Program Extraction for Computing with Higher Order Compact Sets

Dieter Spreen

University of Siegen

15th Tbilisi Symposium on Logic, Language and Computation
Tskaltubo, Georgia, 8–12 September 2025

The research presented in this talk combines two lines of research:

- Program extraction, i.e. the extraction of programs from formal proofs in a constructive logic such as intuitionistic logic extended by inductive and coinductive definitions.

  Such programs are correct by construction. The central tool is a realizability interpretation of the logic.

- Exact real number computation.

  Instead of calculating with floating-point numbers and dealing with rounding and truncation problems, a representation of the real numbers by streams of finite data is used.

  The machine reads the data stream entry by entry, depending on how much information is needed to calculate the result with a certain level of accuracy.

  So the entire calculation is in principle infinite, but for any given accuracy of the result the calculation is finite.

Example (Signed digit representation)

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 the program extraction approach a predicate **S** is defined coinductively expressing the property that

$$x \in [-1, 1] \Rightarrow \bigvee_{d \in \{-1,0,1\}} \bigvee_{y \in [-1,1]} x = (y + d)/2.$$

Classically, $\mathbf{S} = [-1, 1]$, but in the approach it replaces the interval $[-1, 1]$ when working inside the logical calculus.

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:

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

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,

$$\begin{array}{l}
a\,\mathbf{r}\,\mathbf{S}(x) \rightarrow (\exists d)(\exists y)\,x = (y + d)/2 \wedge \\
\qquad \mathbf{pr}_0(a)\,\mathbf{r}\,((d = -1 \vee d = 1) \vee d = 0) \wedge \mathbf{pr}_1(a)\,\mathbf{r}\,\mathbf{S}(y).
\end{array}$$

Definition (Berger, S (2016))

A digit space is a bounded complete nonempty metric space X enriched with a finite set D of contractions $d\colon X \to X$, called digits, that cover the space, i.e.,

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

where $d[X] = \{\, d(x) \mid x \in X \,\}$.

Example (contd.)

$$X = [-1, 1], \quad D = \{\, \mathrm{av}_i \mid i = -1, 0, 1 \,\}, \quad \mathrm{av}_i(x) = (x + i)/2.$$

A central aim of the research in (Berger, S (2016)) was to lay the foundation for computing with nonempty compact sets and for extracting algorithms for such computations from mathematical proofs.

Theorem

If X is a bounded complete metric space, then the set $\mathcal{K}(X)$ of its nonempty compact subsets is a bounded and complete space again with respect to the Hausdorff metric.

Theorem (Berger, S (2016))

In general, there is no finite set of contractions $h\colon \mathcal{K}(X) \to \mathcal{K}(X)$ that covers $\mathcal{K}(X)$.

It follows that $\mathcal{K}(X)$ is not a digit space. However:

Let (X, D) be a digit space and for $d \in D$ and $K \in \mathcal{K}(X)$ set

$$\mathcal{K}(d)(K) = d[K] = \{\, d(x) \mid x \in K \,\}.$$

Then $\mathcal{K}(d)(K) \in \mathcal{K}(X)$. So, we have lifted

$$d\colon X \to X \text{ to a map } \mathcal{K}(d)\colon \mathcal{K}(X) \to \mathcal{K}(X).$$

For $d_1, \dots, d_n \in D$ define

$$[d_1, \dots, d_n] = \bigcup_{\nu=1}^{n} \mathcal{K}(d_\nu).$$

Then $[d_1, \dots, d_n] \colon \mathcal{K}(X)^n \to \mathcal{K}(X)$. Set

$$\mathcal{K}(D) = \{\, [d_1, \dots, d_n] \mid d_1, \dots, d_n \in D \text{ pairwise distinct} \,\}.$$

Theorem (S (2021))

Let (X, D) be a digit space. Then $(\mathcal{K}(X), \mathcal{K}(D))$ is an extended digit space, i.e.,

- *$\mathcal{K}(X)$ is a bounded complete metric space,*
- *$\mathcal{K}(D)$ is a finite set of contractions $\vec{d} \colon \mathcal{K}(X)^{\mathrm{ar}(\vec{d})} \to \mathcal{K}(X)$,*
- *$\mathcal{K}(D)$ covers $\mathcal{K}(X)$.*

Moreover, for $\vec{d} \in \mathcal{K}(D)$, $\mathrm{ar}(\vec{d}) \leqslant \|D\|$.

We would like to iterate this procedure to deal with the higher order compact sets such as compact sets of compact sets. Consider

$$f : \mathcal{K}(X)^2 \to \mathcal{K}(X).$$

Then

$$\mathcal{K}(f) : \mathcal{K}(\mathcal{K}(X)^2) \to \mathcal{K}(\mathcal{K}(X)).$$

- $\mathcal{K}(f)$ is not a self-map of $\mathcal{K}^2(X)$.
- $(\mathcal{K}^2(X), \mathcal{K}^2(D))$ is no longer an extended digit space.

For an extended digit space (Y, E) let $\mathbb{C}_Y$ be a coinductively defined predicate so that

$$\mathbb{C}_Y(y) \to (\exists e)\, e \in E \wedge (\exists \vec{z})\, \mathbb{C}_Y^{\mathrm{ar}(e)}(\vec{z}) \wedge y = e(\vec{z}),$$

which we use to represent the space Y in the logical calculus. Unfold this definition:

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

Notation For spaces X, Y and finite sets F of maps $f : X \to Y$ we write

$$X \xrightarrow{F} Y$$

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

By introducing redundant arguments we let all maps in F have have the same arity.

By unfolding the coinductive definition we obtained the co-chain

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

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

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

This can now be iterated.

The picture opens up a promising way to deal with the general situation.

For each co-chain $(Y_{i+1} \xrightarrow{F_i} Y_i)_{i\in\mathbb{N}}$ of bounded complete metric spaces and finite sets of contractions 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 $(j_\kappa, y_\kappa) \in \mathfrak{Y}$.

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

Note that $\mathfrak{Y}$ carries a canonical ∞-metric coinciding with the given metrics on the components, i.e., the distance between points in different components is ∞, and the distance between points in the same component remains unchanged.

Let $\mathbb{C}_{\mathfrak{Y}}$ be a coinductively defined predicate such that

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

Then (classically) $\mathfrak{Y} = \mathbb{C}_{\mathfrak{Y}}$. $\mathbb{C}_{\mathfrak{Y}}$ is used to represent $\mathfrak{Y}$ in the logical calculus.

Observe that we are only interested in the elements of

$$\mathbb{C}_{\mathfrak{Y}}^{\langle 0\rangle} = \{\, y \mid (0,y) \in \mathbb{C}_{\mathfrak{Y}} \,\}.$$

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.

The typical morphisms between bounded complete metric spaces are uniformly continuous functions.

- Berger (2011) presents a nested coinductive inductive characterization of the uniformly continuous functions $f : [-1, 1] \to [-1, 1]$.
- S (2021) lifts the characterization to the case of uniformly continuous functions between extended digit spaces.

Let $(X_{i+1} \xrightarrow{D_i} X_i)_{i\in\mathbb{N}}, (Y_{i+1} \xrightarrow{E_i} Y_i)_{i\in\mathbb{N}}$ be cochains and $(\mathfrak{X}, \mathfrak{D})$, $(\mathfrak{Y}, \mathfrak{E})$ the associated infinite IFS.
Moreover, for $m > 0$, $j \in \mathbb{N}$, and $j_1 \leqslant \cdots \leqslant j_m \in \mathbb{N}$ let

$$\mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(j)}_{j_1,\ldots,j_m} = \{\, f : \mathfrak{X}^m \rightharpoonup \mathfrak{Y} \mid \operatorname{dom}(f) = \bigtimes_{\nu=1}^{m} (\{j_\nu\} \times X_{j_\nu}) \wedge \operatorname{range}(f) \subseteq \{j\} \times Y_j \,\},$$

$$\mathbb{F}(\mathfrak{X}, \mathfrak{Y})_{j_1,\ldots,j_m} = \bigcup \{\, \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(j)}_{j_1,\ldots,j_m} \mid j \in \mathbb{N} \,\},$$

$$\mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(j)} = \bigcup \{\, \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(j)}_{j_1,\ldots,j_m} \mid j_1 \leqslant \cdots \leqslant j_m \in \mathbb{N} \,\},$$

$$\mathbb{F}(\mathfrak{X}, \mathfrak{Y}) = \bigcup_{m>0, j\in\mathbb{N}} \bigcup_{j_1\leqslant\cdots\leqslant j_m} \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(j)}_{j_1,\ldots,j_m}.$$

The following is a generalisation of U. Berger's coinductive-inductive characterisation of the uniformly continuous functions on the unit interval.

For $F, G \subseteq \mathbb{F}(\mathfrak{X}, \mathfrak{Y})$ define

$$\begin{aligned}\Phi(F)(G) = \{\, f \in \mathbb{F}(\mathfrak{X}, \mathfrak{Y}) \mid \\ & [(\exists (i, e) \in \mathfrak{E})(\exists h_1, \ldots, h_{\mathrm{ar}(e)} \in F \cap \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(i+1)}) \\ & \qquad f = (i, e) \circ (h_1 \times \cdots \times h_{\mathrm{ar}(e)})] \vee \\ & [(\exists j_1 \leqslant \cdots \leqslant j_{\mathrm{ar}(f)} \in \mathbb{N})\, f \in \mathbb{F}(\mathfrak{X}, \mathfrak{Y})_{j_1, \ldots, j_{\mathrm{ar}(f)}} \wedge \\ & \quad (\exists 1 \leqslant \nu \leqslant \mathrm{ar}(f))(\forall d \in D_{j_\nu})\, f \circ (j_\nu, d^{(\nu, \mathrm{ar}(f))}) \in G] \,\}\end{aligned}$$

where

$$\begin{aligned}& d^{(\nu, m)}((j_1, x_1), \ldots, (j_m, x_m)) = \\ & \quad ((j_1, x_1), \ldots, (j_{\nu-1}, x_{\nu-1}), (j_\nu, d(x_\nu)), (j_{\nu+1}, x_{\nu+1}), \ldots, (j_m, x_m)),\end{aligned}$$

for $x_\kappa \in X_{j_\kappa}$ $(\kappa \in \{j_1, \ldots, j_m\} \backslash \{j_\nu\})$ and $x_\nu \in X_{j_\nu + 1}$.

Set

$$\mathcal{J}(F) = \mu\Phi(F).$$

Then $\mathcal{J}(F)$ is the set inductively defined by the following rules:

(W) If $(i, e) \in \mathfrak{E}$ and $h_1, \ldots, h_{\mathrm{ar}(e)} \in F \cap \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(i+1)}$ then

$$(i, e) \circ (h_1 \times \cdots \times h_{\mathrm{ar}(e)}) \in \mathcal{J}(F).$$

(R) If $f \in \mathbb{F}(\mathfrak{X}, \mathfrak{Y})$ and $\nu, j_1, \ldots, j_{\mathrm{ar}(f)} \in \mathbb{N}$ so that

- $j_1 \leqslant \cdots \leqslant j_{\mathrm{ar}(f)}$ and $f \in \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{\nu}_{j_1, \ldots, j_{\mathrm{ar}(f)}}$
- $1 \leqslant \nu \leqslant \mathrm{ar}(f)$ and for all $d \in D_{j_\nu}$, $f \circ d^{(\nu, \mathrm{ar}(f))} \in \mathcal{J}(F)$,

then $f \in \mathcal{J}(F)$.

Set

$$\mathbb{C}_{\mathbb{F}(\mathfrak{X},\mathfrak{Y})} = \nu\mathcal{J} \quad \text{and} \quad \mathbb{C}_{\mathbb{F}(\mathfrak{X}^{\langle 0\rangle},\mathfrak{Y}^{\langle 0\rangle})} = \mathbb{C}_{\mathbb{F}(\mathfrak{X},\mathfrak{Y})} \cap \bigcup\nolimits_{m>0} \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(0)}_{0^{(m)}}$$

where $x^{(m)} = (x, \ldots, x)$ (m times).

Realizers of the elements of $\mathbb{C}_{\mathfrak{X}}^{\langle 0 \rangle}$ are finitely branching infinite trees such that each node of level i is labelled with a digit $d \in D_i$.

A realizer of a map $h \in \mathbb{C}_{\mathbb{F}(\mathfrak{X}^{\langle 0 \rangle}, \mathfrak{Y}^{\langle 0 \rangle}}^{\langle 0 \rangle}$ is a finitely branching infinite tree such that each node a level i is either a

- writing node labelled with a digit $e \in E_i$ and $\mathrm{ar}(e)$ immediate subtrees, or a
- reading node labelled with R_ν^i and $\|D_i\|$ subtrees.

Writing nodes correspond to (inverted) Rule (W) and reading nodes to (inverted) Rule (R).

The condition that every path contains infinitely many writing nodes is reflected by the coinductive nature of the definition of $\mathbb{C}_{\mathfrak{X}}^{\langle 0 \rangle}$ (greatest fixed point w.r.t. F).

The inductive part of the definition (least fixed point w.r.t. G) reflects the fact that between two writing nodes on a path there should only be finitely many reading nodes.

Such trees can easily be interpreted as tree transducers: Given $\mathrm{ar}(h)$ trees $T_1, \ldots, T_{\mathrm{ar}(h)}$ as inputs, run through the tree and output a tree in as follows:

1. At a writing node $[e; S_1, \ldots, S_{\mathrm{ar}(e)}]$ output e and continue with the subtrees $S_1, \ldots, S_{\mathrm{ar}(e)}$.
2. At a reading node $[R^i_\nu; (S'_d)_{d \in D_i}]$ continue with S'_d, where d is the root of T_ν, and replace T_ν by its $\mathrm{ar}(d)$ immediate subtrees.

(W) If $(i, e) \in \mathfrak{E}$ and $h_1, \ldots, h_{\mathrm{ar}(e)} \in F \cap \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^{(i+1)}$ then

$$(i, e) \circ (h_1 \times \cdots \times h_{\mathrm{ar}(e)}) \in \mathcal{J}(F).$$

(R) If $f \in \mathbb{F}(\mathfrak{X}, \mathfrak{Y})$ and $\nu, j_1, \ldots, j_{\mathrm{ar}(f)} \in \mathbb{N}$ so that

- $j_1 \leqslant \cdots \leqslant j_{\mathrm{ar}(f)}$ and $f \in \mathbb{F}(\mathfrak{X}, \mathfrak{Y})^\nu_{j_1, \ldots, j_{\mathrm{ar}(f)}}$
- $1 \leqslant \nu \leqslant \mathrm{ar}(f)$ and for all $d \in D_{j_\nu}$, $f \circ d^{(\nu, \mathrm{ar}(f))} \in \mathcal{J}(F)$,

then $f \in \mathcal{J}(F)$.

Theorem (Berger (2011), S (2021))

Let $f \in \mathbb{F}(\mathfrak{X}, \mathfrak{Y})$. *Then*

$$f \in \mathbb{C}_{\mathbb{F}(\mathfrak{X},\mathfrak{Y})} \Leftrightarrow f \text{ uniformly continuous (constructively).}$$

Theorem

For all $f \in \mathbb{C}^{(1)}_{\mathbb{F}(\mathfrak{X}^{\langle 0\rangle},\mathfrak{Y}^{\langle 0\rangle})}$ *and* $K \in \mathbb{C}^{\langle 0\rangle}_{\mathfrak{K}(\mathfrak{X})}$,

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

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

Classically, the functions in $\mathbb{C}^{(1)}_{\mathbb{F}(\mathfrak{X}^{\langle 0\rangle},\mathfrak{Y}^{\langle 0\rangle})}$ are uniformly continuous and the sets in $\mathbb{C}^{\langle 0\rangle}_{\mathfrak{K}(\mathfrak{X})}$ are compact. Then the results are well known: Compact images of compact sets are compact and the functor $\mathcal{K}$ maps uniformly continuous functions to uniformly continuous functions.

Theorem

The following assertions hold:

1. $\{\bigcup \mathbb{K} \mid \mathbb{K} \in \mathbb{C}^{\langle 0 \rangle}_{\mathfrak{K}^2(\mathfrak{X})}\} \subseteq \mathbb{C}^{\langle 0 \rangle}_{\mathfrak{K}(\mathfrak{X})}$.
2. $\bigcup \in \mathbb{C}^{\langle 0 \rangle}_{\mathbb{F}(\mathfrak{K}^2(\mathfrak{X})^{\langle 0 \rangle}, \mathfrak{K}(\mathfrak{X})^{\langle 0 \rangle})}$.

Classically, the first statement is a famous result by E. Micheal (1951): The compact union of a nonempty compact set of nonempty compact sets is compact again.

The proofs of both theorems use a more geometrical kind of reasoning as usual in topology.

Now, both theorems are formally derived with the help of coinduction, respectively nested induction/coinduction, from which algorithms can be extracted.