Logic for exact real arithmetic

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

Technische Universität Wien,
AB Theoretische Informatik und Logik, 9. November 2016

Kolmogorov 1932: "Zur Deutung der intuitionistischen Logik"

- View a formula A as a computational problem, of type $\tau(A)$, the type of a potential solution or "realizer" of A.
- Example: $\forall_n \exists_{m>n} \mathrm{Prime}(m)$ has type $\mathbf{N} \to \mathbf{N}$.

Express this view via axioms

$$\mathrm{Inv}_A \colon A \leftrightarrow \exists_z (z \mathbf{\ r\ } A) \qquad \text{"invariance under relizability"}.$$

Consequences are choice and independence of premise (Troelstra):

$$\forall_x \exists_y A(y) \to \exists_f \forall_x A(f(x)) \qquad \text{for } A \text{ n.c.}$$
$$(A \to \exists_x B) \to \exists_x (A \to B) \qquad \text{for } A, B \text{ n.c.}$$

All these are realized by identities.

Algorithms in constructive proofs

Theorem. Every totally bounded set $A \subseteq \mathbb{R}$ has an infimum y.

Proof.
Given $\varepsilon = \frac{1}{2^p}$, let $a_0 < a_1 < \cdots < a_{n-1}$ be an ε-net:
$\forall_{x \in A} \exists_{i<n} (|x - a_i| < \varepsilon)$. Let $b_p = \min\{ a_i \mid i<n \}$. $y := \lim_p b_p$. □

Corollary. $\inf_{x \in [a,b]} f(x)$ exists, for $f : [a, b] \to \mathbb{R}$ continuous.

Proof.
Given ε, pick $a = a_0 < a_1 < \cdots < a_{n-1} = b$ s.t. $a_{i+1} - a_i < \omega(\varepsilon)$.
Then $f(a_0), f(a_1), \ldots, f(a_{n-1})$ is an ε-net for f's range. □

Many $f(a_i)$ need to be computed.

Aim: Get x with $f(x) = \inf_{y \in [a,b]} f(y)$ and a better algorithm, assuming convexity.

Intermediate value theorem

Let $a < b$ be rationals. If $f\colon [a,b] \to \mathbb{R}$ is continuous with $f(a) \leq 0 \leq f(b)$, and with a uniform modulus of increase

$$\frac{1}{2^p} < d - c \to \frac{1}{2^{p+q}} < f(d) - f(c),$$

then we can find $x \in [a,b]$ such that $f(x) = 0$.

Proof (trisection method).

1. Approximate Splitting Principle. Let x, y, z be given with $x < y$. Then $z \leq y$ or $x \leq z$.
2. IVTAux. Assume $a \leq c < d \leq b$, say $\frac{1}{2^p} < d - c$, and $f(c) \leq 0 \leq f(d)$. Construct c_1, d_1 with $d_1 - c_1 = \frac{2}{3}(d - c)$, such that $a \leq c \leq c_1 < d_1 \leq d \leq b$ and $f(c_1) \leq 0 \leq f(d_1)$.
3. IVTcds. Iterate the step $c, d \mapsto c_1, d_1$ in IVTAux.

Let $x = (c_n)_n$ and $y = (d_n)_n$ with the obvious modulus. As f is continuous, $f(x) = 0 = f(y)$ for the real number $x = y$. □

Derivatives

Let $f, g\colon I \to \mathbb{R}$ be continuous. g is called derivative of f with modulus $\delta_f\colon \mathbb{Z}^+ \to \mathbb{N}$ of differentiability if for $x, y \in I$ with $x < y$,

$$y \leq x + \frac{1}{2^{\delta_f(p)}} \to \left|f(y) - f(x) - g(x)(y-x)\right| \leq \frac{1}{2^p}(y-x).$$

A bound on the derivative of f serves as a Lipschitz constant of f:

Lemma (BoundSlope)

Let $f\colon I \to \mathbb{R}$ be continuous with derivative f'. Assume that f' is bounded by M on I. Then for $x, y \in I$ with $x < y$,

$$\left|f(y) - f(x)\right| \leq M(y-x).$$

Infimum of a convex function

Let $f, f' \colon [a, b] \to \mathbb{R}$ ($a < b$) be continuous and f' derivative of f. Assume that f is strictly convex with witness q, in the sense that $f'(a) < 0 < f'(b)$ and

$$\frac{1}{2^p} < d - c \to \frac{1}{2^{p+q}} < f'(d) - f'(c).$$

Then we can find $x \in (a, b)$ such that $f(x) = \inf_{y \in [a,b]} f(y)$.

Proof.

- To obtain x, apply the intermediate value theorem to f'.
- To prove $\forall_{y \in [a,b]}(f(x) \leq f(y))$ (this is "non-computational", i.e., a Harrop formula) one can use the standard arguments in classical analysis (Rolle's theorem, mean value theorem). □

Exact real numbers

can be given in different formats:

- Cauchy sequences (of rationals, with Cauchy modulus).
- Infinite sequences ("streams") of signed digits $\{-1, 0, 1\}$, or
- $\{-1, 1, \bot\}$ with at most one $\bot$ ("undefined"): Gray code.

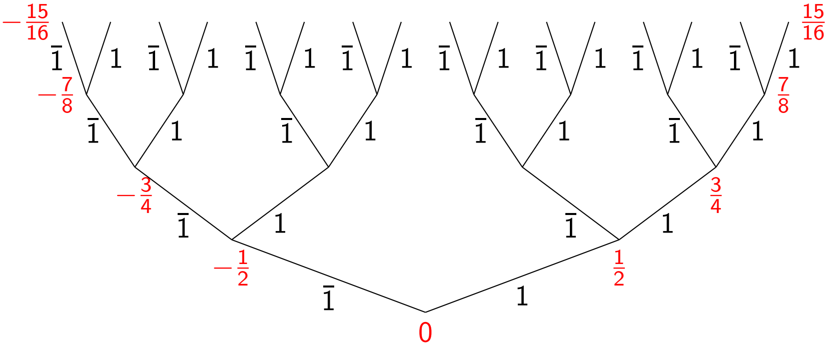
Want formally verified algorithms on reals given as streams.

- Consider formal existence proofs M and apply realizability to extract their computational content.
- Switch between different formate of reals by decoration:
  $\forall_x A \quad \mapsto \quad \forall_x^{\mathrm{nc}}(x \in {}^{\mathrm{co}}I \to A))$ (abbreviated $\forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}I} A$)
- Computational content of $x \in {}^{\mathrm{co}}I$ is a stream representing x.

Representation of real numbers $x \in [-1, 1]$

Dyadic rationals:

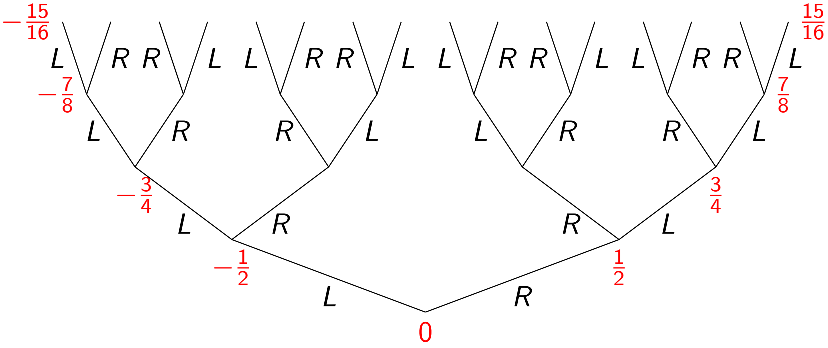
$$\sum_{i<k} \frac{a_i}{2^{i+1}} \qquad \text{with } a_i \in \{-1, 1\}.$$



with $\bar{1} := -1$. Adjacent dyadics can differ in many digits:

$$\frac{7}{16} \sim 1\bar{1}11, \qquad \frac{9}{16} \sim 11\bar{1}\bar{1}.$$

Cure: flip after 1. Binary reflected (or Gray-) code.



$$\frac{7}{16} \sim \mathrm{RRRL}, \qquad \frac{9}{16} \sim \mathrm{RLRL}.$$

Problem with productivity:

$$\bar{1}111 + 1\bar{1}\bar{1}\bar{1}\cdots = ? \qquad \text{(or } \mathrm{LRLL}\ldots + \mathrm{RRRL}\cdots = ?\text{)}$$

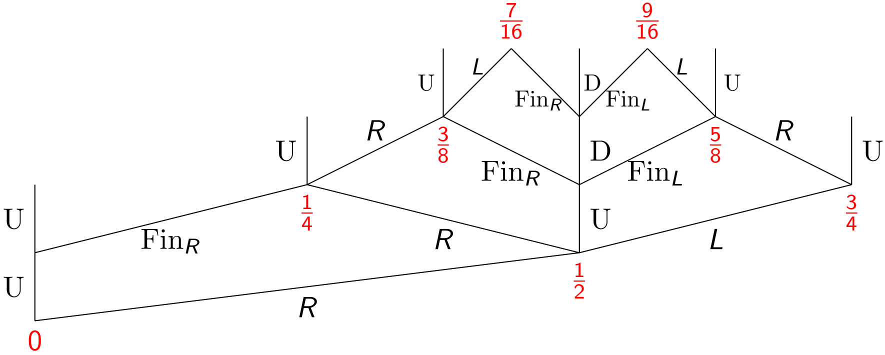
What is the first digit? Cure: delay.

- For binary code: add 0. Signed digit code

$$\sum_{i<k} \frac{d_i}{2^{i+1}} \qquad \text{with } d_i \in \{-1, 0, 1\}.$$

  Widely used for real number computation. There is a lot of redundancy: $\bar{1}1$ and $0\bar{1}$ both denote $-\frac{1}{4}$.
- For Gray-code: add U (undefined), D (delay), $\mathrm{Fin}_{L/R}$ (finally left / right). Pre-Gray code.

Pre-Gray code



After computation in pre-Gray code, one can remove Fin_a by

$$\mathrm{U} \circ \mathrm{Fin}_a \mapsto a \circ \mathrm{R}, \qquad \mathrm{D} \circ \mathrm{Fin}_a \mapsto \mathrm{Fin}_a \circ \mathrm{L}.$$

Another source of non-uniqueness for infinite sequences:

(i) $\mathrm{RRRLLL}\ldots$

(ii) $\mathrm{RLRLLL}\ldots$

(iii) $\mathrm{RUDDDD}\ldots$

all denote $\frac{1}{2}$. From these three infinite sequences remove (i), (ii) and only keep (iii) to denote $\frac{1}{2}$. Then, generally,

- U occurs in a context $\mathrm{UDDDD}\ldots$ only, and
- U appears iff we have a dyadic rational.

Result: unique representation of real numbers by infinite sequences (or streams), called pure Gray code.

Average for signed digit streams

Goal: extract stream algorithms from proofs. Example: proof that the average of two real numbers in $[-1, 1]$ is in $[-1, 1]$ again.

- Need to accomodate streams in our logical framework.
- Model infinite sequences of signed digits (streams) as "objects" in the (free) algebra **I** given by the constructor $\mathrm{C}\colon \mathbf{SD} \to \mathbf{I} \to \mathbf{I}$.
- **SD** $:= \{\mathrm{Lft}, \mathrm{Mid}, \mathrm{Rht}\}$: formal representation of signed digits.

Intuitively, the stream $d_0, d_1, d_2 \dots$ represents the real number

$$\sum_{i=0}^{\infty} \frac{d_i}{2^{i+1}} \qquad \text{with } d_i \in \{-1, 0, 1\}.$$

Conventions: x, y, z reals in $[-1, 1]$, d, e, i, j, k integers, $x = y$ defined equality on reals.

The predicates I and ${}^{\mathrm{co}}I$

Inductively define a predicate I by the single clause

$$\forall^{\mathrm{nc}}_{d \in \mathrm{SD}} \forall^{\mathrm{nc}}_{x \in I} \forall^{\mathrm{nc}}_{y} \left(y = \frac{x+d}{2} \to y \in I \right) \tag{1}$$

which abbreviates

$$\forall^{\mathrm{nc}}_{d,x,y} \left(d \in \mathrm{SD} \to x \in I \to y = \frac{x+d}{2} \to y \in I \right).$$

SD is a (formally inductive) predicate expressing that the integer d is a signed digit, i.e., $|d| \leq 1$.

- $\forall^{\mathrm{nc}}_{d,x,y}$: type of "problem" (1) is independent of d, x, y.
- Computational content only arises from inductive predicates, here SD and I. Hence the type of (1) is $\mathbf{SD} \to \mathbf{I} \to \mathbf{I}$.

Dually to I we coinductively define a predicate ${}^{\mathrm{co}}I$ by the (single) clause

$$\forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}I} \exists^{\mathrm{r}}_{d \in \mathrm{SD}} \exists^{\mathrm{r}}_{x' \in {}^{\mathrm{co}}I} (x = \frac{x' + d}{2}). \tag{2}$$

Here

- $\exists^{\mathrm{r}}_{d} A$ is an (inductively defined) version of $\exists_{d} A$, making the type of $\exists^{\mathrm{r}}_{d} A$ independent of d.
- Hence the type of (2) is $\mathbf{I} \to \mathbf{SD} \times \mathbf{I}$: the stream is destructed into its head and its tail.

I and ${}^{\mathrm{co}}I$ are defined as fixed points of an operator

$$\Phi(X) := \{\, x \mid \exists^{\mathrm{r}}_{d \in \mathrm{SD}} \exists^{\mathrm{r}}_{x' \in X} (x = \frac{x' + d}{2}) \,\}.$$

Then

$$\begin{aligned} I &:= \mu_X \Phi(X) && \text{least fixed point} \\ {}^{\mathrm{co}}I &:= \nu_X \Phi(X) && \text{greatest fixed point} \end{aligned}$$

satisfy the (strengthened) axioms

$$\begin{aligned} \Phi(I \cap X) \subseteq X \to I \subseteq X && \text{induction} \\ X \subseteq \Phi({}^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I && \text{coinduction} \end{aligned}$$

("strengthened" because their hypotheses are weaker than the fixed point property $\Phi(X) = X$).

Goal: compute the average of two stream-coded reals. Prove

$$\forall^{\mathrm{nc}}_{x,x' \in {}^{\mathrm{co}}I} \left(\frac{x + x'}{2} \in {}^{\mathrm{co}}I \right). \tag{3}$$

Computational content of this proof will be the desired algorithm.

Informal proof (from Ulrich Berger & Monika Seisenberger 2006). Define sets P, Q of averages, Q with a “carry” $i \in \mathbb{Z}$:

$$P := \{ \frac{x + y}{2} \mid x, y \in {}^{\mathrm{co}}I \}, \quad Q := \{ \frac{x + y + i}{4} \mid x, y \in {}^{\mathrm{co}}I, i \in \mathrm{SD}_2 \},$$

where SD_2 is a (formally inductive) predicate expressing that the integer i is an extended signed digit, i.e., $|i| \leq 2$.

Recall that ${}^{\mathrm{co}}I$ is a fixed point of Φ. Hence ${}^{\mathrm{co}}I \subseteq \Phi({}^{\mathrm{co}}I)$:

$$\mathrm{CoIClause}\colon \forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}I} \exists^{\mathrm{r}}_{d \in \mathrm{SD}} \exists^{\mathrm{r}}_{x' \in {}^{\mathrm{co}}I} (x = \frac{x' + d}{2}). \qquad (4)$$

It suffices to show that Q satisfies (4).

- Then $Q \subseteq {}^{\mathrm{co}}I$ by the greatest-fixed-point axiom for ${}^{\mathrm{co}}I$.
- Since also $P \subseteq Q$ we obtain $P \subseteq {}^{\mathrm{co}}I$, which is our claim.

(4) implies $P \subseteq Q$:

$$\forall^{\mathrm{nc}}_{x,y \in {}^{\mathrm{co}}I} \exists^{\mathrm{r}}_{i \in \mathrm{SD}_2} \exists^{\mathrm{r}}_{x',y' \in {}^{\mathrm{co}}I} (\frac{x+y}{2} = \frac{x' + y' + i}{4}).$$

Q satisfies the ${}^{\mathrm{co}}I$-clause (4):

$$\forall^{\mathrm{nc}}_{i \in \mathrm{SD}_2} \forall^{\mathrm{nc}}_{x,y \in {}^{\mathrm{co}}I} \exists^{\mathrm{r}}_{j \in \mathrm{SD}_2} \exists^{\mathrm{r}}_{d \in \mathrm{SD}} \exists^{\mathrm{r}}_{x',y' \in {}^{\mathrm{co}}I} \Big(\frac{x+y+i}{4} = \frac{\frac{x'+y'+j}{4} + d}{2} \Big).$$

Proof. Using functions $J, K\colon \mathbb{Z} \to \mathbb{Z}$ such that

$$\forall_k (k = J(k) + 4K(k)) \quad \forall_k (|J(k)| \le 2) \quad \forall_k (|k| \le 6 \to |K(k)| \le 1)$$

we can relate $\frac{x+d}{2}$ and $\frac{x+y+i}{4}$ by

$$\frac{\frac{x+d}{2} + \frac{y+e}{2} + i}{4} = \frac{\frac{x+y+J(d+e+2i)}{4} + K(d+e+2i)}{2}. \qquad (5)$$

Now (4) gives the claim.

By coinduction we obtain $Q \subseteq {}^{\mathrm{co}}I$:

$$\forall^{\mathrm{nc}}_z (\exists^{\mathrm{r}}_{i \in \mathrm{SD}_2} \exists^{\mathrm{r}}_{x,y \in {}^{\mathrm{co}}I} (z = \frac{x+y+i}{4}) \to z \in {}^{\mathrm{co}}I).$$

This gives our claim

$$\forall^{\mathrm{nc}}_{x,y \in {}^{\mathrm{co}}I} (\frac{x+y}{2} \in {}^{\mathrm{co}}I).$$

Implicit algorithm. $P \subseteq Q$ computes the first "carry" $i \in \mathrm{SD}_2$ and the tails of the inputs. Then $f \colon \mathbf{SD}_2 \times \mathbf{I} \times \mathbf{I} \to \mathbf{I}$ defined corecursively by

$$f(i, \mathrm{C}_d(v), \mathrm{C}_e(w)) = \mathrm{C}_{K(d+e+2i)}(f(J(d+e+2i), v, w))$$

is called repeatedly and computes the average step by step.

Average for pre-Gray code

Method essentially the same as for signed digit streams.

- Only need to insert a different computational content to the predicates expressing how a real x is given.
- Instead of ${}^{\mathrm{co}}I$ for signed digit streams we now need two such predicates ${}^{\mathrm{co}}G$ and ${}^{\mathrm{co}}H$, corresponding to the two "modes" we have in pre-Gray code.

Algebras G and H

We model pre-Gray codes as objects in the (simultaneously defined free) algebras **G** and **H** given by the constructors

$$\mathrm{LR}_a\colon \mathbf{G} \to \mathbf{G}$$
$$\mathrm{U}\colon \mathbf{H} \to \mathbf{G}$$
$$\mathrm{Fin}_a\colon \mathbf{G} \to \mathbf{H}$$
$$\mathrm{D}\colon \mathbf{H} \to \mathbf{H}$$

with $a \in \{-1, 1\}$.

Predicates ${}^{\mathrm{co}}G$ and ${}^{\mathrm{co}}H$

Let

$$\Gamma(X,Y) := \{\, x \mid \exists^{\mathrm{r}}_{x' \in X} \exists^{\mathrm{r}}_{a \in \mathrm{PSD}} (x = -a\frac{x'-1}{2}) \vee \exists^{\mathrm{r}}_{x' \in Y} (x = \frac{x'}{2}) \,\},$$

$$\Delta(X,Y) := \{\, x \mid \exists^{\mathrm{r}}_{x' \in X} \exists^{\mathrm{r}}_{a \in \mathrm{PSD}} (x = a\frac{x'+1}{2}) \vee \exists^{\mathrm{r}}_{x' \in Y} (x = \frac{x'}{2}) \,\}$$

and define

$$({}^{\mathrm{co}}G, {}^{\mathrm{co}}H) := \nu_{(X,Y)}(\Gamma(X,Y), \Delta(X,Y)) \qquad \text{(greatest fixed point)}$$

Consequences:

$$\forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}G} (\exists^{\mathrm{r}}_{x' \in {}^{\mathrm{co}}G} \exists^{\mathrm{r}}_{a \in \mathrm{PSD}} (x = -a\frac{x'-1}{2}) \vee \exists^{\mathrm{r}}_{x' \in {}^{\mathrm{co}}H} (x = \frac{x'}{2}))$$

$$\forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}H} (\exists^{\mathrm{r}}_{x' \in {}^{\mathrm{co}}G} \exists^{\mathrm{r}}_{a \in \mathrm{PSD}} (x = a\frac{x'+1}{2}) \vee \exists^{\mathrm{r}}_{x' \in {}^{\mathrm{co}}H} (x = \frac{x'}{2}))$$

Lemma (CoGMinus)

$$\forall^{\mathrm{nc}}_x ({}^{\mathrm{co}}G(-x) \to {}^{\mathrm{co}}Gx),$$
$$\forall^{\mathrm{nc}}_x ({}^{\mathrm{co}}H(-x) \to {}^{\mathrm{co}}Hx).$$

Implicit algorithm. $f\colon \mathbf{G} \to \mathbf{G}$ and $f'\colon \mathbf{H} \to \mathbf{H}$ defined by

$$f(\mathrm{LR}_a(p)) = \mathrm{LR}_{-a}(p), \qquad f'(\mathrm{Fin}_a(p)) = \mathrm{Fin}_{-a}(p),$$
$$f(\mathrm{U}(q)) = \mathrm{U}(f'(q)), \qquad f'(\mathrm{D}(q)) = \mathrm{D}(f'(q)).$$

Using CoGMinus we prove that ${}^{\mathrm{co}}G$ and ${}^{\mathrm{co}}H$ are equivalent.

Lemma (CoHToCoG)

$$\forall^{\mathrm{nc}}_x ({}^{\mathrm{co}}Hx \to {}^{\mathrm{co}}Gx),$$
$$\forall^{\mathrm{nc}}_x ({}^{\mathrm{co}}Gx \to {}^{\mathrm{co}}Hx).$$

Implicit algorithm. $g\colon \mathbf{H} \to \mathbf{G}$ and $h\colon \mathbf{G} \to \mathbf{H}$:

$$g(\mathrm{Fin}_a(p)) = \mathrm{LR}_a(f^-(p)), \qquad h(\mathrm{LR}_a(p)) = \mathrm{Fin}_a(f^-(p)),$$
$$g(\mathrm{D}(q)) = \mathrm{U}(q), \qquad h(\mathrm{U}(q)) = \mathrm{D}(q)$$

where $f^- := \mathrm{cCoGMinus}$ (cL denotes the function extracted from the proof of a lemma L). No corecursive call is involved.

The proof of the existence of the average w.r.t. Gray-coded reals is similar to the proof for signed digit stream coded reals. To prove

$$\forall^{\mathrm{nc}}_{x,y\in {}^{\mathrm{co}}G}\Big(\frac{x+y}{2} \in {}^{\mathrm{co}}G\Big)$$

consider again two sets of averages, the second one with a "carry":

$$P := \{\, \frac{x+y}{2} \mid x, y \in {}^{\mathrm{co}}G \,\}, \quad Q := \{\, \frac{x+y+i}{4} \mid x, y \in {}^{\mathrm{co}}G,\ i \in \mathrm{SD}_2 \,\}.$$

Suffices: Q satisfies the clause coinductively defining ${}^{\mathrm{co}}G$. Then by the greatest-fixed-point axiom for ${}^{\mathrm{co}}G$ we have $Q \subseteq {}^{\mathrm{co}}G$. Since also $P \subseteq Q$ we obtain $P \subseteq {}^{\mathrm{co}}G$, which is our claim.

Lemma (CoGAvToAvc)

$$\forall^{\mathrm{nc}}_{x,y \in {}^{\mathrm{co}}G} \exists^{\mathrm{r}}_{i \in \mathrm{SD}_2} \exists^{\mathrm{r}}_{x',y' \in {}^{\mathrm{co}}G} \left(\frac{x+y}{2} = \frac{x'+y'+i}{4} \right).$$

(Immediate from CoGClause.)

Implicit algorithm.
We can easily prove CoGPsdTimes: $\forall^{\mathrm{nc}}_{a \in \mathrm{PSD}} \forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}G} (ax \in {}^{\mathrm{co}}G)$.
Write f^* for cCoGPsdTimes and s for cCoHToCoG.

$$\begin{aligned} f(\mathrm{LR}_a(p), \mathrm{LR}_{a'}(p')) &= (a + a', f^*(-a, p), f^*(-a', p')), \\ f(\mathrm{LR}_a(p), \mathrm{U}(q)) &= (a, f^*(-a, p), s(q)), \\ f(\mathrm{U}(q), \mathrm{LR}_a(p)) &= (a, s(q), f^*(-a, p)), \\ f(\mathrm{U}(q), \mathrm{U}(q')) &= (0, s(q), s(q')). \end{aligned}$$

Lemma (CoGAvcSatCoICl)

$$\forall^{\mathrm{nc}}_{i \in \mathrm{SD}_2} \forall^{\mathrm{nc}}_{x,y \in {}^{\mathrm{co}}G} \exists^{\mathrm{r}}_{j \in \mathrm{SD}_2} \exists^{\mathrm{r}}_{d \in \mathrm{SD}} \exists^{\mathrm{r}}_{x',y' \in {}^{\mathrm{co}}G} \Big(\frac{x+y+i}{4} = \frac{\frac{x'+y'+j}{4} + d}{2}\Big).$$

(As in CoIAvcSatCoICl we need functions J, K with JKProp (5):

$$\frac{\frac{x+d}{2} + \frac{y+e}{2} + i}{4} = \frac{\frac{x+y+J(d+e+2i)}{4} + K(d+e+2i)}{2}.$$

Then CoGClause gives the claim.)

Implicit algorithm.

$$\begin{aligned}
f(i, \mathrm{LR}_a(p), \mathrm{LR}_{a'}(p')) &= (J(a+a'+2i), K(a+a'+2i), f^*(-a,p), f^*(-a',p')),\\
f(i, \mathrm{LR}_a(p), \mathrm{U}(q)) &= (J(a+2i), K(a+2i), f^*(-a,p), s(q)),\\
f(i, \mathrm{U}(q), \mathrm{LR}_a(p)) &= (J(a+2i), K(a+2i), s(q), f^*(-a,p)),\\
f(i, \mathrm{U}(q), \mathrm{U}(q')) &= (J(2i), K(2i), s(q), s(q')).
\end{aligned}$$

Lemma (CoGAvcToCoG)

$$\forall^{\mathrm{nc}}_{z}(\exists^{\mathrm{r}}_{x,y\in{}^{\mathrm{co}}G}\exists^{\mathrm{r}}_{i\in\mathrm{SD}_2}(z=\frac{x+y+i}{4})\to{}^{\mathrm{co}}G(z)),$$
$$\forall^{\mathrm{nc}}_{z}(\exists^{\mathrm{r}}_{x,y\in{}^{\mathrm{co}}G}\exists^{\mathrm{r}}_{i\in\mathrm{SD}_2}(z=\frac{x+y+i}{4})\to{}^{\mathrm{co}}H(z)).$$

In the proof we need a lemma:

$$\mathrm{SdDisj}\colon\forall^{\mathrm{nc}}_{d\in\mathrm{SD}}(d=0\vee^{\mathrm{r}}\exists^{\mathrm{r}}_{a\in\mathrm{PSD}}(d=a)).$$

Here $\vee^{\mathrm{r}}$ is an (inductively defined) variant of $\vee$ where only the content of the right hand side is kept.

Implicit algorithm.

$$
\begin{aligned}
g(i,p,p') = {} & \text{let } (i_1,d,p_1,p_1') = \text{cCoGAvcSatCoICl}(i,p,p') \text{ in} \\
& \quad \text{case cSdDisj}(d) \text{ of} \\
& \quad\quad 0 \to \mathrm{U}(h(i_1,p_1,p_1')) \\
& \quad\quad a \to \mathrm{LR}_a(g(-ai_1, f^*(-a,p_1), f^*(-a,p_1'))),
\end{aligned}
$$

$$
\begin{aligned}
h(i,p,p') = {} & \text{let } (i_1,d,p_1,p_1') = \text{cCoGAvcSatCoICl}(i,p,p') \text{ in} \\
& \quad \text{case cSdDisj}(d) \text{ of} \\
& \quad\quad 0 \to \mathrm{D}(h(i_1,p_1,p_1')) \\
& \quad\quad a \to \mathrm{Fin}_a(g(-ai_1, f^*(-a,p_1), f^*(-a,p_1'))).
\end{aligned}
$$

Theorem (CoGAverage)

$$\forall^{\mathrm{nc}}_{x,y \in {}^{\mathrm{co}}G} \left(\frac{x+y}{2} \in {}^{\mathrm{co}}G\right).$$

Implicit algorithm. Compose cCoGAvToAvc with cCoGAvcToCoG.

Conclusion

1. Constructive analysis, with constructions $\sim$ good algorithms.
2. Exact real arithmetic.
   - Want formally verified algorithms on real numbers given as streams (signed digits or pre-Gray code).
   - Consider formal existence proofs M and apply realizability to extract their computational content.
   - Switch between different representations of reals by labelling $\forall_x$ as $\forall_x^{\mathrm{nc}}$ and relativise x to a coinductive predicate whose computational content is a stream representing x.
   - The desired algorithm is obtained as the extracted term $\mathrm{et}(M)$ of the existence proof M.
   - Verification by (automatically generated) formal soundness proof of the realizability interpretation.