MAP 2008
Abdus Salam ICTP

A coinductive approach to digital computation

Ulrich Berger
Swansea

Outline

- Introduction
- Induction and coinduction
- Digit spaces
- Metric digit spaces
- Applications: iterated maps, π, integration
- Program extraction
- Analytic functions
- Conclusion

The aims of this talk

- to outline a constructive theory of digital computation;
- to show that program extraction from proofs is a practical method to obtain certified programs for digital computation.

Example: computing with signed digits

$\mathbb{I} := [-1, 1] \subseteq \mathbb{R}$
$\mathrm{SD} := \{-1, 0, 1\}$
$x \in \mathbb{I}$
$a = (a_n)_{n \in \mathbb{N}} \in \mathrm{SD}^\omega$

$$x \sim a \quad :\Leftrightarrow \quad x = \sum_{n=0}^{\infty} a_n \cdot 2^{-(n+1)}$$

A function $f : \mathbb{I} \to \mathbb{I}$ is *represented* by a function $\hat{f} : \mathrm{SD}^\omega \to \mathrm{SD}^\omega$ if

$$\forall x, a \, (\, x \sim a \Rightarrow f(x) \sim \hat{f}(a)\,)$$

Power series as infinite composition

$$\sum_{n=0}^{\infty} a_n \cdot 2^{-(n+1)} = \frac{1}{2}(a_0 + \frac{1}{2}(a_1 + \dots))$$

$\mathrm{av}_d : \mathbb{I} \to \mathbb{I}, \quad \mathrm{av}_d(x) := \frac{1}{2}(d + x) \quad (d \in \mathrm{SD}).$

$$\sum_{n=0}^{\infty} a_n \cdot 2^{-(n+1)} = \mathrm{av}_{a_0}(\mathrm{av}_{a_1}(\dots)) = \mathrm{av}_{a_0} \circ \mathrm{av}_{a_1} \circ \dots$$

Therefore, $x \sim a \;\Leftrightarrow\; x = \mathrm{av}_{a_0} \circ \mathrm{av}_{a_1} \circ \dots$.

$\mathrm{AV} := \{\mathrm{av}_{-1}, \mathrm{av}_0, \mathrm{av}_1\} \subseteq \mathbb{I} \to \mathbb{I}$.

$(\mathbb{I}, \mathrm{AV})$ is an example of a *digit space*.

Digit spaces

We study digit spaces (X, D), where X is a set and $D \subseteq X \to X$, and characterise the functions $f : X \to Y$ that have a continuous digital representation $\hat{f} : D^\omega \to E^\omega$, without reference to infinite objects (like streams of digits).

The characterisation uses inductive/coinductive definitions and yields implementations of $\hat{f}$ by finitely branching non-wellfounded trees.

We also consider *metric digit spaces* (X, σ, P, D), where σ is a metric on X and $P \subseteq X$ is dense, and study the relation between digital representability and uniform continuity.

Induction

$\Phi\colon \mathcal{P}(U) \to \mathcal{P}(U)$ is monotone if $X \subseteq Y$ implies $\Phi(X) \subseteq \Phi(Y)$.

A set $X \subseteq U$ is Φ-*closed* if $\Phi(X) \subseteq X$.

$\mu\Phi$, the set *inductively* defined by Φ, is the least Φ-closed set.

Closure	$\Phi(\mu\Phi) \subseteq \mu\Phi$
Induction	if $\Phi(X) \subseteq X$, then $\mu\Phi \subseteq X$

Example

$$\Phi : \mathcal{P}(\mathbb{R}) \to \mathcal{P}(\mathbb{R}),$$
$$\Phi(X) := \{0\} \cup \{x + 1 \mid x \in X\}$$

$$\mu\Phi = \mathbb{N} = \{0, 1, 2, \ldots\}.$$

Induction:

If $X(0)$ and $\forall x\,(X(x) \to X(x+1))$,

then $\forall x \in \mathbb{N}\, X(x)$.

Coinduction

A set $X \subseteq U$ is Φ-*coclosed* if $X \subseteq \Phi(X)$.

$\nu\Phi$, the set *coinductively* defined by Φ, is the largest Φ-coclosed set.

Coclosure	$\nu\Phi \subseteq \Phi(\nu\Phi)$
Coinduction	if $X \subseteq \Phi(X)$, then $X \subseteq \nu\Phi$

Example

$$\Phi : \mathcal{P}(\mathbb{R}) \to \mathcal{P}(\mathbb{R})$$

$$\Phi(X) := \{x \in \mathbb{I} \mid \exists d \in \mathrm{SD}\, \exists x' \in X\;\; x = \mathrm{av}_d(x')\}$$

Lemma: $\nu\Phi = \mathbb{I}$.

Proof: $\nu\Phi \subseteq \Phi(\nu\Phi) \subseteq \mathbb{I}$.

$\mathbb{I} \subseteq \Phi(\nu\Phi)$ is shown by coinduction.

Need to show $\mathbb{I} \subseteq \Phi(\mathbb{I})$: Let $x \in \mathbb{I}$.

If $x \geq 0$, take $d := 1$, otherwise $d := -1$. $x' := 2 \cdot x - 1$

Digit spaces

A *digit space* is a pair (X, D) consisting of a set X and $D \subseteq X \to X$.

The elements of D are called *digits*.

Digital maps

Let (X, D) and (Y, E) be digit spaces.
We define the set $\mathrm{C}_{D,E} \subseteq X \to Y$ of *digital maps* as follows.

Let F, G range over subsets of $X \to Y$
and let $\nu F. \dots$ stand for $\nu\lambda F \dots$ e.t.c.

$\mathrm{C}_{D,E} :=$

$$\nu F.\mu G.\{e \circ f \mid e \in E, f \in F\} \cup \{h : X \to Y \mid \forall d \in D\ h \circ d \in G\}$$

Identity and composition

Identity Lemma

Let (X, D) be a digit spaces.

(a) $\mathrm{id}_X \in \mathrm{C}_{D,D}$.

(b) $D \subseteq \mathrm{C}_{D,D}$.

Composition Lemma

Let (X_i, D_i) (i=1,2,3) be digit spaces.

If $f \in \mathrm{C}_{D_1,D_2}$ and $g \in \mathrm{C}_{D_2,D_3}$, then $g \circ f \in \mathrm{C}_{D_1,D_3}$.

The category of digit spaces

By the Identity Lemma and the Composition Lemma, digit spaces and digital maps form a category.

Product Lemma

The category $\mathcal{D}$ has finite products.

Digital global elements

The set of global elements of a digit space (X, D) is

$$\mathrm{C}_D := \mathrm{C}_{\mathbf{1},(X,D)}$$

where $\mathbf{1}$ denotes the terminal object $(\mathbf{1}, \{\mathrm{id}_{\mathbf{1}}\})$ in $\mathcal{D}$. We identify C_D with a subset of X.

Global Element Lemma

$$\mathrm{C}_D = \nu A.\{d(x) \mid d \in D, x \in A\}$$

Roughly, $\mathrm{C}_D = \{d_0 \circ d_1 \circ \ldots \mid (d_n)_{n\in\mathbb{N}} \in D^\omega\}$.

Application

Application Lemma

If $f \in \mathrm{C}_{D,E}$ and $x \in \mathrm{C}_D$, then $f(x) \in \mathrm{C}_E$.

Proof: Composition Lemma.

Metric spaces

A *metric space* $X = (X, \sigma, P)$ consists of a set X, a metric σ on X and a dense set $P \subseteq X$.

For a rational number $\epsilon > 0$ and $p \in P$ we define

$$\mathrm{B}_\epsilon(p) := \{x \in X \mid \sigma(p, x) \leq \epsilon\}$$

X is *bounded* if $X \subseteq \mathrm{B}_M(p)$ for some $M > 0$ and $p \in P$.

Uniform continuity

Let $X = (X, P, \sigma)$ and $Y = (Y, Q, \tau)$ be metric spaces.

A relation $f \subseteq X \times Y$ is *uniformly continuous* (*u.c.*) if

$$\forall \epsilon > 0 \, \exists \delta > 0 \, \mathrm{F}_{\delta,\epsilon}(f)$$

where

$$\mathrm{F}_{\delta,\epsilon}(f) := \forall p \in P \, \exists q \in Q \, f[\mathrm{B}_\delta(p)] \subseteq \mathrm{B}_\epsilon(q).$$

Properties of uniform continuity

Lemma

A relation $f \subseteq X \times Y$ is u.c. iff it is a partial function which is uniformly continuous on its domain,
$\mathrm{dom}(f) := \{x \in X \mid \exists y \in Y\,(x,y) \in f\}$, in the usual sense, i.e.

$$\forall \epsilon > 0\,\exists \delta > 0\,\forall x, x \in \mathrm{dom}(F)\,(\sigma(x,x') \leq \delta \Rightarrow \tau(f(x), f(x')) \leq \epsilon)$$

Composition Lemma

If $g \subseteq Y \times Z$ and $f \subseteq X \times Y$ are uniformly continuous, so is $g \circ f \subseteq X \times Z$.

Lipschitz conditions and contractivity

A relation $f \subseteq X \times Y$ is called λ-*Lipschitz* if $\forall \delta > 0\,(f \in \mathrm{F}_{\delta,\lambda\cdot\delta})$.

Lemma

A relation $f \subseteq X \times Y$ is λ-Lipschitz iff it is a partial function and $\tau(f(x), f(x')) \leq \lambda \cdot \sigma(x, x')$ for all $x, x' \in \mathrm{dom}(f)$.

Lipschitz Lemma

If a relation is λ-Lipschitz for some λ, then it is uniformly continuous.

If a relation is called λ-*contracting* if it is λ-Lipschitz with $\lambda < 1$.

Metric digit spaces

A *metric digit space* $X = (X, \sigma, P, D)$ is a metric space (X, σ, P) together with a set of digits $D \subseteq X \to X$.

Metric digit spaces

A metric digit space $X = (X, \sigma, P, D)$ is called

contracting if there is $\lambda < 1$ such that all $d \in D$ are λ-contracting.

invertible if d^{-1} is u.c. for all $d \in D$.

covering if there is an $\epsilon > 0$ such that for all $p \in P$ there exists $d \in D$ with $\mathrm{B}_\epsilon(p) \subseteq d[X]$.

finitely covering if there is a finite subset of D which is uniformly covering.

Example: $(\mathbb{I}, \mathrm{AV})$ has all these properties.

Characterisation of u.c.

Characterisation Lemma

Let $X = (X, \sigma, P, D)$ and $Y = (Y, \tau, Q, E)$ be metric digit spaces. Set $\mathrm{U} := \{f : X \to Y \mid f \text{ u.c.}\}$ and $\mathrm{C} := \mathrm{C}_{D,E}$.

(a) If X is bounded and contracting, and Y is invertible and covering, then $\mathrm{U} \subseteq \mathrm{C}$.

(b) Assume D is finite. If X is invertible and finitely covering, and Y is bounded and contracting, then $\mathrm{C} \subseteq \mathrm{U}$.

Corollary (change of digits)

Let (X, σ, P) be a bounded metric space. Let $D, E \subseteq X \to X$. If D is contracting, and E is invertible and covering, then $\mathrm{C}_D \subseteq \mathrm{C}_E$.

Iterated maps

The family of logistic maps (transformed from $[0,1]$ to $\mathbb{I} = [-1,1]$):

$$f_a : \mathbb{I} \to \mathbb{I}, \quad f(x) = a * (1 - x^2) - 1 \qquad (0 \leq a \leq 2).$$

f_a is $2a$-contracting, hence uniformly continuous (Contraction Lemma), hence in $\mathrm{C} := \mathrm{C}_{\mathrm{AV},\mathrm{AV}} \subseteq \mathbb{I} \to \mathbb{I}$ (Characterisation Lemma (a)).

It follows that the iterated logistic maps $f_a^n : \mathbb{I} \to \mathbb{I}$ are in C (Composition Lemma).

The program extracted from the proof of $f_a^n \in \mathrm{C}$ will be discussed later.

π

For the metric digit space $(\mathbb{I}, \mathrm{AV})$ we have $\pi/4 \in \mathrm{C}_D$.

Proof We use the formula

$$\frac{\pi}{4} = \frac{1}{2} + \frac{1}{3}\left(\frac{1}{2} + \frac{2}{5}\left(\frac{1}{2} + \frac{3}{7}\left(\frac{1}{2} + \frac{4}{9}\left(\frac{1}{2} + \ldots\right)\right)\right)\right)$$

i.e. $\pi/4 = f_0(f_1(\ldots))$ where

$$f_n(x) := \frac{1}{2} + \frac{n\,x}{2n+1}.$$

Hence we have $\pi/4 \in \mathrm{C}_F$ where $F := \{f_n \mid n \in \mathbb{N}\}$. Since F is contracting and AV is invertible and covering, it follows, by change of digits, $\pi/4 \in \mathrm{C}_D$.

Integration

For a continuous function $f : \mathbb{I} \to \mathbb{R}$ we set
$\int f := \int_{-1}^{1} f = \int_{-1}^{1} f(t)\,\mathrm{d}t \in \mathbb{R}$.

Lemma

(a) $\int(\mathrm{av}_i \circ f) = \mathrm{av}_{2\cdot i}(\int f)$

(b) $\int f = \frac{1}{2}(\int(f \circ \mathrm{av}_{-1}) + \int(f \circ \mathrm{av}_1))$.

Integration Lemma

Let (X, σ, P, D) be a covering and invertible metric digit system and $f \in \mathrm{C}_{D\otimes\mathrm{AV},\mathrm{AV}}$. Then the function mapping $(a, b, x) \in \mathbb{I}^2 \times X$ to $\int_a^b f(x, t)\,\mathrm{d}t$ is well-defined and uniformly continuous.

The type of a formula

To every formula A we assign the type $\tau(A)$ of its *realisers*, i.e. the type a program extracted from a proof of A will have:

- $\tau(A)$ is the unit type if A contains neither $\vee$ nor predicate variables (A may contain predicate constants like "$=$", "$\leq$" and "$\in \mathbb{R}$").
- The propositional connectives $\wedge$, $\vee$, $\Rightarrow$ are translated into the type constructors $\times$, $+$, $\rightarrow$.
- Quantifiers and terms are ignored.
- Predicate variables are translated into type variables.
- Inductive and coinductive definitions are translated into initial algebras and terminal coalgebras, respectively.

Example: τ("f is uniformly continuous")

Recall that $f : \mathbb{I} \to \mathbb{I}$ is uniformly continuous if

$$\forall 0 < \epsilon \in \mathbb{Q}\ \exists 0 < \delta \in \mathbb{Q}\ \mathrm{F}_{\delta,\epsilon}(f)$$

where

$$\mathrm{F}_{\delta,\epsilon}(f) := \forall p \in \mathbb{Q} \cap \mathbb{I}\ \ \exists q \in \mathbb{Q} \cap \mathbb{I}\ \ f[\mathrm{B}_\delta(p)] \subseteq \mathrm{B}_\epsilon(q).$$

We have $\tau(p \in \mathbb{Q}) = \mathbb{Q}$.

Therefore

$$\begin{aligned} \tau(f \text{ u.c}) &= \mathbb{Q} \to \mathbb{Q} \times \tau(\mathrm{F}_{\delta,\epsilon}(f)) \\ &= \mathbb{Q} \to \mathbb{Q} \times (\mathbb{Q} \to \mathbb{Q}) \end{aligned}$$

Example: $\tau(\mathrm{C_{AV}})$

Recall the definition of $\mathrm{C_{AV}} \subseteq \mathbb{I}$:

$$\begin{aligned}\mathrm{C_{AV}} &= \nu A\,.\,\{d(x) \in \mathbb{I} \mid d \in \mathrm{AV}, x \in A\} \\ &= \nu A\,.\,\{y \in \mathbb{R} \mid -1 \leq y \leq 1 \wedge \\ &\qquad\qquad \exists d, x\,(d \in \mathrm{AV} \wedge x \in A \wedge y = \mathrm{av}_a(x))\}\end{aligned}$$

where

$\mathrm{AV} = \{\mathrm{av}_a \mid a \in \mathrm{SD}\} = \{d : \mathbb{R} \to \mathbb{R} \mid \exists a \in \mathrm{SD}\; d = \mathrm{av}_a\}$

$\mathrm{SD} = \{-1, 0, 1\} = \{a \mid a = -1 \vee a = 0 \vee a = 1\}$:

Therefore

$$\begin{aligned}\tau(\mathrm{C_{AV}}) &= \nu\alpha\,.\,\mathrm{SD} \times \alpha \\ &= \mathrm{SD}^\omega\end{aligned}$$

Example: $\tau(\mathrm{C}_{\mathrm{AV},\mathrm{AV}})$

Recall the definition of $\mathrm{C}_{\mathrm{AV},\mathrm{AV}} \subseteq \mathbb{I} \to \mathbb{I}$:

$$
\begin{aligned}
\mathrm{C}_{\mathrm{AV},\mathrm{AV}} &= \nu F\,.\,\mu G\,. \\
&\quad \{e \circ f : \mathbb{I} \to \mathbb{I} \mid e \in \mathrm{AV}, f \in F\} \cup \\
&\quad \{h : \mathbb{I} \to \mathbb{I} \mid \forall d \in \mathrm{AV}\ h \circ \mathrm{av}_d \in G\} \\
&= \nu F\,.\,\mu G\,. \\
&\quad \{h : \mathbb{R} \to \mathbb{R} \mid h[\mathbb{I}] \subseteq \mathbb{I} \wedge \\
&\qquad (\exists e, f\,(e \in \mathrm{AV} \wedge f \in F \wedge h = e \circ f) \vee \\
&\qquad (h \circ d_{-1} \in G \wedge h \circ d_0 \in G \wedge h \circ d_1 \in G))\}
\end{aligned}
$$

Therefore

$$\tau(\mathrm{C}_{\mathrm{AV},\mathrm{AV}}) = \nu\alpha\,.\,\mu\beta\,.\,\mathrm{SD} \times \alpha + \beta^3$$

See also [Ghani,Hancock,Pattinson 2008]

Understanding $\tau(\mathrm{C}_{\mathrm{AV},\mathrm{AV}}) = \nu\alpha\,.\,\mu\beta\,.\,\mathrm{SD}\times\alpha+\beta^3$

Define T as the largest solution of the domain equation

$$T = \mathrm{SD} \times T + T^3$$

i.e. the elements of T are non-wellfounded trees with two kinds of nodes:

- **Writing nodes:** $W(d, t)$ where $d \in \mathrm{SD}$ and $t \in T$.
- **Reading nodes:** $R(t_{-1}, t_0, t_1)$ where $t_i \in T$.

Classically, $\tau(\mathrm{C}_{\mathrm{AV},\mathrm{AV}})$ is the set of those trees in T that have on every infinite path infinitely many writing nodes.

Constructively, $\tau(\mathrm{C}_{\mathrm{AV},\mathrm{AV}})$ is the set of those trees in T that have for every $n \in \mathbb{N}$ only finitely many finite paths with less than n writing nodes.

Realising inductive definitions

Assume the set operator Φ corresponds to the type operator φ.

Then, the inductively defined set $\mu\Phi$ together with the axioms

Closure	$\Phi(\mu\Phi) \subseteq \mu\Phi$
Induction	if $\Phi(X) \subseteq X$, then $\mu\Phi \subseteq X$

are realised by the initial algebra $(\mu\varphi, \mathrm{In}_\varphi)$
and the family It_φ of universal arrows, i.e.

$$\begin{aligned} \mathrm{In}_\varphi &: \varphi(\mu\varphi) \to \mu\varphi \\ \mathrm{It}_\varphi[s] &: \mu\varphi \to \alpha \quad (s : \varphi(\alpha) \to \alpha) \end{aligned}$$

with the defining recursion equation expressing that $\mathrm{It}_\varphi[s]$ is an algebra morphism

$$\mathrm{It}_\varphi[s] \circ \mathrm{In}_\varphi = s \circ \mathbf{map}_\varphi(\mathrm{It}_\varphi[s])$$

Realising coinductive definitions

For coinductive definitions the situation is dual.

The coinductively defined set $\nu\Phi$ and its axioms

Coclosure $\nu\Phi \subseteq \Phi(\nu\Phi)$

Coinduction if $X \subseteq \Phi(X)$, then $X \subseteq \nu\Phi$

are realised by the terminal coalgebra $(\nu\varphi, \mathrm{Out}_\varphi)$
and the family $\mathrm{Coit}_\varphi[s]$ of universal arrows

$$\begin{array}{rcl} \mathrm{Out}_\varphi & : & \nu\varphi \to \varphi(\nu\varphi) \\ \mathrm{Coit}_\varphi[s] & : & \alpha \to \nu\varphi \quad (s : \alpha \to \varphi(\alpha)) \end{array}$$

with the equation expressing that $\mathrm{Coit}_\varphi[s]$ is a coalgebra morphism

$$\mathrm{Out}_\varphi \circ \mathrm{Coit}_\varphi[s] = \mathbf{map}_\varphi(\mathrm{Coit}_\varphi[s]) \circ s$$

Computing the iterated logistic maps

$$f_a : \mathbb{I} \to \mathbb{I}, \quad f_a(x) = a * (1 - x^2) - 1 \qquad (0 \leq a \leq 2).$$

Testing program:

If $f : \mathbb{I} \to \mathbb{I}$ with slope not exceeding s, then

$$\mathrm{testit}\, s\, f = f^n(p)$$

where p and n are given interactively.

The results are computed using the extracted program and compared with floating point and exact rational arithmetic.

The main point of this example is to demonstrate the **memoizing** effect of the tree representation of u.c. functions. See also [Hinze, Proc. WGP 2000] and [Altenkirch, TLCA 2001, LNCS 2044].

Computing $\pi/4 = 0.785398163397448$

$$\mathrm{pi4M}\ m$$

computes *m* signed digits of $\pi/4$ and displays it as a Float.

Integrating the logistic map

$f_a : \mathbb{I} \longrightarrow \mathbb{I}, \quad f_a(x) = a * (1 - x^2) - 1 \qquad (0 \leq a \leq 2).$

$\int f_a = \int_{-1}^{1} (a * (1 - x^2) - 1)\, \mathrm{d}x = \frac{4}{3}a - 2$

For example, $\int f_2 = \frac{2}{3}$, $\int f_{1.5} = 0$, $\int f_1 = -\frac{2}{3}$, $\int f_0 = -2$.

$$\mathrm{defint}\, (\mathrm{lmaC}\, a)\, \epsilon$$

computes the integral of f_a with error $\leq \epsilon$ as an exact rational.

Digits of higher type

Higher Type Digit Lemma

Let $q > 0$ and $a_n \in \mathbb{R}$ ($n \in \mathbb{N}$) such that $|a_{n+1}| \leq q \cdot |a_n|$ for all $n \in \mathbb{N}$. Let $u, v \geq 0$ such that $|a_0|, u \leq q \cdot v^2$ and $q \cdot (u + v) < 1$. Set $X := \mathrm{B}_u(0)$ and $Y := \mathrm{B}_v(0)$. Then $f : X \to Y$,

$$f(x) := \sum_{n=0}^{\infty} a_n \cdot x^n$$

is well-defined, and $f \in \mathrm{C}_P$ where

$P := \{p_n : (X \to Y) \to X \to Y \mid n \in \mathbb{N}\}$,

$p(f)(x) := a_n / q^n + q \cdot x \cdot f(x)$.

The Curry Lemma

In order to obtain a digital implementation of an analytic function f we need to show $f \in \mathrm{C}_{D,E}$ for suitable D, E.

But we only got $f \in P$ where P is defined as in the Higher Digit Lemma.

Curry Lemma

Let (X, D) and (Y, E) be digit spaces, and assume that $A \subseteq (X \to Y) \to (X \to Y)$ is such that $\mathrm{uncurry}(A) \subseteq \mathrm{C}_{A \otimes D,E}$. Then $\mathrm{C}_A \subseteq \mathrm{C}_{D,E}$.

Hence it suffices to find a set $A \subseteq (X \to Y) \to (X \to Y)$ such that $P \subseteq A$ and $\mathrm{uncurry}(A) \subseteq \mathrm{C}_{A \otimes D,E}$.

The Contraction Lemma

Contraction Lemma
Let $D \subseteq X \to X$ uniformly contracting, $E \subseteq Y \to Y$ uniformly covering and s.t. all $e \in E$ are injective with a uniform Lipschitz constant for the inverses.

For $p : X \times Y \to Y$ and $q : X \to X$ define

$$\varphi_{p,q} : (X \to Y) \times X \to Y, \quad \varphi_{p,q}(f, x) := p(x, f(q(x)))$$

Let $\lambda < 1$ and $\gamma \geq 0$. Define

$$A := \{\varphi_{p,q} : p \ \lambda\text{-contracting}, \ q \ \gamma\text{-Lipschitz} \} \subseteq (X \to Y) \times X \to Y$$

Then $A \subseteq \mathrm{C}_{\mathrm{curry}(A) \otimes D, E}$.

Further work

We would like to apply the general theory to compute approximations to the compact subsets of a compact metric space, viewed as elements of the compact metric space of non-empty compact sets with the Hausdorff metric.

Unfortunately, on that space no finite system of contracting and uniformly covering digits exists.

This non-existence holds for a large class of metric spaces.

We are working on a further generalisation of digital computation that covers such situations.

Joint work with Dieter Spreen.

Conclusion

- Case studies show that "proofs as programs" works.
- New (correct!) programs extracted that would have been difficult to "guess".
- Using a fine tuning of realisability (see Helmut Schwichtenberg's talk) it is possible to do abstract mathematics as usual, and still get computational content.
- To do: implementation (in Minlog).
- Related work by Edalat, Potts, Heckmann, Ciaffaglione, Gianantonio, Niqui, Escardo, Scriven, Hutchinson, Altenkirch, Hinze, Ghani, Hancock, Pattinson.
- A lot of interesting work on program extraction and program verification in constructive analysis has been done in the Coq community (Bertot, O'Connor,. . . , see Bas Spitter's talk).