Digit Spaces — Topological Foundations

Dieter Spreen
University of Siegen

Interval Analysis and Constructive Mathematics
CMO-BIRS workshop, Oaxaca, 13-18 November 2016

Acknowledgement

The results presented in this talk are based on insights obtained in collaborations and discussions with Ulrich Berger and Hideki Tsuiki.

1. Infinitary objects generated via co-inductive definitions

A central issue in computing is to have programs the correctness of which has formally been verified. An important idea to achieve this is by extracting a program from a formal proof of a problem specification.

We cannot compute with abstract and infinitary objects directly. But we can compute with their representations, streams or trees. Obviously, both, streams and trees over a finite alphabet can be generated co-inductively.

The idea is now, not to deal with the representations directly, but to have the representations be generated stepwise by the extracted programme. To this end one tries to find a co-inductive characterisation for the spaces under investigation and to construct proofs on the basis of these definitions instead of the classical ones.

The central notion in Berger's abstract framework is the digit space.

Definition (U. Berger)

A digit space (X, D) consists of a bounded and complete nonempty metric space (X, μ) and a finite set D of contractions on X, called digits, that cover X, that is,

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

Thus, every digit space is a compact Hausdorff space.

Aim.

- Develop the theory for compact Hausdorff spaces.
- Allow digit maps to be multi-ary.

2. Digit spaces

Let

- (X, τ) be a topological Hausdorff space and
- $\mathbb{C}(X) = \{ f \colon X^m \to X \mid f \text{ continuous } \wedge m \geq 1 \}$.

For $f \in \mathbb{C}(X)$, let $\mathrm{ar}(f)$ denote its arity.

For $D \subseteq \mathbb{C}(X)$, (X, D) is covering if

$$X = \bigcup \{ d[X^{\mathrm{ar}(d)}] \mid d \in D \}.$$

Definition

A digit space (X, D) consists of a compact Hausdorff space (X, τ) and a finite subset $D \subseteq \mathbb{C}(X)$ so that (X, D) is covering.

Define $\mathcal{C}_X$ co-inductively to be the largest subset of X such that for all $x \in X$,

$$x \in \mathcal{C}_X \Rightarrow (\exists d \in D)(\exists y_1, \ldots, y_{\mathrm{ar}(d)} \in \mathcal{C}_X)x = d(y_1, \ldots, y_{\mathrm{ar}(d)}).$$

Lemma

$\mathcal{C}_X = X.$

Proof.

By definition, $\mathcal{C}_X \subseteq X$. The converse inclusion follows by coinduction. Note that by the covering property of X, the defining implication of $\mathcal{C}_X$ is true if $\mathcal{C}_X$ is replaced by X. $\square$

Let $\mathcal{T}_D$ be the set of all finitely branching trees with nodes $d \in D$ such that every node d has exactly $\mathrm{ar}(d)$ immediate successor nodes. Trees of this kind are called digital trees. Obviously, every path in a digital tree is infinite.

Write $T = [d; T_1, \dots, T_{\mathrm{ar}(d)}]$ to denote that d is the root of T and $T_1, \dots, T_{\mathrm{ar}(d)}$ are the immediate subtrees.

For $m \geq 0$ and $T \in \mathcal{T}_D$, the initial segment $T^{(m)}$ of T of hight m is recursively defined as follows:

$$T^{(0)} = \emptyset$$

$$T^{(m+1)} = [d; T_1^{(m)}, \dots, T_{\mathrm{ar}(d)}^{(m)}], \text{ if } T = [d; T_1, \dots, T_{\mathrm{ar}(d)}].$$

Set

$$\operatorname{ar}(T^{(0)}) = 1, \qquad \operatorname{ar}(T^{(m+1)}) = \sum_{i=1}^{\operatorname{ar}(d)} \operatorname{ar}(T_i^{(m)}).$$

Then the arity of $T^{(m)}$ is the sum of the arities of the digits at its leaves.

Each initial subtree $T^{(m)}$ of T defines a continuous map $T^{(m)} \colon X^{\operatorname{ar}(T^{(m)})} \to X$ by

$$\begin{aligned} T^{(0)} &= \mathrm{id}_X \\ T^{(m+1)} &= d \circ (T_1^{(m)}, \ldots, T_{\operatorname{ar}(d)}^{(m)}). \end{aligned}$$

Co-inductively, define Val to be the largest subset of $\mathcal{T}_D \times \mathcal{C}_X$ so that for all $(T, x) \in \mathcal{T}_D \times \mathcal{C}_X$,

$$(T, x) \in \mathrm{Val} \Rightarrow (\exists d \in D)(\exists (T_1, x_1), \ldots, (T_{\mathrm{ar}(d)}, x_{\mathrm{ar}(d)}) \in \mathrm{Val}) \\ T = [d; T_1, \ldots, T_{\mathrm{ar}(d)}] \wedge x = d(x_1, \ldots, x_{\mathrm{ar}(d)}).$$

Lemma

For all $(T, x) \in \mathrm{Val}$ and $m \geq 0$, $x \in T^{(m)}[X^{\mathrm{ar}(T^{(m)})}]$.

Hence,

$$x \in \bigcap_{m \geq 0} T^{(m)}[X^{\mathrm{ar}(T^{(m)})}].$$

Note that $\bigcap_{m \geq 0} T^{(m)}[X^{\mathrm{ar}(T^{(m)})}] \neq \emptyset$, as X is compact.

Definition

(X, D) is weakly hyperbolic, if for all $T \in \mathcal{T}_D$,

$$\|\bigcap_{m\geq 0} T^{(m)}[X^{\mathrm{ar}(T^{(m)})}]\| \leq 1.$$

For what follows, let (X, D) be weakly hyperbolic. Then Val is the graph of a function $[\![\cdot]\!]$ with

$$[\![[d; T_1, \dots, T_{\mathrm{ar}(d)}]]\!] = d([\![T_1]\!], \dots, [\![T_{\mathrm{ar}(d)}]\!]).$$

Lemma

$\mathrm{range}([\![\cdot]\!]) \subseteq \mathbb{C}_X$.

By the definition of $\mathbb{C}_X$, a digital tree T with $[\![T]\!] = x$ can stepwise be constructed starting from the root, for every $x \in \mathbb{C}_X$.

Proposition

$[\![\cdot]\!]\colon \mathcal{T}_D \to \mathbb{C}_X$ *is surjective.*

Proposition

For all open subsets O of X and all $T \in \mathcal{T}_D$ with $[\![T]\!] \in O$ there is some $n \geq 0$ so that $T^{(n)}[X^{\mathrm{ar}(T^{(n)})}] \subseteq O$.

Note that $\mathcal{T}_D$ comes equipped with a canonical metric

$$\delta(S, T) = \begin{cases} 0 & S = T, \\ 2^{-\min\{\, n \geq 1 \mid S^{(n)} \neq T^{(n)} \,\}} & \text{otherwise.} \end{cases}$$

Lemma

$(\mathcal{T}_D, \delta)$ *is bounded and complete, hence compact.*

Corollary

$[\![\cdot]\!]$ *is continuous.*

Theorem

Let (X, τ) be a compact Hausdorff space. Then there is exactly one separating uniformity $\mathfrak{U}$ on X with the following properties:

1. *$\mathfrak{U}$ is compatible with topology τ.*
2. *$\mathfrak{U}$ consists of all neighbourhoods of the diagonal Δ in $X \times X$ furnished with the product topology.*
3. *$(X, \mathfrak{U})$ is a complete uniform space.*
4. *For a finite open covering $\mathcal{C} = \{C_1, \ldots, C_n\}$ let*

$$U_{\mathcal{C}} = \bigcup\nolimits_{i=1}^{n} C_i \times C_i.$$

Then the collection of all such neighbourhoods $U_{\mathcal{C}}$ is a fundamental system of $\mathfrak{U}$.

Theorem

1. $[\![\cdot]\!]\colon (\mathcal{T}_D, \delta) \to (X, \mathfrak{U})$ *is uniformly continuous.*
2. *The finite open covering uniformity* $\mathfrak{U}$ *on* X *is the quotient uniformity relative to* $[\![\cdot]\!]$.
3. *The collection of relations*

$$U_m = \bigcup \{\, T^{(m)}[X^{\mathrm{ar}(T^{(m)})}] \times T^{(m)}[X^{\mathrm{ar}(T^{(m)})}] \mid T \in \mathcal{T}_D \,\}$$

with $m \geq 0$ *is a fundamental system for the finite open covering uniformity on* X.

As is well known, every countably based uniformity can be generated by a pseudometric.

Let $q = 2^{\max\{\,\mathrm{ar}(d) \mid d \in D\,\}}$ and for $x, y \in X$ define

$$\rho(x,y) = \inf\{\,\sum_{j=0}^{m-1} q^{-i_j} \mid m, i_0, \dots i_{m-1} \geq 0 \text{ and there exists a path } z_0, \dots, z_m \text{ from } x \text{ to } y \text{ such that for } 1 \leq j < m,\ (z_j, z_{j+1}) \in U_{i_j}\,\}.$$

Theorem

1. *ρ is a metric on X.*
2. *Each $d \in D$ is contracting with contracting factor $\mathrm{ar}(d)/q$. Here, each power of X is furnished with the maximum metric.*
3. *(X, ρ) is bounded.*

3. Continuous functions

Goal: Co-inductive characterization of the uniformly continuous maps.

- For $f\colon X^n \to X$, $m \geq 1$, and $1 \leq i \leq m$, define $f_{i,m}\colon X^{n+m} \to X^m$ by

$$f_{i,m}(y_1, \ldots, y_n, x_1, \ldots, x_m) := (x_1, \ldots, x_{i-1}, f(y_1, \ldots, y_n), x_{i+1}, \ldots, x_m).$$

Let

- $\mathrm{pr}_i^{(m)}\colon X^m \to X$ projection on i-th component.
- (X, D) and (Y, E) digit spaces.

Set

$$\mathbb{F}(X, Y) := \{\, f\colon X^m \to Y \mid m \geq 0 \,\}.$$

Define

$$\Phi\colon \mathcal{P}(\mathbb{F}(X,Y)) \to (\mathcal{P}(\mathbb{F}(X,Y)) \to \mathcal{P}(\mathbb{F}(X,Y)))$$

by

$$\begin{aligned}
&\Phi(F)(G) := \\
&\quad \{\, e \circ (f_1,\ldots,f_{\mathrm{ar}(e)}) \mid e \in E \wedge f_1,\ldots,f_{\mathrm{ar}(e)} \in F \,\} \cup \\
&\quad \{\, h \in \mathbb{F}(X,Y) \mid (\exists 1 \le i \le \mathrm{ar}(h))(\forall d \in D) h \circ d_{i,\mathrm{ar}(h)} \in G \,\}.
\end{aligned}$$

- $\Phi(F)(G)$ is monotone in G, for all $F \subset \mathbb{F}(X,Y)$. Thus, the minimal fixed point $\mathcal{J}(F) = \mu\Phi(F)$ of $\lambda G.\ \Phi(F)(G)$ exists.
- $\mathcal{J}$ is monotone. Hence the greatest fixed point $\nu\mathcal{J}$ of $\lambda F.\ \mathcal{J}(F)$ exists.

Note $\mathcal{J}(F)$ is the smallest subset of $\mathbb{F}(X, Y)$ such that

- W If $e \in E$ and $f_1, \ldots, f_{\mathrm{ar}(e)} \in F$ then $e \circ (f_1, \ldots, f_{\mathrm{ar}(e)}) \in \mathcal{J}(F)$.
- R If $h \in \mathbb{F}(X, Y)$ and $1 \leq i \leq \mathrm{ar}(h)$ with $h \circ d_{i,\mathrm{ar}(h)} \in \mathcal{J}(F)$, for all $d \in D$, then $h \in \mathcal{J}(F)$.

Theorem

Let (X, D) and (Y, E) be invertible and well-covering digit spaces. Then

$$\nu\mathcal{J} = \{\, f \in \mathbb{F}(X, Y) \mid f \text{ uniformly continuous} \,\}.$$

Definition

A digit space (X, D) is

1. invertible if each $d \in D$ has a continuous right inverse $d' \colon \operatorname{range}(d) \to X^{\operatorname{ar}(d)}$, i.e., $d \circ d' = \operatorname{id}_{\operatorname{range}(d)}$.
2. well-covering if $X = \bigcup \{ \operatorname{int}(d[X^{\operatorname{ar}(d)}]) \mid d \in D \}$.

4. Separability

Let Q be a dense subset of X. In most applications dense elements are finite objects (rationals e.g. in the case of the reals).

Density means that in every neighbourhood of x there is some $u \in Q$. We want to prove that

$$x \in \mathcal{C}_X \iff (\forall n \in \mathbb{N})(\exists u \in Q)\mu(x, u) < 2^{-n}.$$

From a proof of this result we can extract programs converting between realizers of

$$\text{“}x \in \mathrm{C}_X\text{”} \quad \text{and} \quad \text{“}(\forall n \in \mathbb{N})(\exists u \in Q)\mu(x, u) < 2^{-n}\text{”}$$

What are these realizers?

Lemma

- *T is an realizer of $x \in \mathrm{C}_X$ iff $T \in \mathcal{T}_D$ and $[\![T]\!] = x$.*
- *f realizes $(\forall n \in \mathbb{N})(\exists u \in Q)\mu(x, u) < 2^{-n}$ iff $f : \mathbb{N} \to Q$ such that $(\forall n \in \mathbb{N})\mu(x, f(n)) < 2^{-n}$.*

Lemma

Let (X, D) be well-covering. Then there exists $\varepsilon \in \mathbb{Q}_+$ such that for every $x \in X$ there exists $d \in D$ with $\mathrm{B}_\mu(x, \varepsilon) \subseteq d[X^{\mathrm{ar}(d)}]$.

Here

$$\mathrm{B}_\mu(x, \varepsilon) := \{\, y \in X \mid \mu(x, y) < \varepsilon \,\}.$$

Definition

(X, D, Q) is decidable if for every $u \in Q$, $\varepsilon \in \mathbb{Q}_+$, and $d \in D$ it can be decided whether $\mathrm{B}_\mu(u, \varepsilon) \subseteq d[X^{\mathrm{ar}(d)}]$.

Definition

(X, D, Q) has approximable choice if for every $d \in D$ there is an effective procedure $\lambda(\theta, u).\vec{v}_u^\theta : \mathbb{Q} \times d[X^{\mathrm{ar}(d)}] \cap Q \to Q^{\mathrm{ar}(d)}$ such that for all $\theta \in \mathbb{Q}$:

1. For all $u \in d[X^{\mathrm{ar}(d)}] \cap Q$ and all $\hat{\theta} \in \mathbb{Q}$, $\mu_{\mathrm{m}}(\vec{v}_u^\theta, \vec{v}_u^{\hat{\theta}}) < \max\{\theta, \hat{\theta}\}$.
2. One can compute $\theta' \in \mathbb{Q}$ such that for all $u, u' \in d[X^{\mathrm{ar}(d)}] \cap Q$, if $\mu(u, u') < \theta'$ then $\mu_{\mathrm{m}}(\vec{v}_u^\theta, \vec{v}_{u'}^\theta) < \theta$.
3. For all $u \in d[X^{\mathrm{ar}(d)}] \cap Q$ there is some $\vec{z} \in d^{-1}[u]$ with $\mu_{\mathrm{m}}(\vec{z}, \vec{v}_u^\theta) < \theta$.

Theorem

Let (X, D, Q) be a well-covering and decidable digit space with approximable choice. Then

$$x \in \mathrm{C}_X \iff (\forall n \in \mathbb{N})(\exists u \in Q)\mu(x, u) < 2^{-n}.$$

"$\Rightarrow$" follows by induction on n and "$\Leftarrow$" by coinduction.

Special cases:

- Compact separable Hausdorff space X.
- The space $(\mathrm{K}(X), \mu_{\mathrm{H}})$ of all non-empty compact subspaces of X endowed with the Hausdorff metric μ_{H}.

Note

- $(\mathrm{K}(X), \mu_{\mathrm{H}})$ is a bounded complete metric space, just as X is.
- The nonempty *finite* sets of dense points in X form a dense subset $\mathcal{Q}$.

Set

$$D_{\mathrm{K}(X)} := \{\, [d_1, \dots, d_n] \mid d_1, \dots, d_n \in D \text{ pairwise distinct} \,\}$$

where $$[d_1, \dots, d_n](\vec{A}_1, \dots, \vec{A}_n) = \bigcup_{i=1}^{n} d[\vec{A}_i].$$

In this case

$$A \in \mathcal{C}_{\mathrm{K}(X)} \Rightarrow (\exists d_1, \dots, d_n \in D \text{ pairwise distinct})$$
$$(\exists \vec{A}_1 \in \mathcal{C}_{\mathrm{K}(X)}^{\mathrm{ar}(d_1)}, \dots, \vec{A}_n \in \mathcal{C}_{\mathrm{K}(X)}^{\mathrm{ar}(d_n)}) A = [d_1, \dots, d_n](\vec{A}_1, \dots, \vec{A}_n).$$

Theorem

Let $(\mathrm{K}(X), D_{\mathrm{K}(X)}, \mathcal{Q})$ *be well-covering and decidable with approximable choice. Then*

$$A \in \mathcal{C}_{\mathrm{K}(X)} \iff (\forall n \in \mathbb{N})(\exists U \in \mathcal{Q})\mu_{\mathrm{H}}(A, U) < 2^{-n}.$$

The assumptions in this theorem are not of the kind we are interested in: we want assumptions on space (X, D, Q), but not on $(\mathrm{K}(X), D_{\mathrm{K}(X)}, \mathcal{Q})$.

Lemma

Let (X, D, Q) *be well-covering, then also* $(\mathrm{K}(X), D_{\mathrm{K}(X)}, \mathcal{Q})$ *is well-covering. If, in addition,* (X, D, Q) *is decidable, the same holds for* $(\mathrm{K}(X), D_{\mathrm{K}(X)}, \mathcal{Q})$.

Lemma

Let (X, D, Q) *have approximable choice, then also* $(\mathrm{K}(X), D_{\mathrm{K}(X)}, \mathcal{Q})$ *has approximable choice.*

5. Applications:

- **Signed-digit representation**
  - $X = \mathbb{I} = [-1, 1]$
  - $D_{\mathrm{SD}} = \{ d_a \mid a \in \{-1, 0, +1\} \}$ with

$$d_a(x) = \frac{x + a}{2}.$$

  - (X, D) is well-covering.

- **Pre-Gray code**

$$X = \mathbb{I}$$
$$D_{\mathrm{pG}} = \{\, \mathrm{LR}_a \mid a \in \{-1, +1\} \,\} \cup \{D, U\} \cup \{\, \mathrm{Fin}_a \mid a \in \{-1, +1\} \,\}$$

with

$$\mathrm{LR}_a(x) = -a\frac{x-1}{2}, \quad \mathrm{Fin}_a(x) = a\frac{x+1}{2}, \quad D(x) = U(x) = \frac{x}{2}.$$

(X, D_{pG}) is well-covering.

The admissible streams over D_{pG} are determined by the following typing:

$$\begin{aligned} \mathrm{LR}_a &\colon \mathbf{G} \to \mathbf{G}, & \qquad U &\colon \mathbf{H} \to \mathbf{G} \\ \mathrm{Fin}_a &\colon \mathbf{G} \to \mathbf{H}, & \qquad D &\colon \mathbf{H} \to \mathbf{H}. \end{aligned}$$

This leads to the following set of admissible streams:

$$\begin{aligned} \mathrm{GH} = & [\{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^* U D^* \{\mathrm{Fin}_{\bar{1}}, \mathrm{Fin}_1\}]^* \{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^\omega \\ & \cup [\{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^* U D^* \{\mathrm{Fin}_{\bar{1}}, \mathrm{Fin}_1\}]^* \{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^* U D^\omega \\ & \cup [\{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^* U D^* \{\mathrm{Fin}_{\bar{1}}, \mathrm{Fin}_1\}]^\omega, \end{aligned}$$

where $\bar{1} = -1$.

Lemma

GH *is closed in the metric topology on* D^{ω}_{pG}.

Proposition

1. GH *is a compact Hausdorff space with respect to the restriction of the canonical metric on* D_{pG}.
2. $(\mathbb{I}, \{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1, U\})$ *is well-covering.*
3. *The restriction of* $[\![\cdot]\!]$ *to* GH *is surjective.*

- **Gray code**
  - $X = \mathbb{I}$
  - $D_G = \{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1, d_0\}$
  - The set of admissible streams T is not closed in the metric topology on $\{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1, d_0\}^\omega$

where

$$\begin{aligned} T =& [\{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^\omega \cup \{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^* d_0 \mathrm{LR}_{\bar{1}}^\omega] \\ & \quad \setminus \{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\}^* \{\mathrm{LR}_{\bar{1}}, \mathrm{LR}_1\} \mathrm{LR}_1 \mathrm{LR}_{\bar{1}}^\omega . \end{aligned}$$