent a real as a nested sequence of intervals with an explicitly given modulus of convergence realizing (1). We could avoid the explicit modulus by requiring a fixed rate of convergence, say $q_n - p_n < 2^{-n}$. Implementations of exact real arithmetic along these lines tend to suffer from various inefficiencies. We can express convergence of widths to 0 with the weaker condition

$$\forall\, \epsilon \geq 0 \,.\, ((\forall\, n \in \mathbb{N} \,.\, q_n - p_n \geq \epsilon) \implies \epsilon = 0) \tag{2}$$

which has a trivial realizer and states the same thing, classically. In addition, (2) is precisely what is needed for the chain $([p_n, q_n])_{n \in \mathbb{N}}$ to converge to a maximal element of the interval domain. However, in order to show that every chain satisfying (2) determines a real number we need to know that the sequence $(p_n)_n$ satisfies the Cauchy condition, which it does if Markov Principle holds. Thus we accept it, even though we believe that all efforts should be made to develop constructive mathematics with as few extra-logical principles as possible.

The computational content of Markov Principle is unbounded search, which means that indiscriminate use can result in inefficient implementation. In our case Markov Principle is not used to perform unbounded search but to allow representation of real numbers without explicit information about the speed of convergence of the approximating sequence. The only use of unbounded search occurs at the "top level" when the user explicitly asks for an approximation with given precision.

[2]Caveat: believing that realizability validates Markov Principle requires one to believe in Markov Principle at the meta-level. We do, as we prefer to think that programs which do not run forever terminate.

To summarize, the text is written in Bishop style constructive mathematics without powersets and with Markov Principle. All uses of Markov Principle are explicitly marked, and in fact we do not use it until Section 5. Thus the statements we prove are valid classically, as well as in (relative) realizability models, which cover many well known models of computability.

3 Predomains and their bases

We first review basic order-theoretic definitions. A *partially ordered set (poset)* $(P, \leq)$ is a set P with a reflexive, transitive and antisymmetric relation $\leq$. A *chain* in a poset is a monotone sequence $(a_n)_n$. The supremum of a chain, if it exists, is denoted by $\bigvee^{\uparrow}_n a_n$. An *ω-complete poset (ω-cpo)* $(P, \leq)$ is a poset in which every increasing chain has a supremum. If x and y are elements of a poset P, we say that *x approximates y*, or that *x is way below y*, written $x \ll y$, when for every chain $(a_n)_n$ with a supremum, if $y \leq \bigvee^{\uparrow}_n a_n$ then $x \leq a_n$ for some $n \in \mathbb{N}$. We define $\twoheaddownarrow y = \{x \in P \mid x \ll y\}$. A *$\ll$-chain* is a sequence $(a_n)_n$ which is monotone with respect to $\ll$.

A map $f : P \to Q$ between posets is *continuous* if it is monotone and preserves existing suprema of chains.

It is customary to define the approximation relation and continuous maps only for ω-cpos, but we need definitions that apply to posets. Still, the approximation relation has the usual properties, e.g., $x \leq y \ll z$ or $x \ll y \leq z$ implies $x \ll z$. Continuous maps behave as expected, also. Identities and projections are continuous, continuous maps are closed under composition, and a map of several arguments is continuous if, and only if, it is continuous in each argument separately.

An ω-cpo D is *continuous* when every $x \in D$ is the supremum of a chain in $\twoheaddownarrow x$. A continuous ω-cpo is called a *(continuous) predomain* and one with a least element a *(continuous) domain*. In a predomain D the approximation relation has the property that whenever $x \ll z$ then $x \ll y \ll z$ for some $y \in D$. From this we can prove, using Dependent Choice, that every $x \in D$ is the supremum of a $\ll$-chain $(a_n)_n$, which we call an *approximating sequence* for x. The notion of an approximating sequence makes sense in any poset.

A *base* D_0 for a predomain D is a subset $D_0 \subseteq D$ such that every $x \in D$ is the supremum of a chain in $\twoheaddownarrow x \cap D_0$. Because a predomain D might be a very complex space, an important question is how to find a suitable simple base, and how to reconstruct the predomain from it. For this purpose we first need to identify the structure of a base on its own.

Definition 3.1 A *predomain base* is a poset $(B, \leq)$ in which every element has an approximating sequence.

A predomain base has the usual *interpolation property* which states that, for every finite[3] subset $M \subseteq B$ and $u \in B$,

$$M \ll u \implies \exists v \in B \,.\, M \ll v \ll u \;,$$

where $M \ll u$ means that every element of M is way below u. Indeed, suppose $(a_n)_n$ is an approximating sequence for u. If $M \ll u$ then there is $n \in \mathbb{N}$ such that $w \leq a_n$ for all $w \in M$ but then $M \leq a_n \ll a_{n+1} \ll u$.

If $D_0 \subseteq D$ is a base for a predomain D, then $(D_0, \leq)$ is a predomain base on its own. The interesting question is how to go in the opposite direction and construct a domain out of a predomain base. We shall provide three answers: a construction by rounded ideal completion, an abstract characterization, and a construction suitable for implementation.

3.1 Conditional upper semilattices

We say that x and y in a poset are *bounded* or *consistent*, written $x \uparrow y$, if there is z such that $x \leq z$ and $y \leq z$. A *conditional $\vee$-semilattice (cusl)* is a poset P such that if $x \uparrow y$ then their least upper bound $x \vee y$ exists. Several constructions simplify significantly for predomains that are conditional $\vee$-semilattices. We call them *cusl predomains.*

In a cusl predomain, the consistency relation $\uparrow$ is continuous, by which we mean that, given chains $(a_n)_n$ and $(b_n)_n$, if $a_n \uparrow b_n$ for all $n \in \mathbb{N}$, then $(\bigvee_n a_n) \uparrow (\bigvee_n b_n)$. This is so because $\bigvee_n (a_n \vee b_n)$ exists, and is easily verified to be the supremum of $\bigvee_n a_n$ and $\bigvee_n b_n$.

The base $D_0 \subseteq D$ of a predomain cusl D need not itself be a cusl, and even if it is, the consistency relation in D_0 need not be continuous, so we require these extra properties of D_0, cf. Proposition 3.8.

Proposition 3.2 *Suppose a predomain base B is a cusl. Let $(a_n)_n$ and $(b_n)_n$ are approximating sequences for u and v, respectively. If $u \vee v$ exists then $(a_n \vee b_n)_n$ is its approximating sequence.*

Proof. Because B is a cusl, each $a_n \vee b_n$ exists. We must show that $(a_n \vee b_n)_n$ is a $\ll$-chain whose supremum is $u \vee v$.

It is easily verified that $x \ll y$ and $x' \ll y'$ implies $x \vee y \ll x' \vee y'$, as long as $x \vee y$ and $x' \vee y'$ exist. From this it follows that $(a_n \vee b_n)_n$ is a $\ll$-chain.

The join $u \vee v$ is an upper bound for $(a_n \vee b_n)_n$ because, for every $n \in \mathbb{N}$, $a_n \leq u$ and $b_n \leq v$, hence $a_n \vee b_n \leq u \vee v$. To see that it is the least one, suppose w is an upper bound for $(a_n \vee b_n)_n$. Then w is an upper bound for $(a_n)_n$, hence $u = \bigvee_n a_n \leq w$, and similarly $v \leq w$, therefore $u \vee v \leq w$. ∎

Proposition 3.3 *Suppose a predomain base B is a cusl and $u \ll v \vee w$. Then there exist v', w' such that $u \ll v' \vee w'$, $v' \ll v$, and $w' \ll w$.*

[3]By *finite* we mean Kuratowski finite, or listed by a finite sequence, possibly with repetitions.

Proof. Let $(a_n)_n$ and $(b_n)_n$ be approximating sequences for u and v, respectively. By Proposition 3.2, $(a_n \vee b_n)$ is an approximating sequence for $u \vee v$. There exists $n \in \mathbb{N}$ such that $u \leq a_n \vee b_n$. Taking $v' = a_{n+1}$ and $w' = b_{n+1}$ does the job. ∎

3.2 Completion by rounded ideals

Let $(B, \leq)$ be a predomain base. A *rounded ideal* in B is a subset $I \subseteq B$ such that there exists an $\ll$-chain $(a_n)_n$ in B for which

$$u \in I \iff \exists n \in \mathbb{N} . u \leq a_n .$$

We say that $(a_n)_n$ *generates* the ideal I, which we denote as $I = \langle a_n \rangle_n$. We use lower-case Greek letters for rounded ideals. Needless to say, a rounded ideal in our sense is so in the usual sense: an ideal I is a lower set and whenever $u, v \in I$ then $\{u, v\} \ll w$ for some $w \in I$. But, importantly, we have restricted attention only to those ideals that are generated by $\ll$-chains. This allows us to collect all such ideals into a set $\mathsf{RIdl}(B)$ without resorting to general powersets, because we may define $\mathsf{RIdl}(B)$ as a suitable quotient of the set of all $\ll$-chains in B.

We order the set of rounded ideals $\mathsf{RIdl}(B)$ by inclusion $\subseteq$. For every $u \in B$ the set $\twoheaddownarrow u$ is a rounded ideal because it is generated by an approximating sequence for u. Thus we may define a map $e : B \to \mathsf{RIdl}(B)$ by $e(u) = \twoheaddownarrow u$. It preserves and reflects $\leq$, i.e., $u \leq v$ if, and only if $e(u) \leq e(v)$. For suppose $(a_n)_n$ and $(b_n)_n$ are approximating sequences for u and v, respectively. If $u \leq v$ then every a_m is way below some b_n, hence $e(u) = \langle a_m \rangle_m \subseteq \langle b_n \rangle_n = e(v)$. Conversely, if $e(u) \subseteq e(v)$ then every a_m is way below some b_n, hence $u = \bigvee^{\uparrow}_m a_m \leq \bigvee^{\uparrow}_n b_n = v$. In particular, e is injective and we may view B as a subset of $\mathsf{RIdl}(B)$.

Lemma 3.4 *Suppose $(a_{m,n})_{m,n}$ is a double sequence in a poset such that $(a_{m,n})_n$ is a $\ll$-chain for every m, and whenever $m < n$ then every $a_{m,i}$ is way below some $a_{n,j}$. Then there exists a subsequence $b_i = a_{i,k_i}$ which is a $\ll$-chain and such that every $a_{m,n}$ is way below some b_i.*

Proof. For all $m, n \in \mathbb{N}$ there exists $k \in \mathbb{N}$ such that $a_{i,j} \ll a_{m+1,k}$ for all $0 \leq i \leq m$ and $0 \leq j \leq n$. By Number Choice there is a map $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that $a_{i,j} \ll a_{m+1,c(m,n)}$ for all $0 \leq i \leq m$ and $0 \leq j \leq n$. Define $k_0 = c(0,0)$, $k_{i+1} = c(i, \max(i, k_i))$, and $b_i = a_{i,k_i}$. Observe that $(b_i)_i$ is a $\ll$-chain because $b_i = a_{i,k_i} \ll a_{i+1,c(i,\max(i,k_i))} = a_{i+1,k_{i+1}} = b_{i+1}$. By construction we also have $a_{m,n} \ll b_{\max(m,n)}$ for all $m, n \in \mathbb{N}$. ∎

Proposition 3.5 *The poset $(\mathsf{RIdl}(B), \subseteq)$ is a predomain with a base B.*

Proof. First we show that a chain $(\xi_m)_m$ in $\mathsf{RIdl}(B)$ has a supremum. By Number Choice there exists a double sequence $(a_{m,n})_{m,n}$ such that ξ_m is generated by the $\ll$-chain $(a_{m,n})_n$. Let $(b_i)_i$ be a sequence which we get by applying Lemma 3.4 to $(a_{m,n})_{m,n}$. Clearly, $b_m \in \xi_m$ which shows $\langle b_m \rangle_m \subseteq \bigcup_m \xi_m$. Conversely, if $x \in \bigcup_m \xi_m$ then $x \ll a_{m,n}$ for some $m, n \in \mathbb{N}$, and then $x \ll a_{m,n} \ll b_i$ for some $i \in \mathbb{N}$. This shows $\bigcup_m \xi_m = \langle b_m \rangle_m$.

Next we show that $\mathsf{RIdl}(B)$ is continuous with a base B. Suppose ξ is a rounded ideal generated by a $\ll$-chain $(b_m)_m$. Because $e(b_m) \subseteq e(b_{m+1})$ and $\xi = \bigcup_m e(b_m)$ it suffices to show $e(b_m) \ll \xi$ for all $m \in \mathbb{N}$. If $(\zeta_n)_n$ is a chain whose supremum is ξ then there is $n \in \mathbb{N}$ such that $b_m \in \zeta_n$, hence $e(b_m) \subseteq \zeta_n$. ∎

Proposition 3.6 *The inclusion $e : B \to \mathsf{RIdl}(B)$ preserves and reflects $\ll$ and is continuous.*

Proof. Suppose $u, v \in N$, $u \ll v$, and let $(a_m)_m$ be an approximating sequence for v. There is m such that $u \leq a_m$. If $(\xi_n)_n$ is a chain such that $e(v) \subseteq \bigcup_n \xi_n$ then $a_m \in \xi_n$ for some n, therefore $u \in \xi_n$ from which $e(u) \subseteq \xi_n$ follows.

Conversely, suppose $e(u) \ll e(v)$ and let a_n be a chain in B with a supremum such that $v \leq \bigvee^{\uparrow}_n a_n$. Let $(b_n)_n$ be an approximating sequence for $\bigvee^{\uparrow}_n a_n$. Then $e(v) \subseteq e(\bigvee^{\uparrow}_n a_n) = \langle b_n \rangle_n = \bigcup_n e(b_n)$, hence $e(u) \leq e(b_n)$ for some $n \in \mathbb{N}$. Because e reflects $\leq$ we get $u \leq b_n \ll \bigvee^{\uparrow}_n a_n$, whence $u \ll a_m$ for some $m \in \mathbb{N}$, as required.

It remains to show that e is continuous. Suppose $(a_n)_n$ is a chain in B with supremum $u = \bigvee^{\uparrow}_n a_n$, and let $(b_n)_n$ be an approximating sequence for u. We want to show that $e(u) = \bigcup_n e(a_n)$. Trivially, $e(u) \supseteq \bigcup_n e(a_n)$. For the other inclusion, if $v \in e(u)$ then $v \ll b_n$ for some $n \in \mathbb{N}$. Because $b_n \ll u$ there exists $m \in \mathbb{N}$ such that $b_n \leq a_m$, from which it follows that $v \in e(a_m)$. ∎

Proposition 3.7 *Let B be a predomain base and $f : B \to D$ a continuous map. There exists a unique continuous extension $\overline{f} : \mathsf{RIdl}(B) \to D$ of f along $e : B \to \mathsf{RIdl}(B)$.*

Proof. First we show uniqueness. If both $g : \mathsf{RIdl}(B) \to D$ and $h : \mathsf{RIdl}(B) \to D$ continuously extend f then for every $\xi \in \mathsf{RIdl}(B)$ with $\xi = \langle a_n \rangle_n$ we have

$$g(\xi) = \bigvee^{\uparrow}_n g(e(a_n)) = \bigvee^{\uparrow}_n f(a_n) = \bigvee^{\uparrow}_n h(e(a_n)) = h(\xi) \ .$$

Define $\overline{f} : \mathsf{RIdl}(B) \to E$ by $\overline{f}(\langle a_n \rangle_n) = \bigvee^{\uparrow}_n f(a_n)$. If $\langle a_n \rangle_n = \langle b_n \rangle_n$ then the sequences $(a_n)_n$ and $(b_n)_n$ are interleaved, hence so are $(f(a_n))_n$ and $(f(b_n))_n$, which means that $\bigvee^{\uparrow}_n f(a_n) = \bigvee^{\uparrow}_n f(b_n)$. Thus $\overline{f}$ is well defined.

To see that $\overline{f}$ extends f, consider any $u \in B$ and an approximating sequence $(a_n)_n$ for u. Then

$$\overline{f}(e(u)) = \overline{f}(\langle a_n \rangle_n) = \textstyle\bigvee^{\!\!\uparrow}_n f(a_n) = f(\bigvee^{\!\!\uparrow}_n a_n) = f(u)\ .$$

Finally, we verify that $\overline{f}$ is continuous. Given a chain $(\xi_m)_m$, there is a double sequence $(a_{m,n})_{m,n}$ in B such that $\xi_m = \langle a_{m,n} \rangle_n$. We can find a subsequence $b_i = a_{i,k_i}$ which is a $\ll$-chain and such that every $a_{m,n}$ is way below some b_i. Then it follows that

$$\textstyle\bigvee^{\!\!\uparrow}_m \overline{f}(\xi_m) = \bigvee^{\!\!\uparrow}_m \bigvee^{\!\!\uparrow}_n f(a_{m,n}) = \bigvee^{\!\!\uparrow}_i f(b_i) = \overline{f}(\langle b_i \rangle_i) = \overline{f}(\bigvee^{\!\!\uparrow}_m \xi_m)\ .$$

■

We remark that the previous proof used only *monotonicity* of f to show that the map $\overline{f}$ is well defined and continuous. We needed continuity of f only to show that $f = \overline{f} \circ e$. In fact, for every monotone map $f : B \to D$ there exists the *greatest* continuous $\overline{f} : \mathsf{RIdl}(B) \to D$ such that $f \geq \overline{f} \circ e$. This situation is analogous to the classical treatment of abstract bases for continuous domains [1].

Proposition 3.8 *If a predomain base B is a cusl then so is $\mathsf{RIdl}(B)$ and the embedding $e : B \to \mathsf{RIdl}(B)$ preserves existing binary joins. Furthermore, if the consistency relation on B is continuous, the embedding e reflects it.*

Proof. Suppose $\xi = \langle a_n \rangle_n$ and $\zeta = \langle b_n \rangle_n$ are contained in $\theta = \langle c_n \rangle_n$ in $\mathsf{RIdl}(B)$. For every $n \in \mathbb{N}$, a_n and b_n are bounded by some c_m, therefore $a_n \vee b_n$ exists. We claim that $\eta = \bigcup_n e(a_n \vee b_n)$ is the least upper bound of ξ and ζ. It is an upper bound because $\xi = \bigcup_n e(a_n) \subseteq \bigcup_n e(a_n \vee b_n) = \eta$, and similarly $\zeta \subseteq \eta$. It is the least one because if $\rho = \langle d_n \rangle_n$ is an upper bound for ξ and ζ then, for every $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $a_n \vee b_n \leq d_m$, hence $e(a_n \vee b_n) \subseteq e(d_m) \subseteq \rho$, from which $\eta \subseteq \rho$ follows.

Next we check that e preserves existing joins. Suppose $u \vee v$ exists in B, and let $(a_n)_n$ and $(b_n)_n$ be approximating sequences for u and v, respectively. By Proposition 3.2 $(a_n \vee b_n)_n$ is an approximating sequence for $u \vee v$, and so $e(u \vee v) = \langle a_n \vee b_n \rangle_n$. Because e is monotone $e(u \vee v)$ is an upper bound for $e(u)$ and $e(v)$. If $\xi = \langle c_n \rangle_n$ is another upper bound for $e(u)$ and $e(v)$ then for every $n \in \mathbb{N}$ there is $m \in \mathbb{N}$ such that $a_n \leq c_m$ and $b_n \leq c_m$, but then $a_n \vee b_n \leq c_m$. This shows $e(u \vee v) \subseteq \xi$.

Let us show that $e(u) \uparrow e(v)$ implies $u \uparrow v$ when $\uparrow$ is continuous in B. Let $(a_n)_n$ and $(b_n)_n$ be approximating sequences for u and v, respectively, and suppose $\xi = \langle c_n \rangle_n$ is an upper bound for $e(u)$ and $e(v)$. Then for every n there is m such that both a_n and b_n are below c_m, hence $a_n \uparrow b_n$. By continuity of $\uparrow$ it follows that $u = (\bigvee^{\!\!\uparrow}_n a_n) \uparrow (\bigvee^{\!\!\uparrow}_n b_n) = v$. ■

3.3 A characterization of rounded ideal completion

The most evident characterization of the rounded ideal completion is as reflection from the category of predomain bases and continuous maps to the category of predomains (with chosen bases) and continuous maps. However, we desire an intrinsic characterization which does not refer to all objects of a category.[4]

Theorem 3.9 *Suppose* $(B, \leq)$ *is a predomain base and* $f : B \to D$ *a continuous map into a continuous domain* D*. The following are equivalent:*

1. f *reflects* $\leq$*, preserves* $\ll$*, and for every* $x \in D$ *there exists a chain* $(a_n)_n$ *such that* $x = \bigvee^{\uparrow}_n f(a_n)$*,*

2. *the unique continuous extension* $\overline{f} : \mathsf{RIdl}(B) \to D$ *of* f *is an isomorphism of posets.*

In this situation we say that $f : B \to D$ *is a* (continuous) completion *of* B*.*

Proof. If $\overline{f}$ is an isomorphism, the desired properties of f follow easily because we proved that $e : B \to \mathsf{RIdl}(B)$ has them.

Conversely, suppose f has the stated properties. First we show that the unique continuous extension $\overline{f} : \mathsf{RIdl}(B) \to D$ reflects $\leq$. Suppose $\overline{f}(\langle a_n \rangle_n) \leq \overline{f}(\langle b_m \rangle_m)$, i.e., $\bigvee^{\uparrow}_n f(a_n) \leq \bigvee^{\uparrow}_n f(b_n)$. Because f preserves $\ll$ it holds that $f(a_n) \ll \bigvee^{\uparrow}_m f(b_m)$, therefore $f(a_n) \leq f(b_m)$ for some m. Because f reflects $\leq$ this implies that every a_n is below some b_m, hence $\langle a_n \rangle_n \subseteq \langle b_m \rangle_m$. This shows that $\overline{f}$ reflects $\leq$, an immediate consequence of which is that it is injective.

To see that $\overline{f}$ is surjective, consider an arbitrary $x \in D$. There exists a chain $(a_n)_n$ in B such that $x = \bigvee^{\uparrow}_n f(a_n)$, and then

$$\overline{f}(\textstyle\bigcup_n e(a_n)) = \bigvee^{\uparrow}_n \overline{f}(e(a_n)) = \bigvee^{\uparrow}_n f(a_n) = x.$$

Because $\overline{f}$ is a bijection which preserves and reflects partial order, it is an isomorphism of posets. ∎

3.4 Algebraic predomains and ideal completion

Closely related to continuous domains and completion by rounded ideals are algebraic domains and completion by ideals.

An element $x \in P$ in a poset $(P, \leq)$ is *compact* when $x \ll x$, or equivalently when for every chain $(a_n)_n$ with a supremum in P, $x \leq \bigvee^{\uparrow}_n a_n$ implies $x \leq a_n$ for some $n \in \mathbb{N}$. An ω-cpo D is an *algebraic predomain* when every

[4] In RZ we *can* express the fact that the rounded ideal completion is a reflection, but the resulting specification is somewhat heavy-weight and not easy to use.

$x \in D$ is the supremum of chain of compact elements. Evidently, every algebraic predomain is a continuous predomain with compact elements forming a base.

A poset $(P, \leq)$ may be completed to an algebraic domain as follows. A subset $I \subseteq P$ of a poset $(P, \leq)$ is an *ideal* if there exists a chain $(a_n)_n$ in P such that, for all $u \in P$,

$$u \in I \iff \exists\, n \in \mathbb{N} \,.\, u \leq a_n \;.$$

We denote the ideal generated by a chain $a = (a_n)_n$ by $\langle\!\langle a \rangle\!\rangle = \langle\!\langle a_n \rangle\!\rangle_n$. Just like in the case of rounded ideals, we have restricted to ideals generated by chains. This allows us to form the *ideal completion* $\mathsf{Idl}(P)$ as the set of all ideals without resorting to powersets. Ordered by $\subseteq$, $\mathsf{Idl}(P)$ is an ω-cpo in which suprema of chains are computed as unions. The compact elements of $\mathsf{Idl}(P)$ are precisely those of the form $\downarrow u$, $u \in P$. For every monotone $f : P \to D$ to an ω-cpo D there exists a unique continuous extension $\overline{f} : \mathsf{Idl}(P) \to D$ of f along the embedding $u \mapsto \downarrow u$ of P into $\mathsf{Idl}(P)$. These fact are all very familiar from domain theory so we omit the proofs.

Since ideal completions are simpler than rounded ideal completions, you may wonder why we are bothering with the continuous predomains in the first place. To tell the truth, our implementation indirectly uses algebraic domains, as we describe in the next section. However, we are interested in the (continuous) interval domain on its own merits, and not just as a domain which contains the real numbers. There are many examples where a partial map on the reals is most naturally viewed as a (total) continuous map into the interval domain, e.g., when it has a pole or a sudden jump. Thus we want to understand the structure of the interval domain directly, and not just through a quotient of its algebraic cousin.

3.5 An alternative construction of rounded ideal completion

If $(B, \leq)$ is a domain base we can complete it to $\mathsf{Idl}(B)$ as well as to $\mathsf{RIdl}(B)$. The completions are related by a continuous section-retraction pair. Because every rounded ideal is an ideal, the section $s : \mathsf{RIdl}(B) \to \mathsf{Idl}(B)$ is just inclusion. The retraction $r : \mathsf{Idl}(B) \to \mathsf{RIdl}(B)$ maps an ideal $\langle\!\langle a_n \rangle\!\rangle_n$ to $r(\langle\!\langle a_n \rangle\!\rangle_n) = \bigcup_n \twoheaddownarrow a_n$.

The rounded ideal completion $\mathsf{RIdl}(B)$ has a mathematically pleasing universal property but lacks practical usefulness, because an implementation of $\mathsf{RIdl}(B)$ would represent its elements as $\ll$-chains of basic elements. In the case of the interval domain, see Section 7, this would mean that a real number must be represented by a sequence of *strictly* nested intervals, which we want to avoid. In contrast, the ideal completion does have its elements represented by ordinary chains of basic elements. Thus we may represent elements of $\mathsf{RIdl}(B)$ as ordinary chains if we pass them through the retraction $r : \mathsf{Idl}(B) \to \mathsf{RIdl}(B)$. We work out an explicit description of such a representation.

Let $\mathsf{Chain}(B)$ be the set of chains in B. Because $\langle\!\langle - \rangle\!\rangle : \mathsf{Chain}(B) \to \mathsf{Idl}(B)$ and $r : \mathsf{Idl}(B) \to \mathsf{RIdl}(B)$ are quotient maps, $\mathsf{RIdl}(B)$ is isomorphic to the quotient $\widetilde{B} = \mathsf{Chain}(B)/{\sim}$ by the equivalence relation $\sim$ defined for $a, b \in \mathsf{Chain}(B)$ by

$$a \sim b \iff r(\langle\!\langle a \rangle\!\rangle) = r(\langle\!\langle b \rangle\!\rangle) \ .$$

We denote the equivalence class of a by $[a]$ or $[a_n]_n$. Explicitly, $a \sim b$ means

$$\forall\, u \in B \,.\, ((\exists\, n \in \mathbb{N} \,.\, u \ll a_n) \iff (\exists\, n \in \mathbb{N} \,.\, u \ll b_n)) \ .$$

Similarly, the partial order on $\widetilde{B}$ is given by

$$[a] \leq [b] \iff \forall\, u \in B \,.\, ((\exists\, n \in \mathbb{N} \,.\, u \ll a_n) \implies (\exists\, n \in \mathbb{N} \,.\, u \ll b_n)) \ .$$

The base B is embedded in $\widetilde{B}$ by the map $i : u \mapsto [u]_n$ which maps a basic element u to the constant chain $(u)_n$.

3.6 Computation of suprema of sequences

The supremum of a chain $(x_m)_m$ in $\widetilde{B}$ may be computed as follows. By Number Choice there exists a double sequence $(a_{m,n})_{m,n}$ such that, for every $m \in \mathbb{N}$, $(a_{m,n})_n$ is a $\ll$-chain and $x_m = [a_{m,n}]_n$. The supremum $\bigvee^{\!\nearrow}_m x_m$ equals $[b_i]_i$ where $(b_i)_i$ is obtained from $(a_{m,n})_{m,n}$ by Lemma 3.4. However, because computing with $\ll$-chains is undesirable and the realizer for Lemma 3.4 gives an inefficient algorithm, we seek seek conditions that allow us to improve the calculation.

Suppose then B is a predomain base and let $(x_m)_m$ be a chain in $\widetilde{B}$. As before, there is a double sequence $(a_{m,n})_{m,n}$ in B such that $x_m = [a_{m,n}]_n$, but this time we assume that $(a_{m,n})_n$ is only an ordinary chain. How can we compute $\bigvee^{\!\nearrow}_m x_m$ in terms of $(a_{m,n})_{m,n}$? One may think at first that the sequence $b_n = a_{n,n}$ represents the supremum, but this is not so because it may fail to be a chain, and even if it is, it may still give the wrong value. For a simple counterexample consider $a_{m,n} = \bot$ for $n \leq m$ and $a_{m,n} = u$ otherwise, for a fixed $u > \bot$.

We describe a general method for computing suprema in $\widetilde{B}$ when B is a cusl with continuous consistency relation. In this case we may compute suprema of a sequence $(x_n)_n$ which is not necessarily a chain, as long as its finite prefixes are consistent. So suppose $(x_n)_n$ is a sequence of consistent elements in $\widetilde{B}$, and let $(a_{m,n})_{m,n}$ be a double sequence in B such that $x_m = [a_{m,n}]_n$. The idea is to represent $\bigvee_m x_m$ by a chain $(b_i)_i$ where

$$b_i = a_{0,k(0,i)} \vee a_{1,k(1,i)} \vee \cdots \vee a_{i,k(i,i)} \ . \tag{3}$$

for suitably chosen indices $k(i, j)$. In particular we require the map $k : \{\langle i, j \rangle \mid i \leq j\} \to \mathbb{N}$ to be monotone and unbounded in the second argument:

- for all $i, n \in \mathbb{N}$ there exists $j \geq i$ such that $k(i,j) \geq n$, and
- for all $i, j \in \mathbb{N}$, $k(i,j) \leq k(i,j+1)$.

First observe that the set $\{i(a_{m,n}) \mid m, n \in \mathbb{N}\}$, where $i : B \to \widetilde{B}$ is the embedding, is bounded in $\widetilde{B}$ by an upper bound for $(x_m)_m$, whence by Proposition 3.8 any finite set of terms of $(a_{m,n})_{m,n}$ is bounded in B, so the join in (3) exists. Because $(a_{m,n})_{m,n}$ and k are both monotone in the second argument, $(b_i)_i$ is a chain.

Every $a_{m,n}$ is below some b_i, from which it follows easily that $[b_i]_i$ is an upper bound for $(x_m)_m$. Suppose $[c_\ell]_\ell$ is another upper bound for $(x_m)_m$. If $u \ll b_i$ then by Proposition 3.3 there exist $v_0, \ldots, v_i$ such that $v_j \ll a_{j,k(j,i)}$ and $u \ll v_0 \vee \ldots \vee v_i$. There exists ℓ such that $v_j \leq c_\ell$ for $j = 0, \ldots, i$, therefore $u \ll c_\ell$. This means that $[b_i]_i \leq [c_\ell]_\ell$, which concludes the proof that $\bigvee_m x_m = [b_i]_i$.

Depending on implementation details some choices of k may work better than others. A reasonable one is $k(i,j) = j$, giving us

$$\bigvee_m x_m = \bigvee_m [a_{m,n}]_n = [a_{0,i} \vee a_{1,i} \vee \cdots \vee a_{i,i}]_i = [b_i]_i \ ,$$

which has the advantage that the i-th approximation of the supremum involves only the i-th approximations of terms of the chain $(x_m)_m$. The disadvantage is that a typical calculation of b_i may take i times longer than the calculation of $a_{i,i}$. Assuming each next approximation takes twice as long as the previous one, a better choice for k is

$$k(i,j) = \begin{cases} \lfloor j/2 \rfloor, & \text{if } i \leq \lfloor j/2 \rfloor, \\ i, & \text{otherwise.} \end{cases}$$

Calculating b_i using this sequence typically takes only about twice the time needed for $a_{i,i}$. Naturally, extra information about the chain $(x_m)_m$ or $(a_{m,n})_{m,n}$ can help significantly speed up the computation of $\bigvee_m x_m$.

4 Representation of continuous maps

Suppose D and E are domains with bases D_0 and E_0, respectively, and let $i_D : D_0 \to D$ and $i_E : E_0 \to E$ be the inclusions. We seek a representation of continuous maps $D \to E$ in terms of functions on the underlying bases. Because a continuous map $f : D \to E$ is determined by its restriction $f : D_0 \to E$ and every element in E is the supremum of a chain in E_0, we represent f by a map $f_0 : D_0 \times \mathbb{N} \to E_0$ so that for $u \in D_0$ we have $f(u) = \bigvee_n i_E(f_0(u,n))$. For this to make sense $(f_0(u,n))_n$ must be a chain. We shall require more, namely that f_0 be monotone in *both* arguments so that $u \leq v$ and $m \leq n$ implies $f_0(u,m) \leq f_0(v,n)$. This is expected behavior (better input gives better output), and it also makes it possible to efficiently compute composition of functions in terms of their representatives, see below.

If $f_0 : D_0 \times \mathbb{N} \to E_0$ is monotone in each argument then the map $f : D_0 \to E$, defined by $f(a) = \bigvee^{\uparrow}_n i_E(f_0(a, n))$ is continuous if, and only if,

$$\bigvee^{\uparrow}_n \bigvee^{\uparrow}_m i_E(f_0(a_m, n)) = \bigvee^{\uparrow}_n i_E(f_0(\bigvee^{\uparrow}_m a_m, n)) \tag{4}$$

for every chain $(a_n)_n$ in D_0 that has a supremum in D_0. Indeed, if f_0 satisfies (4) and $(a_m)_m$ is a chain in D_0 with a supremum in D_0 then

$$\begin{aligned}\bigvee^{\uparrow}_m f(a_m) &= \bigvee^{\uparrow}_m \bigvee^{\uparrow}_n i_E(f_0(a_m, n)) = \\ &= \bigvee^{\uparrow}_n \bigvee^{\uparrow}_m i_E(f_0(a_m, n)) = \bigvee^{\uparrow}_n i_E(f_0(\bigvee^{\uparrow}_m a_m, n)) = f(\bigvee^{\uparrow}_m a_m) ,\end{aligned}$$

hence f is continuous. Conversely, if f is continuous then

$$\begin{aligned}\bigvee^{\uparrow}_n \bigvee^{\uparrow}_m i_E(f_0(a_m, n)) &= \bigvee^{\uparrow}_m \bigvee^{\uparrow}_n i_E(f_0(a_m, n)) = \\ &= \bigvee^{\uparrow}_m f(a_m) = f(\bigvee^{\uparrow}_m a_m) = \bigvee^{\uparrow}_n i_E(f_0(\bigvee^{\uparrow}_m a_m, n)) .\end{aligned}$$

Condition (4) can be expressed in terms of bases only. For a monotone f_0 the left-hand side of (4) is less or equal to the right-hand side. The opposite inequality means that for all $u \in E_0$, if $u \ll f_0(\bigvee^{\uparrow}_m a_m, n)$ for some $n \in \mathbb{N}$ then there exists $m \in \mathbb{N}$ such that $u \ll f_0(a_m, n)$. We summarize this in a definition.

Definition 4.1 Let D and E be predomains with bases D_0 and E_0, respectively. A *representation* of a continuous map $f : D \to E$ is a monotone map $f_0 : D_0 \times \mathbb{N} \to E_0$ satisfying, for all $u \in E_0$, $n \in \mathbb{N}$, and chains $(a_m)_m$ in D_0 with supremum in D_0,

$$u \ll f_0(\bigvee^{\uparrow}_m a_m, n) \implies \exists\, m \in \mathbb{N} \,.\, u \ll f_0(a_m, m) .$$

This is equivalent to f_0 satisfying (4).

The map f may be computed from f_0 as follows. If $x \in D$ and $(a_m)_m$ is a chain in D_0 such that $x = \bigvee^{\uparrow}_m i_D(a_m)$ in D, then

$$f(x) = \bigvee^{\uparrow}_n i_E(f_0(a_n)) .$$

In particular, if a continuous map $f : \widetilde{B} \to \widetilde{C}$ is represented by a map $f_0 : B \times \mathbb{N} \to C$ we have the simple relationship $f([a_n]_n) = [f_0(a_n)]_n$. This formula tells us that the value of a continuous maps at stage n depends only on the value of the argument at stage n.

Suppose D, E, F are predomains with bases D_0, E_0, F_0, respectively, and that continuous maps $f : D \to E$ and $g : E \to F$ are represented by $f_0 : D_0 \times \mathbb{N} \to E_0$ and $g_0 : E_0 \times \mathbb{N} \to F$, respectively. Then for every $u \in D_0$

$$\begin{aligned}g(f(u)) &= g(\bigvee^{\uparrow} i_E(f_0(u, n))) = \bigvee^{\uparrow}_n g(i_E(f_0(u, n))) = \\ &= \bigvee^{\uparrow}_n \bigvee^{\uparrow}_m i_F(g_0(f_0(u, n), m)) = \bigvee^{\uparrow}_k i_F(g_0(f_0(u, k), k)) ,\end{aligned}$$

which shows that the composition $h = g \circ f$ is represented by the map $h_0 : D_0 \times \mathbb{N} \to E_0$ defined by $h_0(u,k) = g_0(f_0(u,k),k)$, provided that h_0 is monotone, which it clearly is, and it satisfies (4), which it does because the map $h(u) = \bigvee^{\nearrow}_k h_0(u,k)$ is continuous.

Does every continuous map $f : D \to E$ have a representation? If D_0 is enumerated by $d_0, d_1, \ldots$, by Number Choice there is always a double sequence $(a_{i,j})_{i,j}$ in E_0 such that $f(d_i) = \bigvee^{\nearrow}_n a_{i,j}$. The question then is whether the sequence $(a_{i,j})_{i,j}$, which is monotone in j, can be rectified to a function $f_0 : D_0 \times \mathbb{N} \to E_0$ which is monotone in both arguments. The following proposition covers all cases that we intend to implement.

Proposition 4.2 *Let D be a predomain with a decidable base D_0 which is either finite or countably infinite. Let E be a predomain with base E_0 such that E_0 is a cusl and has finite meets. Then every continuous map $f : D \to E$ has a representation $f_0 : D_0 \times \mathbb{N} \to E_0$.*

Proof. We give the proof for D_0 a countably infinite set. It is easy to adapt the construction to the case when D_0 is finite. Let $(d_i)_i$ be an enumeration of D_0 without repetitions. By Number Choice there exists a double sequence $(a_{i,j})_{i,j}$ in E_0 such that, for all $i \in \mathbb{N}$, $(a_{i,j})_j$ is an approximating sequence for $f(d_i)$. The sets

$$L_i = \{k < i \mid d_k \leq d_i\} \qquad \text{and} \qquad U_i = \{k < i \mid d_i \leq d_k\}$$

are finite decidable subsets of $\mathbb{N}$. Define a map $f_0 : D_0 \times \mathbb{N} \to E_0$ by

$$f_0(d_i, j) = \Big(a_{i,j} \vee \bigvee_{k \in L_i} f_0(d_k, j)\Big) \wedge \bigwedge_{m \in U_i} f_0(d_m, j) \ , \tag{5}$$

where we omit the join if $L_i = \emptyset$ and omit the meet if $U_i = \emptyset$. In particular, this gives us $f_0(d_0, j) = a_{0,j}$. First we verify that f_0 is well defined by showing that the join in (5) exists. More precisely, we prove:

Claim 1: For all $i \in \mathbb{N}$, if $k \in L_i$ then $f_0(d_k, j) \ll f(d_k)$, $f_0(d_i, j)$ is defined, and $f_0(d_i, j) \ll f(d_i)$.

Proof by induction on i: given $i \in \mathbb{N}$ and $k \in L_i$, by induction hypothesis $f_0(d_k, j)$ is defined. Because $d_k \leq d_i$ and f is monotone, $f_0(d_k, j) \ll f(d_k) \leq f(d_i)$. All the terms appearing in the join in (5) are way below $f(d_i)$, therefore they are consistent in E_0, hence the join exists and $f_0(d_i, j)$ is defined. Furthermore, $f_0(d_i, j) \leq a_{i,j} \vee \bigvee_{k \in L_i} f_0(d_k, j) \ll f(d_i)$. The claim is proved.

Monotonicity of f_0 follows from the following two claims.

Claim 2: If $i \in \mathbb{N}$ and $m \in U_i$ then $f_0(i, j) \leq f_0(m, j)$.

Proof: the claim holds because $f_0(m, j)$ appears in the infimum in (5).

Claim 3: If $i \in \mathbb{N}$ and $k \in L_i$ then $f(k, j) \leq f_0(i, j)$.

Proof by induction on i: if $m \in U_i$ then $d_k \leq d_i \leq d_m$, hence either $k \in L_m$ or $m \in U_k$. In the former case, we apply the induction hypothesis to get $f_0(k, j) \leq f_0(m, j)$, while in the latter case we apply claim 2 to get the same conclusion. Therefore, $f_0(k, j)$ is smaller than every term of the infimum appearing in (5). Because $f_0(k, j)$ appears in the supremum in (5) this means $f_0(k, j) \leq f_0(i, j)$. The claim is proved.

To conclude that $f_0(d_i, j)$ is monotone, observe that it is monotone in j because $(a_{i,j})_j$ is monotone in j. It is also monotone in the first argument because, assuming $d_k \leq d_i$, the inequality $f(d_k, j) \leq f(d_i, j)$ is either a triviality, or follows from claim 2, or from claim 3, depending on whether $k = i$, $k > i$, or $k < i$, respectively.

Finally, we prove that $f(d_i) = \bigvee^{\uparrow}_j f_0(d_i, j)$ for all $i \in \mathbb{N}$. Claim 1 implies that $f(d_i) \geq \bigvee^{\uparrow}_j f_0(d_i, j)$. The opposite inequality holds provided that for all $i, k \in \mathbb{N}$, there exists $j \in \mathbb{N}$ such that $f_0(d_i, j) \geq a_{i,k}$, which we prove by induction on i. For every $m \in U_i$ there exists $\ell \in \mathbb{N}$ such that $a_{m,\ell} \geq a_{i,k}$, because $a_{i,k} \ll f(d_i) \leq f(d_m) = \bigvee^{\uparrow}_\ell a_{m,\ell}$. Furthermore, by induction hypothesis there is $j' \in \mathbb{N}$ such that $f_0(d_m, j') \geq a_{m,\ell} \geq a_{i,k}$. As U_i is finite, there exists a single $j' \in \mathbb{N}$ such that $f_0(d_m, j') \geq a_{i,k}$ for all $m \in U_i$. By taking $j = \max(k, j')$ we get

$$f_0(d_i, j) \geq a_{i,j} \wedge \bigwedge_{m \in U_i} f_0(d_m, j) \geq a_{i,j} \wedge a_{i,k} \geq a_{i,k} \; .$$

■

Proposition 4.2 is useful, but not because we would want to apply its realizer to compute a representation f_0 from a map f. Rather, we want to define f by giving f_0, and the proposition tells us that we will always be able to do so.

5 Bases with semidecidable partial order

We would like to use predomain bases as datatypes which represent continuous domains. In order to be able to perform concrete calculations on bases they should not be arbitrarily complicated, which means that we need to impose restrictions on the (logical) complexity of predomain bases.

Recall that a predicate ϕ on a set A is *decidable* when $\phi(x) \vee \neg\phi(x)$ holds for all $x \in A$. This is equivalent to saying that ϕ is represented as a map $\phi : A \to \{0, 1\}$. A predicate ϕ on a set A is *semidecidable* when, for all $x \in A$ there exists $f : \mathbb{N} \to \{0, 1\}$ such that $\phi(x)$ is equivalent to $\exists n \in \mathbb{N} \,.\, f(n) = 1$. A predicate ϕ is *$\neg\neg$-stable* if $\neg\neg\phi(x)$ implies $\phi(x)$ for all $x \in A$.

Under the realizability interpretation decidable and semidecidable predicates correspond to decision and semidecision procedures, respectively, while the $\neg\neg$-stable predicates have no computational content, i.e., their realizers do not compute anything useful and may be omitted. Markov Principle implies that semidecidable predicates are $\neg\neg$-stable.

Without any simplifying assumptions the partial order on the completion of a predomain base cannot be shown $\neg\neg$-stable, which annoyingly requires us to implement realizers for $\leq$. For example, we would have to represent a chain $(x_n)_n$ as a sequence of elements *together with* a sequence of realizers showing that $x_n \leq x_{n+1}$ for all $n \in \mathbb{N}$. We would prefer $\leq$ to be $\neg\neg$-stable.

Proposition 5.1 *Suppose Markov Principle holds. If the partial order on a base is semidecidable then the partial order on the predomain is $\neg\neg$-stable.*

Proof. Suppose D is a predomain and D_0 a base with semidecidable $\leq$. Consider any $x, y \in D_0$. There exist approximating sequences $(a_n)_n$ and $(b_n)_n$ in D_0 for x and y, respectively. It is easily seen that $x \leq y$ is equivalent to

$$\forall\, n \in \mathbb{N} \,.\, \exists\, m \in \mathbb{N} \,.\, a_n \leq b_m \;.$$

This is a $\neg\neg$-stable proposition because the inner existential is, thanks to Markov Principle and the assumption that $\leq$ on D_0 is semidecidable. ∎

Similarly, we would like to avoid implementing explicit realizers for $\ll$. Fortunately, the same simplifying assumption works in the case we care about.

Proposition 5.2 *Suppose D is a predomain and $D_0 \subseteq D$ a base with semidecidable $\leq$. Then the relation $u \ll x$, with $u \in D_0$ and $x \in D$, is semidecidable.*

Proof. Consider any $u \in D_0$ and $x \in D$. There exists an approximating sequence $(a_n)_n$ in D_0 for x. The statement $u \ll x$ is equivalent to the statement $\exists\, n \in \mathbb{N} \,.\, u \leq a_n$, which is semidecidable because $\leq$ restricted to D_0 is semidecidable by assumption. ∎

6 Constructions and examples

6.1 Products

Given posets P and Q, we order $P \times Q$ component-wise by

$$(x, y) \leq (x', y') \iff x \leq x' \wedge y \leq y' \;,$$

where $x, x' \in P$ and $y, y' \in Q$. It follows that

$$(x, y) \ll (x', y') \iff x \ll x' \wedge y \ll y' \;. \tag{6}$$

Indeed, if $x \ll x'$ and $y \ll y'$ and $(x', y') \leq \bigvee^{\uparrow}_n (a_n, b_n)$ then $x \leq a_m$ and $y \leq b_n$ for some $m, n \in \mathbb{N}$ because $\leq$ and $\bigvee^{\uparrow}$ are computed component-wise. Then $(x, y) \leq (a_k, b_k)$ where $k = \max(m, n)$. The converse is similarly easy to check.

If D and E are predomains then the cartesian product $D \times E$ is also a predomain and the projection maps are continuous. Furthermore, using (6) we can show that if D_0 and E_0 are bases for D and E, respectively, then $D_0 \times E_0$ is a base for $D \times E$. It is easily checked that $D \times E$ is a cusl predomain if D and E are.

6.2 Flat domains

For any set A we define the *flat domain* $A_\perp$ as the ideal completion $\mathsf{Idl}(A_0)$ of the set $A_0 = A + \{\mathtt{undef}\}$, ordered by

$$x \leq y \iff x = \mathtt{undef} \lor x = y \; .$$

A map $f : A \to B$ may be extended to a continuous map $f_\perp : A_\perp \to B_\perp$ by

$$f_\perp(\langle\!\langle a_n \rangle\!\rangle_n) = \langle\!\langle b_n \rangle\!\rangle_n$$

where $b_n = \mathtt{undef}$ if $a_n = \mathtt{undef}$ and $b_n = f(a_n)$ if $a_n \in A$. We say that $A_\perp$ and $f_\perp$ are *liftings* of A and f, respectively.

Our first application is the domain Σ of semidecidable truth values, which is the lifting of the singleton set, $\Sigma = \{0\}_\perp$. The smallest element of Σ is $\perp$ and is represented by a constant sequence of `undef`'s. The element $\top$ represented by sequences that contain a 1 is the largest element of Σ.

Proposition 6.1 *A predicate ϕ on a set A is semidecidable if, and only if, it is characterized by a map $\chi : A \to \Sigma$, by which we mean that $\phi(x) \iff \chi(x) = 1$, for all $x \in A$.*

Proof. Suppose ϕ is semidecidable. For each $x \in A$ there exist $f : \mathbb{N} \to 2$ such that $\phi(x) \iff \exists\, n \in \mathbb{N} \,.\, f(n) = 1$. Define the chain $(a_n)_n$ in $\{\mathtt{undef}, 1\}$ by

$$a_n = \begin{cases} 1 & \text{if } \exists\, k \leq n \,.\, f(k) = 1, \\ \mathtt{undef} & \text{otherwise.} \end{cases}$$

and let $\chi(x) = \langle\!\langle a_n \rangle\!\rangle_n$. Now if $\phi(x)$ holds then $(a_n)_n$ contains a 1, hence $\chi(x) = \top$. On the other hand, if $\chi(x) = \top$ then there is $n \in \mathbb{N}$ such that $a_n = 1$, hence $f(m) = 1$ for some $m \leq n$. We see that χ characterizes ϕ.

Conversely, suppose $\chi : A \to \Sigma$ characterizes ϕ. For every $x \in A$ there is a chain $(a_n)_n$ such that $\chi(x) = \langle\!\langle a_n \rangle\!\rangle_n$. Then $\phi(x)$ is equivalent to $\chi(x) = \top$, which in turn is equivalent to $\exists\, n \in \mathbb{N} \,.\, a_n = 1$, so we can take

$$f(n) = \begin{cases} 0 & \text{if } a_n = \mathtt{undef}, \\ 1 & \text{of } a_n = 1. \end{cases}$$

■

It is perhaps worth pointing out that $\{1, \texttt{undef}\}$, ordered as $\texttt{undef} \leq 1$, is *not* an ω-cpo and Σ does *not* coincide with it, unless we accept the non-constructive Limited Principle of Omniscience.[5]

A second example is the domain of *partial booleans* $\mathbb{B} = 2_\perp$. An element of $\mathbb{B}$ is represented by a sequence b_0, b_1, b_2, ... of basic elements, an initial segment of which consists of `undef`'s, and as soon as a term b_i equals 0 or 1, the subsequent terms are equal to it. The domain of partial booleans is used for comparison of real numbers, see Section 7.

6.3 Examples of decidable predomain bases

We constructed flat domains $A_\perp$, Σ and $\mathbb{B}$ as completions by ideals. We would also like to show instances of simple predomain bases that we can complete by rounded ideals. Surprisingly, existence of non-trivial such examples implies Markov Principle.

Proposition 6.2 *Suppose B is a predomain base with decidable partial order and $x, y, z \in B$ such that $x < y \ll z$. Then Markov Principle holds.*

Proof. By $x < y$ we mean $x \leq y$ and $x \neq y$. Suppose $(a_n)_n$ is a sequence of 0's and 1's not all of which are 0. We must show that $a_k = 1$ for some $k \in \mathbb{N}$. Define a chain $(b_n)_n$ in B by

$$b_n = \begin{cases} x & \text{if } \forall\, k \leq n \,.\, a_k = 0, \\ z & \text{otherwise.} \end{cases}$$

Each b_n is equal to x or z and not all of them equal to x. We claim that z is the supremum of $(b_n)_n$. Clearly, z is an upper bound for $(b_n)_n$. If t is another upper bound and $\neg(z \leq t)$ then z does not appear in $(b_n)_n$ because $b_n \leq t$ for all $n \in \mathbb{N}$. But this contradicts the fact that not all b_n are x, therefore $z \leq t$. This proves the claim. Because $y \ll z = \bigvee^{\uparrow}_n b_n$ there exists $n \in \mathbb{N}$ such that $y \leq b_n$. Now $x < y \leq b_n$ implies $b_n = z$, hence $a_k = 1$ for some $k \leq n$. ∎

If Markov Principle holds, examples of predomains bases are easily obtained.

Proposition 6.3 *If Markov Principle holds, a flat domain $A_\perp$ is continuous and $A + \{\texttt{undef}\}$ is its base.*

Proof. We just need to show that $x \ll x$ for every $x \in A + \{\texttt{undef}\}$. If $x = \texttt{undef}$ this is obvious. For the other case, suppose $x \in A$ and $x \leq \bigvee^{\uparrow}_n y_n$. Not all of y_n are `undef`, otherwise we would have $x = \texttt{undef}$. By Markov principle there exists $m \in \mathbb{N}$ such that $y_m \in A$. Because x and y_m are both bounded by $\bigvee^{\uparrow}_n y_n$ we see that $x = y_m = \bigvee^{\uparrow}_n y_n$. ∎

[5] The principle states that every infinite binary sequence is either all zeroes or it contains a one [6]. Its computational power is that of a Halting Oracle.

Lemma 6.4 *Suppose P is a poset with decidable order and $(x_n)_n$ a chain with a supremum such that $x_n < \bigvee^{\uparrow}_k x_k$ for all $n \in \mathbb{N}$. If Markov Principle holds then P is infinite.*

Proof. Consider any $n \in \mathbb{N}$. If $x_n = x_m$ for all $m \geq n$ then $x_n < \bigvee^{\uparrow}_m x_m = x_n$, a contradiction. By Markov Principle and Number Choice we obtain a function $c : \mathbb{N} \to \mathbb{N}$ such that $x_n < x_{c(n)}$ for all $n \in \mathbb{N}$. The sequence $x_0, x_{c(0)}, x_{c(c(0))}, \ldots$ is strictly increasing, hence P is infinite. ∎

Proposition 6.5 *If Markov Principle holds then a finite poset with decidable order is a predomain base in which $\ll$ coincides with $\leq$.*

Proof. Let P be a finite poset with decidable order. It suffices to show that every $x \in P$ is compact. Suppose $(y_n)_n$ is a chain such that $x \leq \bigvee^{\uparrow}_k y_k$. By Lemma 6.4 it is not the case that $y_n < \bigvee^{\uparrow}_k y_k$ for all $n \in \mathbb{N}$. By Markov Principle there exists $n \in \mathbb{N}$ such that $y_n = \bigvee^{\uparrow}_k y_k$, therefore $x \leq y_n$. ∎

We still have not exhibited any predomain bases whose rounded ideal completion differs from the ideal completion. It is time we proceed to our main example, the interval domain.

7 The interval domain and real numbers

Henceforth we assume Markov Principle, as most of the following constructions rely on it. We quickly review our main objects of interest are the real numbers and the interval domain.

Real numbers. The reals $\mathbb{R}$ are characterized as a Cauchy-complete Archimedean ordered field. Because Number Choice is valid, the constructions of real numbers by Dedekind cuts and by Cauchy sequences agree. For every real number $x \in \mathbb{R}$ there exists a sequence of nested intervals $[p_0, q_0] \supseteq [p_1, q_1] \supseteq \cdots$ such that $p_n \leq x \leq q_n$ for all $n \in \mathbb{N}$ and

$$\forall \epsilon > 0 \,.\, \exists n \in \mathbb{N} \,.\, q_n - p_n < \epsilon \,. \tag{7}$$

The endpoints p_n, q_n can be chosen to be rationals, or elements of any dense subset of $\mathbb{R}$ with decidable order. Every sequence of nested intervals $[p_0, q_0] \supseteq [p_1, q_1] \supseteq \cdots$ satisfying (7) determines a unique $x \in \mathbb{R}$ such that $x \in [p_n, q_n]$ for all $n \in \mathbb{N}$, namely x is the limit of Cauchy sequence $(p_n)_n$.

Markov Principle allows us to reformulate (7) as the $\neg\neg$-stable formula

$$\forall \epsilon \geq 0 \,.\, ((\forall n \in \mathbb{N} \,.\, q_n - p_n \geq \epsilon) \implies \epsilon = 0) \,. \tag{8}$$

The implication from (7) to (8) is an easy exercise. For the converse, suppose (8) holds and let $\epsilon > 0$. By Markov Principle it suffices to show $\neg\forall n \in \mathbb{N} \,.\, q_n - p_n \geq \epsilon$: if $\forall n \in \mathbb{N} \,.\, q_n - p_n \geq \epsilon$ then (8) implies $\epsilon = 0$, which contradicts $\epsilon > 0$.

Lower and upper reals. In close relation to the real numbers are the *lower reals* $\mathbb{R}_<$. These are constructed either by lower Dedekind cuts or by bounded *strictly* increasing rational sequences $p_0 < p_1 < p_n < \cdots$. With a slight abuse of notation we denote the lower real represented by such a sequence by $\sup_n p_n$. We define a partial order $\leq$ on $\mathbb{R}_<$ by

$$\sup_n p_n \leq \sup_m q_m \iff \forall n \in \mathbb{N} \,.\, \exists m \in \mathbb{N} \,.\, p_n \leq q_m \;.$$

This also makes it clear that $(p_n)_n$ and $(q_m)_m$ represent the same lower real when each p_n is below some q_m, and vice versa.

While classically the lower reals are isomorphic to the reals, constructively we can only prove that the reals form a subspace of the lower reals, using the fact that every real is the supremum of a strictly increasing rational sequence. Consequently, we must be careful with arithmetic on $\mathbb{R}_<$. We shall only need addition, defined by

$$\sup_n p_n + \sup_n q_n = \sup_n (p_n + q_n) \;.$$

It is an associative and commutative operation with the neutral element $0 = \sup_n(-2^{-n})$. Even though we cannot show constructively that $\mathbb{R}_<$ forms an additive group, there is still a cancellation law.

Proposition 7.1 *For all $x, y, z \in \mathbb{R}_<$, if $x+y \leq x+z$ then $y \leq z$. Therefore, $x + y = x + z$ implies $y = z$.*

Proof. Suppose $x = \sup_n p_n$, $y = \sup_n q_n$, and $z = \sup_n r_n$, and $x + y \leq x + z$. Consider any $n \in \mathbb{N}$. We need to show that $q_n \leq r_m$ for some $m \in \mathbb{N}$. By Markov Principle it suffices to show that $\neg\forall m \in \mathbb{N} \,.\, r_m < q_n$. So suppose $r_m < q_n$ for all $m \in \mathbb{N}$. Let $\epsilon = q_{n+1} - q_n$. We claim that for every $k \in \mathbb{N}$ there exist $k', k'' \geq k$ such that $p_{k'} - p_{k''} > \epsilon$. Let $k \in \mathbb{N}$ be given. Because $x = \sup_i p_{k+i}$ and $x + y \leq x + z$, there exists $m \in \mathbb{N}$ such that $p_{k+n+1} + q_{n+1} \leq p_{k+m} + r_m$, hence $q_{n+1} - r_m \leq p_{k+m} - p_{k+n+1}$ and

$$\epsilon = q_{n+1} - q_n \leq q_{n+1} - r_m \leq p_{k+m} - p_{k+n+1} \;.$$

By taking $k' = k + m$ and $k'' = k + n + 1$ we see that the claim holds. But the claim contradicts the assumption that $(p_n)_n$ is bounded, which concludes the proof. ∎

In fact, the "negation" of $x = \sup_n p_n$ is the *upper* real $-x = \sup_n(-p_n)$. The upper reals $\mathbb{R}_>$ are formed just like $\mathbb{R}_<$, except that strictly decreasing bounded sequences are used. Thus, even though we cannot subtract lower reals from each other, we may subtract an upper real from a lower one, or vice versa.

If $x = \sup_n p_n$ is a lower and $y = \inf_m q_m$ an upper real, we define $x \leq y$ to mean that every p_n is below every q_m, and $y \leq x$ that some q_m is below some p_n.

The interval domain. In classical accounts of domain theory the interval domain is defined as the poset whose elements are closed intervals $[x, y]$ with real endpoints $x, y \in \mathbb{R}$, ordered by reverse inclusion. This is *not* a good constructive definition because the resulting poset fails to be an ω-cpo. The trouble is that a chain $[x_0, y_0] \supseteq [x_1, y_1] \supseteq \cdots$ has a supremum only if the supremum of $(x_n)_n$ and the infimum of $(y_n)_n$ exist. However, knowing just that $(x_n)_n$ is a bounded monotone sequence is not enough to conclude that it has a supremum, unless we assume the Limited Principle of Omniscience. We shall see below that the endpoints of intervals must be lower and upper reals.

We construct the interval domain as the rounded ideal completion of a suitable predomain base. Let $\mathsf{D} \subseteq \mathbb{R}$ be a subring of $\mathbb{R}$ such that $1/2 \in \mathsf{D}$ and $\leq$ restricted to D is decidable. Such a ring is dense in $\mathbb{R}$ and contains the integers. The smallest example is the ring of dyadic rationals $\mathbb{D} = \{a/2^k \mid a, k \in \mathbb{Z}\}$. The fields of rational and algebraic numbers are examples, too. Define the set

$$\mathsf{ID} = \{\langle p, q\rangle \in \mathsf{D} \times \mathsf{D} \mid p \leq q\} + \{\bot\} \ .$$

For $u = \langle p, q\rangle$ we define $\underline{u} = p$ and $\overline{u} = q$ and let $\sqsubseteq$ be a decidable partial order on ID, defined by

$$u \sqsubseteq v \iff u = \bot \lor (u \neq \bot \land v \neq \bot \land \underline{u} \leq \underline{v} \leq \overline{v} \leq \overline{u}) \ .$$

Proposition 7.2 *For all $u, v \in \mathsf{ID}$,*

$$u \ll v \iff u = \bot \lor (u \neq \bot \land v \neq \bot \land \underline{u} < \underline{v} \leq \overline{v} < \overline{u}) \ .$$

Proof. The case $u = \bot$ is easy so we only consider $u \neq \bot$ and $v \neq \bot$. Suppose $u \ll v$. Because $\bigvee^{\uparrow}_n \langle \underline{v} - 2^{-n}, \overline{v} + 2^{-n}\rangle = v$ there exists an $n \in \mathbb{N}$ such that $u \sqsubseteq \langle \underline{v} - 2^{-n}, \overline{v} + 2^{-n}\rangle$, therefore

$$\underline{u} \leq \underline{v} - 2^{-n} < \underline{v} \leq \overline{v} < \overline{v} + 2^{-n} \leq \overline{u} \ .$$

Conversely, suppose $\underline{u} < \underline{v} \leq \overline{v} < \overline{u}$ and $v \leq \bigvee^{\uparrow}_n w_n$. Let $t = \bigvee^{\uparrow}_n w_n$. It is not hard to check that $\underline{t}$ is the supremum of $(\underline{w_n})_n$ in D. Because $\underline{u}$ is strictly smaller than the supremum $\underline{t}$ of $(\underline{w_n})_n$, by Markov Principle there exists $n \in \mathbb{N}$ such that $\underline{u} \leq \underline{w_n}$. Similarly, there exists $m \in \mathbb{N}$ such that $\overline{w}_m \leq \overline{u}$, and then $u \sqsubseteq w_{\max(m,n)}$. ∎

Corollary 7.3 *The poset ID is a predomain base.*

Proof. An approximating chain for $u \in \mathsf{ID}$ is $(\langle \underline{u} - 2^{-n}, \overline{u} + 2^{-n}\rangle)_n$. ∎

The *interval domain* IR is the continuous completion of ID. Concretely, the construction $\mathsf{IR} = \widetilde{\mathsf{ID}}$ is suitable for implementation, while for proving theorems it is sometimes more convenient to take $\mathsf{IR} = \mathsf{RIdl}(\mathsf{ID})$.

For every $x \in \mathsf{IR}$ there is a $\ll$-chain $(u_n)_n$ in ID such that $x = \bigvee^{\uparrow}_n e(u_n)$, where $e : \mathsf{ID} \to \mathsf{IR}$ is the embedding of the base. If $x \neq \bot$ we define $\underline{x} = \sup_n \underline{u}_n$ and $\overline{x} = \inf_n \overline{u}_n$. The values $\underline{x}$ and $\overline{x}$ are independent of the choice of approximating sequence $(u_n)_n$. Conversely, any $a \in \mathbb{R}_<$ and $b \in \mathbb{R}_>$ satisfying $a \leq b$ determine a unique $x \in \mathsf{IR}$ such that $\underline{x} = a$ and $\overline{x} = b$. Thus $\mathsf{IR} \setminus \{\bot\}$ is isomorphic to the set $\{\langle a, b\rangle \in \mathbb{R}_< \times \mathbb{R}_> \mid a \leq b\}$.

Every $x \in \mathsf{IR}$ determines the subset of $\mathbb{R}$

$$\{y \in \mathbb{R} \mid x \neq \bot \implies \underline{x} \leq y \leq \overline{x}\} ,$$

which can be thought of as an interval whose left endpoint is the lower real $\underline{x}$ and the right endpoint is the upper real $\overline{x}$. Because of this we write $x = [\underline{x}, \overline{x}]$ and call the elements of IR *intervals*, and those that are different from $\bot$ *proper intervals*. It is convenient to write $[\underline{x}, \overline{x}] \subseteq [\underline{y}, \overline{y}]$ for $y \sqsubseteq x$ and $u \in [\underline{x}, \overline{x}]$ for $x \neq \bot \implies \underline{x} \leq u \leq \overline{x}$. If x and y are proper intervals, $x \sqsubseteq y$ is equivalent to $\underline{x} \leq \underline{y} \leq \overline{y} \leq \overline{x}$.

The *width* of a proper interval $[\underline{x}, \overline{x}]$ is the upper real $\mathsf{w}(x) = \overline{x} - \underline{x}$. We do not assign a width to $\bot$, and whenever we speak of the width of an interval we tacitly assume it proper.

Lemma 7.4 *For proper intervals x and y:*

1. *if $x \sqsubseteq y$ then $\mathsf{w}(y) \leq \mathsf{w}(x)$, and*
2. *if $x \sqsubseteq y$ and $\mathsf{w}(x) = \mathsf{w}(y)$ then $x = y$.*

Proof. The first statement follows directly from the fact that $x \sqsubseteq y$ is the same as $\underline{x} \leq \underline{y} \leq \overline{y} \leq \overline{x}$. For the second statement, observe that $\overline{y} \leq \overline{x}$ implies $\overline{y} - \underline{x} \leq \overline{x} - \underline{x} = \mathsf{w}(x) = \mathsf{w}(y) = \overline{y} - \underline{y}$, therefore $\underline{y} \leq \underline{x}$ by the cancellation law. The proof of $\overline{x} \leq \overline{y}$ is analogous. ∎

Proposition 7.5 *An interval has zero width if, and only if, it is a maximal element of* IR.

Proof. If $x, y \in \mathsf{IR}$ are proper, $x \sqsubseteq y$, and $\mathsf{w}(x) = 0$ then the first part of Lemma 7.4 implies $\mathsf{w}(y) = 0$, and then the second part implies $x = y$. Therefore, if $\mathsf{w}(x) = 0$ then x is maximal.

Conversely, suppose $x \in \mathsf{IR}$ is maximal. Clearly, it is a proper interval so there exists an approximating sequence $(u_n)_n$ for x such that $\bot \neq u_0$. By Markov Principle $\mathsf{w}(x) = 0$ follows from $\forall k \in \mathbb{N} . \neg(\mathsf{w}(x) \geq 2^{-k})$, which we prove. Suppose $\mathsf{w}(x) \geq 2^{-k}$ and let $q_0, \ldots, q_m \in \mathsf{D}$ be a subdivision of u_0, namely

$$\underline{u}_0 = q_0 \leq q_1 \leq \cdots \leq q_m = \overline{u}_0 ,$$

such that $q_{i+1} - q_i < 2^{-k-1}$. The interval x cannot contain any of the p_i's because $p_i \in x$ and maximality of x would imply $x = [p_i, p_i]$ and $2^{-k} < \mathsf{w}(x) = p_i - p_i = 0$, which is nonsense. By Markov Principle, for each $i = 0, \ldots, m$ there is $n_i \in \mathbb{N}$ such that $p_i \notin u_{n_i}$. Let $N = \max(n_0, \ldots, n_m)$. Because $p_i \notin u_{n_i} \sqsubseteq u_N$ the interval u_N does not contain any p_i's. But this cannot be the case, as the width of u_N is at least twice as large as the gap between two consecutive p_i's. ∎

We can now identify the maximal elements of IR as the real numbers, up to isomorphism. Every real $a \in \mathbb{R}$ determines a maximal interval $[a, a]$, where a plays the role of a lower (upper) real at the left (right) endpoint. Conversely, if the supremum of an approximating sequence $(u_n)_n$ is maximal and $u_n \neq \bot$ for all $n \in \mathbb{N}$, then $(u_n)_n$ satisfies (8) because the width of its supremum is zero. There is then a unique $x \in \mathbb{R}$ such that $x \in u_n$ for all $n \in \mathbb{N}$.

We next describe how to compute with reals in view of the fact that $\mathbb{R}$ is a subspace of IR. The plan is to extend maps on $\mathbb{R}$ to continuous maps on IR, preferably in such a way that the extensions make sense on their own. Because IR with base ID satisfies the conditions of Proposition 4.2, such extensions will have representations that we can actually use to compute the original maps. In this section we consider linear order and limits of Cauchy sequences. Basic arithmetic and general real functions are the topic of Section 8.

Comparison functions. The strict order relation $<$ on $\mathbb{R}$ is semidecidable. By Proposition 6.1 it is characterized by a map $\texttt{less} : \mathbb{R} \times \mathbb{R} \to \Sigma$ which maps (x, y) to $\top$ when $x < y$ and to $\bot$ when $y \leq x$. We can extend it to a map $\texttt{less} : \mathsf{IR} \times \mathsf{IR} \to \Sigma$ so that $\texttt{less}(x, y) = \top$ if, and only if, $\overline{x} < \underline{y}$. A more useful version of comparison function is $\texttt{cmp} : \mathsf{IR} \times \mathsf{IR} \to \mathbb{B}$ such that:

1. $\texttt{cmp}(x, y) = 0$ if $\overline{x} < \underline{y}$,
2. $\texttt{cmp}(x, y) = 1$ if $\overline{y} < \underline{x}$,
3. $\texttt{cmp}(x, y) = \bot$ if x and y are consistent.

Note that this is *not* a definition of $\texttt{cmp}$, because we may not be able to constructively decide which of the three cases holds. Essentially the same definition of a map $c : \mathsf{ID} \times \mathsf{ID} \to \{0, 1, \texttt{undef}\}$,

$$c(u, v) = \begin{cases} 0 & \text{if } \overline{u} < \underline{v}, \\ 1 & \text{if } \overline{v} < \underline{u}, \\ \texttt{undef} & \text{otherwise}, \end{cases}$$

is valid because the base ID has decidable order. We then define

$$\texttt{cmp}(\textstyle\bigvee^{\uparrow}_n u_n, \bigvee^{\uparrow}_n v_n) = \bigvee^{\uparrow}_n c(u_n, v_n).$$

The map c is actually used in Era.

Limits of Cauchy sequences. We would like to compute the limit of a Cauchy sequence as the supremum of a sequence of consistent intervals, as described in Section 3.6.

We say that a real sequence $(r_n)_n$ is a *remainder* sequence for a real sequence $(a_n)_n$ when $m \geq n$ implies $|a_m - a_n| \leq r_n$, for all $m, n \in \mathbb{N}$. The sequence $(a_n)_n$ converges if there are arbitrarily small remainders, i.e., for every $\epsilon > 0$ there is $n \in \mathbb{N}$ such that $r_n < \epsilon$. By Markov Principle, this condition is equivalent to the $\neg\neg$-stable proposition

$$\forall \epsilon \geq 0 \,.\, ((\forall k \in \mathbb{N} \,.\, r_k \geq \epsilon) \implies \epsilon = 0) \;. \tag{9}$$

As the input for computation of the limit of a sequence we take a real sequence $(a_n)_n$ with a remainder sequence $(r_n)_n$ satisfying (9). From this we may form the sequence of proper intervals $x_n = [a_n - r_n, a_n + r_n]$ which are consistent because $a_i - a_j \leq |a_i - a_j| \leq \max(r_i, r_j) \leq r_i + r_j$ implies that every left endpoint $a_i - r_i$ is below every right endpoint $a_j + r_j$. We described the procedure for computing the supremum $y = \bigvee_n x_n$ of such a chain in Section 3.6. Because $\mathsf{w}(y) \leq \mathsf{w}(x_n) = 2r_n$ for all $n \in \mathbb{N}$ and $(r_n)_n$ satisfies (9), $\mathsf{w}(y) = 0$ so that y is a maximal element of IR. It is easily checked that y is the limit of $(a_n)_n$. Observe that we can compute y even if $(r_n)_n$ does not satisfy (9), except that in this case y need not be maximal. In the implementation we require $(r_n)_n$ to be a sequence in D which speeds up the computation, and nothing is gained by allowing r_n's to be real.

8 Extensions of real functions

Every continuous map $\mathsf{IR}^d \to \mathsf{IR}$ has a representation because the conditions of Proposition 4.2 are satisfied. This gives us a way of computing with a real map $\mathbb{R}^d \to \mathbb{R}$, as long as we can extend it continuously to the interval domain. The theoretical question is which real maps can be so extended, and the practical one is how to obtain concrete representations for them. These are the topics of the present section.

Throughout we consider a multivariate real map defined on a subset of $S \subseteq \mathbb{R}^d$. This covers most common functions such as basic arithmetic, including division, and elementary functions. An element $a \in \mathsf{IR}^d$ all of whose components are proper intervals is called a *proper box*. We identify it with the set

$$\{x \in \mathbb{R}^d \mid \forall i \in \{1, \ldots, d\} \,.\, \underline{a}_i \leq x_i \leq \overline{a}_i\} \;,$$

and write $x \in a$ instead of $a \sqsubseteq x$ for $x \in \mathbb{R}^n$. The *width* $\mathsf{w}(a)$ of a proper box is the maximum of the widths of its components.

Lemma 8.1 *Suppose $f : S \to \mathbb{R}$ is a map defined on $S \subseteq \mathbb{R}^n$. Then f has a continuous extension $\overline{f} : \mathsf{IR}^n \to \mathsf{IR}$ if, and only if, there exists a monotone map $g : \mathsf{ID}^n \to \mathsf{IR}$ such that:*

1. *for all $x \in S$ and $a \in \mathsf{ID}^n$, if $x \in a$ then $f(x) \in g(a)$, and*
2. *if a chain $(a_n)_n$ in ID^n converges to $x \in S$ then $\bigvee^{\nearrow}_n g(a_n)$ is a real number, i.e., a maximal element of IR.*

Proof. If f has a continuous extension $\overline{f}$, we may simply take g to be the restriction of $\overline{f}$ to ID^n. For the converse, suppose $g : \mathsf{ID}^n \to \mathsf{IR}$ is monotone and satisfies the stated conditions. Define the map $\overline{f} : \mathsf{IR}^n \to \mathsf{IR}$ by

$$\overline{f}(\langle a_n \rangle_n) = \bigvee^{\nearrow}_n g(a_n) \; .$$

This definition is the same as the definition of continuous extension in Proposition 3.7, except that in the present situation g need not be continuous. Nevertheless, $\overline{f}$ is still well defined and continuous, as was already remarked in the paragraph following the proof of Proposition 3.7. We just need to check that $\overline{f}$ coincides with f. If $x = \langle a_n \rangle_n \in S$ then $x \in a_n$, hence by the first condition $g(a_n) \sqsubseteq f(x)$. Therefore $\overline{f}(x) = \bigvee^{\nearrow}_n g(a_n) \sqsubseteq f(x)$ and then by the second condition $\overline{f}(x)$ is maximal, which implies $\overline{f}(x) = f(x)$. ∎

It is tempting to think that f from the previous lemma must be bounded on closed intervals if the corresponding g exists. But there is a counterexample in the effective topos [10], because in it there exists a continuous real map which is unbounded on a closed interval [16], and Ulrich Berger [5] showed that every real map has a continuous extension to the interval domain.[6]

Lemma 8.1 is not very deep, but it allows us to easily cover the common cases. A basic *open* box in $\mathbb{R}^d$ determined by a proper box $a \in \mathsf{ID}^d$ is the set $\dot{a} = \{x \in \mathbb{R}^d \mid \forall\, i \in \{1, \ldots, n\} \,.\, \underline{a}_i < x_i < \overline{a}_i\}$.

Proposition 8.2 *Suppose $S \subseteq \mathbb{R}^n$ is a countable union of basic* open *boxes. If $f : S \to \mathbb{R}$ is uniformly continuous on every* closed *box contained in S then it has an extension $\overline{f} : \mathsf{IR}^n \to \mathsf{IR}$.*

Proof. Let $(b_k)_k$ be a sequence in ID^n such that $S = \bigcup_{n \in \mathbb{N}} \dot{b}_n$. Define $h : \mathsf{ID}^n \times \mathbb{N} \to \mathsf{IR}$ by

$$h(a, n) = \begin{cases} [\min_{x \in a} f(x), \max_{x \in a} f(x)] & \text{if } \exists\, m \leq n \,.\, b_m \ll a, \\ \bot & \text{otherwise.} \end{cases}$$

The map h is well defined because $b_j \ll a$ implies that $f(x)$ is defined for every $x \in a$, and since f is uniformly continuous it has the minimum and the

[6] To be precise, Berger's result shows that maps can be extended to the *algebraic* interval domain. This does not present a problem because the interval domains is a continuous retract of its algebraic variant, with the retraction-section preserving the real numbers.

maximum on the closed and totally bounded set a. Now define $g : \mathsf{ID}^d \to \mathsf{IR}$ by

$$g(a) = \bigvee\!\!\!\!\nearrow_n h(a, n) \; .$$

Let us verify that g satisfies the conditions of Lemma 8.1. Suppose $x \in S$, $a \in \mathsf{ID}^d$ and $x \in a$. Then $h(a, n) \sqsubseteq f(x)$ for all $n \in \mathbb{N}$, therefore $g(a) = \bigvee\!\!\!\!\nearrow_n h(a, n) \sqsubseteq f(x)$, which is the first condition. If $\bigvee\!\!\!\!\nearrow_n a_n = x \in S$ then, since $x \in \dot{b}_k$ for some $k \in \mathbb{N}$, for sufficiently large n we have $a_n \subseteq S$. Because f is continuous at x the width of $g(a_n)$ can be made as small as desired by sufficiently increasing n. Therefore, $\bigvee\!\!\!\!\nearrow_n g(a_n)$ is maximal. ∎

Corollary 8.3 *Suppose $S \subseteq \mathbb{R}^d$ is a uniformly continuous retract of a countable union of basic open boxes. If $f : S \to \mathbb{R}$ is uniformly continuous on every intersection $S \cap a$ with a closed proper box $a \in \mathsf{IR}^d$ then it has a continuous extension $\overline{f} : \mathsf{IR}^d \to \mathsf{IR}$.*

Proof. Let $T \subseteq \mathbb{R}^d$ be a countable union of basic open boxes and $r : T \to S$ a uniformly continuous retraction, i.e., $r(x) = x$ for $x \in S$. If we apply Proposition 8.2 to the map $f \circ r : T \to \mathbb{R}$ we get the desired extension. ∎

Proposition 8.2 and Corollary 8.3 ensure that basic elementary functions have continuous extensions to the interval domain. The former takes care of $+$, $-$, $\times$, $/$, trigonometric, logarithmic, and exponential functions, and the latter of roots, inverse trigonometric functions, and more. In fact, constructively we cannot exhibit a map $\mathbb{R}^n \to \mathbb{R}$ which fails to satisfy Proposition 8.2.

Realizers for Proposition 8.2, Corollary 8.3, and Proposition 4.2 comprise a general procedure for computing a representation of a continuous extension $\overline{f} : \mathsf{IR}^d \to \mathsf{IR}$ from realizers for $f : S \to \mathbb{R}$ and its uniform continuity on closed boxes. However, such a procedure is extremely inefficient. In practice we *start* with a representation of a continuous $\overline{f} : \mathsf{IR}^d \to \mathsf{IR}$ which coincides with a desired $f : \mathbb{R}^d \to \mathbb{R}$ on maximal elements of IR^d.

It may sound surprising, but already the identity map $\mathrm{id}_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ has a computationally useful representation, called *normalization.* A proper basic interval $[\underline{a}, \overline{a}]$ whose endpoints are dyadic rationals $\underline{a} = m_1 \cdot 2^{e_1}$ and $\overline{a} = m_2 \cdot 2^{e_2}$ takes approximately $\log_2 |m_1| + \log_2 |e_1| + \log_2 |m_2| + \log_2 |e_2|$ bits of memory. In practice the exponents e_1 and e_2 never exceed a fixed size, say 64 bits, but the size of mantissas m_1 and m_2 can quickly grow large. The normalization operation `norm` $: \mathsf{ID} \times \mathbb{N} \to \mathsf{ID}$ takes $\langle [\underline{a}, \overline{a}], n \rangle$ to an interval $[\underline{b}, \overline{b}]$ such that $\underline{b}$ and $\overline{b}$ have at most n-bit mantissas and $b \sqsubseteq a$. For large enough n we have $a = b$, which means that `norm` is a representation in the sense of Definition 4.1. It represents none other than the identity map $\mathrm{id}_{\mathsf{IR}}$. Thus, by composing with `norm` we can always sacrifice a little bit of precision for better space and time complexity.

Addition, subtraction and multiplication are examples of maps $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ which restrict to $\mathsf{D} \times \mathsf{D} \to \mathsf{D}$ and are monotone in each argument, by which we mean that $x_1 \leq x \leq x_2$ and $y_1 \leq y \leq y_2$ implies

$$\min(f(x_1, y), f(x_2, y)) \leq f(x, y) \leq \max(f(x_1, y), f(x_2, y))$$

and

$$\min(f(x, y_1), f(x, y_2)) \leq f(x, y) \leq \max(f(x, y_1), f(x, y_2)) \ .$$

In this case an explicitly given representation of an extension $\overline{f} : \mathsf{IR} \times \mathsf{IR} \to \mathsf{IR}$ is the map $f_0 : \mathsf{ID} \times \mathsf{ID} \times \mathbb{N} \to \mathsf{ID}$ defined by $f_0([a, b], [c, d]) = [m, M]$ where

$$m = \min(f(a, c), f(a, d), f(b, c), f(b, d)) \ ,$$
$$M = \max(f(a, c), f(a, d), f(b, c), f(b, d)) \ .$$

An optimized algorithm does not actually compute all four values $f(a, c)$, $f(a, d)$, $f(b, c)$, and $f(b, d)$, but rather determines the smallest and the largest directly. In the case of $+$, $-$, and $\times$ we get the usual interval arithmetic operations, e.g., $[a, b] + [c, d] = [a + b, c + d]$. We may further compose these with the normalization function `norm` to obtain representations that save space.

Because D may not be a subfield of $\mathbb{R}$, division may not restrict to a map $\mathsf{D} \times (\mathsf{D} \setminus \{0\}) \to \mathsf{D}$. However, since D is dense in $\mathbb{R}$, it has *approximate division* which computes arbitrarily good approximations of quotients. This suffices for a representation of division as an operation on $\mathbb{R}$.

Lastly, let us describe a representation of a typical elementary function. A monotone function, let us take exp, is represented by a map $e : \mathsf{ID} \times \mathbb{N} \to \mathsf{ID}$ that takes $\langle [\underline{a}, \overline{a}], n \rangle$ to $[\underline{b}, \overline{b}]$ such that $\exp(\underline{a}) - 2^{-n} \leq \underline{b} \leq \exp(\underline{a}) \leq \exp(\overline{a}) \leq \overline{b} \leq \exp(\overline{a}) + 2^{-n}$. Numerical libraries such as MPFR [9], GMP [8], and Numerix [14] have readily available routines that compute b from a.

A piece-wise monotone function such as sin is represented by a map $s : \mathsf{ID} \times \mathbb{N} \to \mathsf{ID}$ that computes an output interval from $\langle [\underline{a}, \overline{a}], n \rangle$ in much the same way as e above, except that it first needs to determine how $[\underline{a}, \overline{a}]$ is related to piece-wise monotonicity of sin. Once again, numerical libraries are able to perform these tasks efficiently, so we omit details.

9 Discussion

In this paper we focused on exact real arithmetic within the framework of domain theory. In particular, the interval domain IR was our primary datatype, while the reals $\mathbb{R}$ were viewed as a subspace of IR. We insisted that maps $\mathbb{R}^d \to \mathbb{R}$ be implemented via their domain-theoretic extensions $\mathsf{IR}^d \to \mathsf{IR}$.

It was already observed by Norbert Müeller, Branimir Lambov, and others that one may "sacrifice" the interval domain, or domain theory altogether, to further improve performance of exact real arithmetic. We discuss two such options which we would like to understand better from the domain-theoretic point of view.

First, we may replace the interval domain with a mathematically less elegant, but practically more efficient domain. Too see how this is done, consider an approximating interval $a = [\underline{a}, \overline{a}] \in \mathsf{ID}$. Typically, the dyadic rationals $\underline{a}$ and $\overline{a}$ will take similar amounts of memory, say n bits for each. If the intervals serve only as approximations to real numbers, we do not particularly care about the exact values of their endpoints. In this case it is better to use *lean intervals*, i.e., those of the form $[c - r, c + r]$ where the center c still takes n bits, but the mantissa of r has a fixed small size, say 32 bits. This saves not only half the space compared to $[\underline{a}, \overline{a}]$, but also makes the basic arithmetic functions faster. For example, addition of $[c_1 - r_1, c_1 + r_1]$ and $[c_2 - r_2, c_2 + r_2]$ only requires one long addition $c_1 + c_2$ and one short one $r_1 + r_2$, as opposed to two long additions in case of $[\underline{a}_1, \overline{a}_1] + [\underline{b}_1, \underline{b}_2] = [\underline{a}_1 + \underline{b}_1, \overline{a}_2 + \overline{b}_2]$. The lean intervals form a predomain base whose continuous completion can be used in place of the interval domain because the maximal elements are (isomorphic to) the reals $\mathbb{R}$.

Second, we may relax the notion of approximation and allow an element $x \in D$ of a continuous domain D to be represented by a possibly non-monotone sequence $(a_n)_n$ of elements from a base $D_0 \subseteq D$. The question is what conditions $(a_n)_n$ should satisfy. Clearly, we would expect $x = \bigvee_n a_n$, but this is not enough because continuous maps do not generally preserve non-directed joins. We also need to know when a sequence $(a_n)_n$ in D_0, without a given x, is a representing sequence. Assuming D_0 and D are cusls, the correct condition seems to be that, for all $n \in \mathbb{N}$, $u \in D_0$, and a strictly increasing sequence $(m_i)_{i \in \mathbb{N}}$ of numbers,

$$u \ll a_n \implies \exists\, i \in \mathbb{N} \,.\, u \ll a_{m_i}. \tag{10}$$

Essentially, this says that $(a_n)_n$ converges in the Scott topology on D, but is phrased carefully so that the corresponding realizers are trivial when Markov principle holds and $\ll$ is semidecidable on D_0. While we could well represent the elements of D with such sequences, it is not clear how this would interact with representations of continuous maps.

Too see how non-monotone approximating sequences help improve performance, consider again a lean interval $[c - r, c + r]$. If r is large, it makes little sense to keep a very precise c. By increasing the least significant bit of r we get a slightly larger r' and room for rounding c to a nearby value c' which uses fewer bits. Even though the resulting map $[c-r, c+r] \mapsto [c'-r', c'+r']$ is not monotone we can safely apply it to an approximating sequence for a real number (but not to an approximating sequence for an interval), provided we allow non-monotone sequences. It remains to be seen whether these ideas, which are used in practice, have a domain-theoretic explanation.

Acknowledgment. We thank Martin Escardó, Achim Jung, Branimir Lambov, and Norbert Müller for fruitful discussions.

References

[1] Samson Abramsky and Achim Jung. Domain theory. In S. Abramsky, D. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science Volume 3*, pages 1–168. Oxford University Press, 1994.

[2] A. Bauer. *The Realizability Approach to Computable Analysis and Topology*. PhD thesis, Carnegie Mellon University, 2000. Available as CMU technical report `CMU-CS-00-164`.

[3] Andrej Bauer and Iztok Kavkler. Implementing real numbers with RZ. In Klaus Weihrauch and Ning Zhong, editors, *Fourth International Conference on Computability and Complexity in Analysis*, Electronic Notes in Theoretical Computer Science, 2007.

[4] Andrej Bauer and Christopher Stone. RZ: a tool for bringing constructive and computable mathematics closer to programming practice. In *Computability in Europe 2007*, June 2007. To apear in a special issue of Journal of Logic and Computation.

[5] Ulrich Berger. Total sets and objects in domain theory. *Annals of Pure and Applied Logic*, 60:91–117, 1993.

[6] E. Bishop and D. Bridges. *Constructive Analysis*, volume 279 of *Grundlehren der math. Wissenschaften*. Springer-Verlag, 1985.

[7] Douglas Bridges and Fred Richman. *Varieties of Constructive Mathematics*. Number 97 in London Mathematical Society Lecture Notes Series. Cambridge University Press, 1987.

[8] Torbjörn Granlund et. al. *GNU Multiple Precision Arithmetic Library*. Free Software Foundation. `http://gmplib.org/`.

[9] Guillaume Hanrot, Vincent Lefèvre, Patrick Pélissier, and Paul Zimmermann. *The MPFR Library*. INRIA. `http://www.mpfr.org/`.

[10] J.M.E. Hyland. The effective topos. In A.S. Troelstra and D. Van Dalen, editors, *The L.E.J. Brouwer Centenary Symposium*, pages 165–216. North Holland Publishing Company, 1982.

[11] Branimir Lambov. *Topics in the Theory and Practice of Computable Analysis*. PhD thesis, Department of Computer Science, University of Aarhus, Denmark, December 2005.

[12] Branimir Lambov. RealLib: An efficient implementation of exact real arithmetic. *Mathematical Structures in Computer Science*, 17:81–98, 2007.

[13] Norbert Müller. The iRRAM: Exact arithmetic in C++. In Jens Blanck, Vasco Brattka, and Peter Hertling, editors, *Computability and Complexity in Analysis: 4th International Workshop, CCA 2000 Swansea, UK, September 17, 2000, Selected Papers*, number 2064 in Lecture Notes in Computer Science, pages 222–252. Springer, 2001.

[14] Michel Quercia. *Numerix: Big Integer Library, version 0.22.* INRIA. `http://pauillac.inria.fr/~quercia/`.

[15] V. Stoltenberg-Hansen, I. Lindström, and E.R. Griffor. *Mathematical Theory of Domains.* Number 22 in Cambridge Tracts in Computer Science. Cambridge University Press, 1994.

[16] A.S. Troelstra and D. van Dalen. *Constructivism in Mathematics, An Introduction, Vol. 1.* Number 121 in Studies in Logic and the Foundations of Mathematics. North-Holland, 1988.