Program Extraction for Computing with Higher Order Compact Sets

Dieter Spreen
University of Siegen, 57068 Siegen, Germany
Email: spreen@math.uni-siegen.de

In investigations on exact computations with continuous objects such as the real numbers, objects are usually represented by streams of finite data. This is true for theoretical studies in the Type-Two Theory of Effectivity approach (cf. e.g. [16]) as for practical research, where prevalently the signed digit representation is used (cf. [2, 5, 9]), but also others [6, 7, 15].

For an infinite sequence $p = (p_i)_{i<\omega}$ of signed digits $p_i \in \{-1, 0, 1\}$ set

$$[\![p]\!] \stackrel{\text{Def}}{=} \sum_{i<\omega} p_i 2^{-i} \in [-1, 1].$$

If $x = [\![p]\!]$, then p is called a *signed digit representation* of $x \in [-1, 1]$.

In [1] Berger shows how to use the method of program extraction from proofs to extract certified algorithms working with the signed digit representation in a semi-constructive logic allowing inductive and co-inductive definitions. To this end a predicate $\mathbf{S}$ is defined co-inductively expressing the property that, if $x \in [-1, 1]$ then there are $d \in \{-1, 0, 1\}$ and $y \in [-1, 1]$ such that $x = (y + d)/2$. Classically, $\mathbf{S} = [-1, 1]$, but in Berger's approach it replaces the interval $[-1, 1]$ when working inside the logic.

In addition to producing correct algorithms, this approach allows reasoning in a representation-free way, as in usual mathematical practice. Concrete representations of the objects needed in computations are generated automatically by the extraction procedure.

A detailed description of the logic (i.e. Intuitionistic Fixed Point Logic (IFP)) and the realisability approach used for extracting programs can be found in [4].

Realisers can be thought of a being (idealised, but executable) functional programs. Formally, they are elements of an appropriately constructed Scott domain. In the following conditions $a\,\mathbf{r}\,A$ means that a is a realiser of A:

$$\begin{array}{lcll}
a\,\mathbf{r}\,A & = & a = \mathbf{Nil} \wedge A & (A \text{ disjunction-free}) \\
a\,\mathbf{r}\,(A \vee B) & = & (\exists b)\,(a = \mathbf{Left}(b) \wedge b\,\mathbf{r}\,A) \vee (\exists c)\,(a = \mathbf{Right}(c) \wedge c\,\mathbf{r}\,B) & \\
a\,\mathbf{r}\,(A \wedge B) & = & \mathbf{pr}_0(a)\,\mathbf{r}\,A \wedge \mathbf{pr}_1(a)\,\mathbf{r}\,B & \\
a\,\mathbf{r}\,(\exists x)A(x) & = & (\exists x)a\,\mathbf{r}\,A(x). &
\end{array}$$

There are similar conditions for implication and the universal quantifier. Note that quantifiers are treated uniformly in this version of realisability. Realisers of (co-)inductively defined predicates are defined (co-)inductively again. Thus, if $a\,\mathbf{r}\,\mathbf{S}(x)$, then there are d, y with $x = (y+d)/2$ so that $\mathbf{pr}_0(a)\,\mathbf{r}\,((d = -1 \vee d = 1) \vee d = 0)$ and $\mathbf{pr}_1(a)\,\mathbf{r}\,\mathbf{S}(y)$.

Although IFP is based on intuitionistic logic a fair amount of classical logic is available. For example, soundness of the realisability interpretation used for program extraction holds in the presence of any disjunction-free axioms that are classically true. In case of the reals e.g., one uses a disjunction-free formulation of the axioms of real-closed fields, equations for exponentiation and the defining axiom for max.

In order to generalise from the different finite objects used in the various stream representations, Berger and the present author [3] used the abstract framework of what was coined *digit space*, that is, a bounded complete non-empty metric space X enriched with a finite set D of contractions on X, called *digits*, that *cover* the space, that is

$$X = \bigcup \{\, d[X] \mid d \in D \,\},$$

where $d[X] = \{ d(x) \mid x \in X \}$. In case of the reals with the signed digit representation $X = [-1, 1]$ and $D = \{ \mathrm{av}_i \mid i = -1, 0, 1 \}$, where $\mathrm{av}_i(x) = (x + i)/2$.

Spaces of this kind were studied by Hutchinson [8] in his basic theoretical work on self-similar sets and used later also by Scriven [13] in the context of exact real number computation.

A central aim of the joint research was to lay the foundation for computing with non-empty compact sets and for extracting algorithms for such computations from mathematical proofs. It is a familiar fact that the set $\mathcal{K}(X)$ of non-empty compact subsets of a bounded complete metric space X is a bounded and complete space again with respect to the Hausdorff metric. However, as was shown in [3], in general, there is no finite set of contractions that covers the hyperspace. Therefore, the hyperspace of all non-empty subsets of a digit space is not a digit space.

On the other hand, non-empty compact subsets can be represented in a natural way by finitely branching infinite trees of digits. Moreover, all characterisations in [3] derived for the stream representation of the elements of a digit space hold true for the tree representation of the non-empty compact subsets of the space. In particular it was demonstrated that the approach is of the same computational power as Weihrauch's Type-Two Theory of Effectivity.

In [14] it was shown by the present author that a uniform treatment of both cases—points and non-empty compact subsets—is possible, if the contractions of a digit space are allowed to be multi-ary, leading to the class of *extended digit spaces*. Points are then no longer represented by digit streams but by finitely branching infinite trees. As was shown, not only a uniform version of the results in [3] can be derived but also an analogue of Berger's nested co-inductive inductive characterisation of the (constructively) uniformly continuous endofunctions on the unit interval [1], which allows representing also such functions as finitely branching infinite digit trees.

As we will see next, there is still another obstacle. For compact metric spaces X, Y and finite sets F of contractions $f \colon X \to Y$ we write

$$X \xrightarrow{F} Y \tag{1}$$

to mean that for every $y \in Y$ there are $f \in F$ and $x \in X$ with $y = f(x)$.

Now, let (X, D) be a digit space. As in the example $[-1, 1]$, instead of X we deal with the co-inductively largest predicate $\mathbf{C}_X$ with

$$\mathbf{C}_X(x) \to (\exists d)\, d \in D \wedge (\exists y)\, \mathbf{C}_X(y) \wedge x = d(y).$$

By unfolding this definition we obtain the following co-chain

$$X \xleftarrow{D} X \xleftarrow{D} X \xleftarrow{D} X \leftarrow \cdots \tag{2}$$

.

For X, Y and F as in (1) let $\mathcal{K}(F)$ be the finite set of maps $[f_1, \dots, f_n] \colon \mathcal{K}(X)^n \to \mathcal{K}(Y)$ where the $f_1, \dots, f_n \in F$ are pairwise distinct and $[f_1, \dots, f_n](K_1, \dots K_n) = \bigcup_{\nu=1}^n f_\nu[K_\nu]$. These maps are contractions again with respect to the Hausdorff metric. Moreover, $n \leqslant \|F\|$, because of the distinctness condition. Thus, the arity of the maps in $\mathcal{K}(F)$ is not larger than $\|F\|$. By introducing redundant arguments we let all maps in $\mathcal{K}(F)$ have this arity.

Now, apply $\mathcal{K}$ to the situation in (2). Then we obtain the co-chain

$$\mathcal{K}(X) \xleftarrow{\mathcal{K}(D)} \mathcal{K}(X)^{\|D\|} \xleftarrow{\mathcal{K}(D)^{\|D\|}} (\mathcal{K}(X)^{\|D\|})^{\|D\|} \leftarrow \cdots$$

This is the case where we have to consider extended digit spaces: The maps in $\mathcal{K}(D)$ are no longer unary, in general.

One more application of $\mathcal{K}$ leads to the following co-chain

$$\mathcal{K}^2(X) \xleftarrow{\mathcal{K}(\mathcal{K}(D))} \mathcal{K}(\mathcal{K}(X)^{\|D\|})^{\|\mathcal{K}(D)\|} \xleftarrow{\mathcal{K}(\mathcal{K}(D)^{\|D\|})^{\|\mathcal{K}(D)\|}} \mathcal{K}(\mathcal{K}(X)^{(\|D\|^2)})^{(\|\mathcal{K}(D)\|^2)} \leftarrow \cdots$$

Note here that the maps in $\mathcal{K}(\mathcal{K}(D))$ have compact subsets of $\mathcal{K}(X)^{\|D\|}$ as input, not just compact subsets of $\mathcal{K}(X)$. Hence, they are no longer self-maps of $\mathcal{K}^2(X)$.

This shows that the concept of extended digit spaces is still too narrow to deal with the higher compact hyperspaces. The picture we just used, however, opens up a promising way to follow.

For each co-chain $(Y_{i+1} \xrightarrow{F_i} Y_i)_{i\in\mathbb{N}}$ let

- $\mathfrak{Y} = \sum_{i\in\mathbb{N}} Y_i$ be the topological sum of the Y_i and
- $\mathfrak{F} = \bigcup_{i\in\mathbb{N}}\{i\} \times F_i$ be the disjoint union of the F_i.

Then $(\mathfrak{Y}, \mathfrak{F})$ is an infinite extended iterated function system (IFS). The maps in $\mathfrak{F}$ operate only locally on the components, i.e., for $(i, f) \in \mathfrak{F}$ and $(j_\kappa, y_\kappa) \in \mathfrak{Y}$.

$$(i,f)((j_1,y_1),\dots,(j_{\mathrm{ar}(f)},y_{\mathrm{ar}(f)})) = \begin{cases} (i, f(y_1,\dots,y_{\mathrm{ar}(f)})) \\ \quad \text{if } j_\kappa = i+1,\ (1 \leqslant \kappa \leqslant \mathrm{ar}(f)), \\ \text{undefined} \qquad\qquad \text{otherwise.} \end{cases}$$

Note that $\mathfrak{Y}$ carries a canonical ∞-metric coinciding with the given metrics on the components.

Let $\mathbf{C}_\mathfrak{Y}$ be the co-inductively largest subset of $\mathfrak{Y}$ such that

$$(i,y) \in \mathbf{C}_\mathfrak{Y} \to (\exists f)\, f \in F_i \wedge (\exists z_1,\dots,z_{\mathrm{ar}(f)})$$
$$\bigwedge_{\kappa=1}^{\mathrm{ar}(f)} (i+1, z_\kappa) \in \mathbf{C}_\mathfrak{Y} \wedge (i,y) = (i,f)((i+1,z_1),\dots,(i+1,z_{\mathrm{ar}(f)})).$$

Then (classically) $\mathfrak{Y} = \mathbf{C}_\mathfrak{Y}$. Observe that we are only interested in the points in $\mathbf{C}_\mathfrak{Y}^{\langle 0\rangle} = \{\, y \mid (0,y) \in \mathbf{C}_\mathfrak{Y} \,\}$. The elements in the other components of $\mathfrak{Y}$ appear only as part of the approximation. Note further that though $\mathfrak{F}$ is infinite, the local sets F_i are finite. Moreover, as we have seen in the above consideration, in case we start from a digit space (X, D) and want to deal with sets in $\mathcal{K}^n(X)$, the local components $\mathcal{K}^n(D)_i$ in the co-chain $(\mathcal{K}^n(X)_{i+1} \xrightarrow{\mathcal{K}^n(D)_i} \mathcal{K}^n(X)_i)_{i\in\mathbb{N}}$ depend recursively on i, n.

As mentioned above, the nested co-inductive inductive characterisation of the (constructively) uniformly continuous functions on the unit interval given by Berger [1] was lifted to the general case of extended digit spaces by the present author [14]. The result can be further generalised to the infinite extended IFS introduced above. Let $\mathbf{C}_{\mathbb{F}(\mathfrak{X},\mathfrak{Y})}$ be the class of functions thus obtained and $\mathbf{C}^{(m)}_{\mathbb{F}(\mathfrak{X}^{\langle 0\rangle},\mathfrak{Y}^{\langle 0\rangle})}$ be the subset of those functions of arity $m \in \mathbb{N}$ that map component $\mathbf{C}_{\mathfrak{X}^{\langle 0\rangle}}$ to component $\mathbf{C}_{\mathfrak{Y}^{\langle 0\rangle}}$. These functions will be the morphisms of our category. Among others the following results are obtained:

Theorem 1. *1. The structure* **CDS** *with*

- *Objects:* $\mathbf{C}_\mathfrak{X}^{\langle 0\rangle}$*, for co-chains* $(X_{i+1} \xrightarrow{D_i} X_i)_{i\in\mathbb{N}}$ *of bounded compact metric spaces* X_i *and finite sets* D_i *of contractions* $d\colon X_{i+1} \to X_i$
- *Morphisms:* $\mathbf{C}^{(1)}_{\mathbb{F}(\mathfrak{X}^{\langle 0\rangle},\mathfrak{Y}^{\langle 0\rangle})}$*, the subset of unary* $f \in \mathbf{C}_{\mathbb{F}(\mathfrak{X},\mathfrak{Y}}$ *with* $f[\mathbf{C}_{\mathfrak{X}^{\langle 0\rangle}}] \subseteq \mathbf{C}_{\mathfrak{Y}^{\langle 0\rangle}}$

is a category and $\mathfrak{K}\colon$ **CDS** $\to$ **CDS** *is a monad with unit and multiplication analogous to the case of the power set monad.*

2. Let $(X_{i+1} \xrightarrow{D_i} X_i)_{i\in\mathbb{N}}$ *and* $(Y_{i+1} \xrightarrow{E_i} Y_i)_{i\in\mathbb{N}}$ *be co-chains and* $(\mathfrak{X}, \mathfrak{D})$*,* $(\mathfrak{Y}, \mathfrak{E})$ *the associated infinite IFS. Then for all* $f \in \mathbf{C}^{(1)}_{\mathbb{F}(\mathfrak{X}^{\langle 0\rangle},\mathfrak{Y}^{\langle 0\rangle})}$ *and* $K \in \mathbf{C}^{\langle 0\rangle}_{\mathfrak{K}(\mathfrak{X})}$*,*

(a) $f[K] \in \mathbf{C}^{\langle 0\rangle}_{\mathfrak{K}(\mathfrak{Y})}$*,*

(b) $\mathcal{K}(f) \in \mathbf{C}^{(1)}_{\mathbb{F}(\mathfrak{K}(\mathfrak{X})^{\langle 0\rangle},\mathfrak{K}(\mathfrak{Y})^{\langle 0\rangle})}$.

Here, $(\mathfrak{K}(\mathfrak{X}), \mathfrak{K}(\mathfrak{D}))$ is the infinite extended IFS associated with the co-chain that is obtained by applying $\mathcal{K}$ to $(X_{i+1} \xrightarrow{D_i} X_i)_{i\in\mathbb{N}}$.

Classically, the functions in $\mathbf{C}^{(1)}_{\mathbb{F}(\mathfrak{X}^{\langle 0\rangle},\mathfrak{Y}^{\langle 0\rangle})}$ and $\mathbf{C}^{(1)}_{\mathbb{F}(\mathfrak{K}(\mathfrak{X})^{\langle 0\rangle},\mathfrak{K}(\mathfrak{Y})^{\langle 0\rangle})}$ are uniformly continuous and the sets in $\mathbf{C}^{\langle 0\rangle}_{\mathfrak{K}(\mathfrak{X})}$ are compact. In this case the results are well known [10, 11, 12]. Now, they are formally derived by co-induction, respectively nested induction and co-induction, from which algorithms for computing $f[K]$ and $\mathcal{K}(f)$ can be extracted.

References

[1] U. Berger. From coinductive proofs to exact real arithmetic: theory and applications. *Logical Methods Computer Science* 7(1) (2011) 1–24; doi: 10.2168/LMCS7(1:8)2011.

[2] U. Berger, T. Hou. Coinduction for exact real number computation. *Theory Computing Systems* 43 (2008) 394–409; doi: 10.1007.s0022400790176.

[3] U. Berger, D. Spreen. A coinductive approach to computing with compact sets. *J. Logic Analysis* 8(3) (2016) 1–35; doi: 10.4115/jla.2016.8.3.

[4] U. Berger, H. Tsuiki. Intuitionistic fixed point logic. *Annals Pure Applied Logic* 172 (2021) 102902; doi.org/10.1016/j.apal.2020.102903.

[5] A. Ciaffaglione, P. Di Gianantonio. A certified, corecursive implementation of exact real numbers. *Theoretical Computer Science* 351 (2006) 39–51; doi: 10.1016/j.tcs.2005.09.061.

[6] A. Edalat, R. Heckmann. Computing with real numbers: I. The LFT approach to real number computation; II. A domain framework for computational geometry. In: G. Barthe, P. Dybjer, L. Pinto and J. Saraiva (eds.), *Applied Semantics — Lecture Notes from the International Summer School, Caminha, Portugal*, Springer-Verlag, Berlin (2002), 193–267; doi: 10.1007/35404569965.

[7] A. Edalat, P. Sünderhauf. A domain-theoretic approach to real number computation. *Theoretical Computer Science* 210 (1998) 73–98; doi: 10.1016/S03043975(98)000978.

[8] J.E. Hutchinson. Fractals and self-similarity. *Indiana University Mathematics J.* 30(5) (1981) 713–747.

[9] J.R. Marcial-Romero, M. Hötzel Escardó. Semantics of a sequential language for exact real number computation. *Theoretical Computer Science* 379(12) (2007) 120–141; doi: 10.1016/j.tcs.2007.01.021.

[10] E. Michael. Topologies on spaces of subsets. *Transact. Amer. Math. Soc.* 71 (1951) 152–182.

[11] J.R. Munkres. *Topology*, 2nd ed, Prentice Hall, Upper Sadle River, NJ. (2000).

[12] T. Radul. A functional representation of the hyperspace monad. *Comment. Math. Univ. Carolin.* 38(1) (1997) 165–168.

[13] A. Scriven. A functional algorithm for exact real integration with invariant measures. *Electronic N. Theoretical Computer Science* 218 (2008) 337–353.

[14] D. Spreen. Computing with continuous objects: a uniform co-inductive approach. *Mathematical Structures Computer Science* 31 (2021) 144–192; doi:10.1017/S0960129521000116.

[15] H. Tsuiki. Real number computation through Gray code embedding. *Theoretical Computer Science* 284(2) (2002) 467–485.

[16] K. Weihrauch. *Computable analysis.* Springer-Verlag, Berlin (2000); doi: 10.1007/9783642569999.