Logic for exact real arithmetic: Lab, Minlog

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

Interval analysis and constructive mathematics
CMO-BIRS, Oaxaca, 13. -18. November 2016

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 proofs M and apply realizability to extract their computational content.
- Switch between different formats 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.

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

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

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

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 proofs M and apply realizability to extract their computational content.
- Switch between different formats 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:

$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 1\}.$$

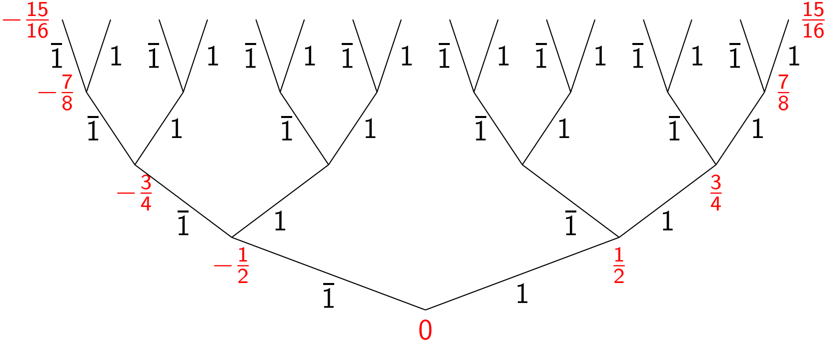
with $\bar{1} := -1$. Adjacent dyadics can differ in many digits:

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

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

Dyadic rationals:

$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 1\}.$$



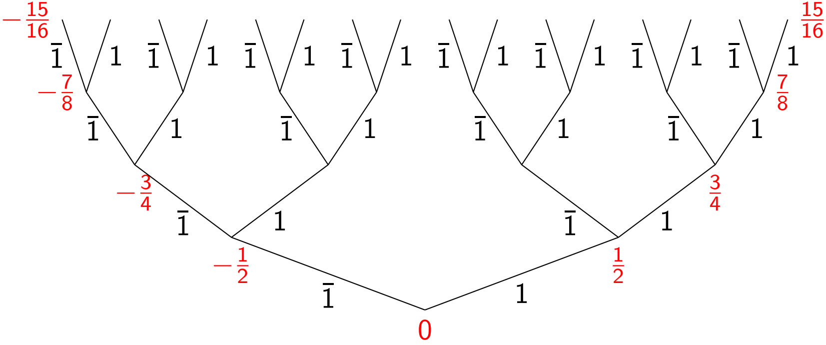
with $\bar{1} := -1$. Adjacent dyadics can differ in many digits:

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

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

Dyadic rationals:

$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 1\}.$$



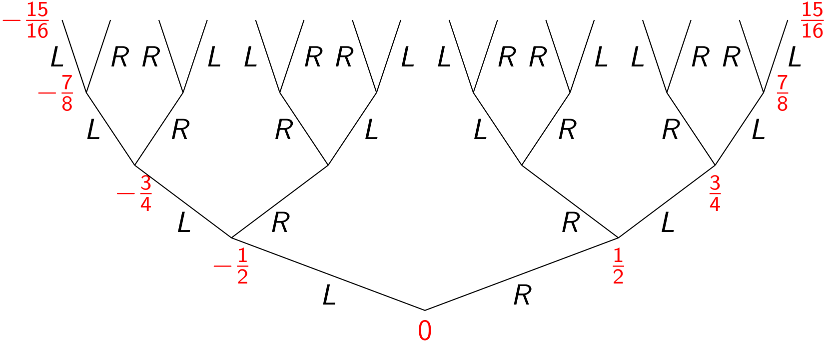
with $\bar{1} := -1$. Adjacent dyadics can differ in many digits:

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

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

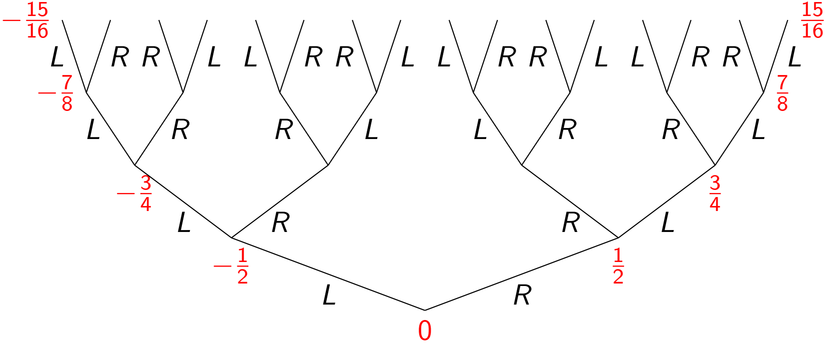
$$\frac{7}{16} \sim \mathrm{RRRL}, \qquad \frac{9}{16} \sim \mathrm{RLRL}.$$

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



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

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

$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 0, 1\}.$$

  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.

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

$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 0, 1\}.$$

  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.

Problem with productivity:

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

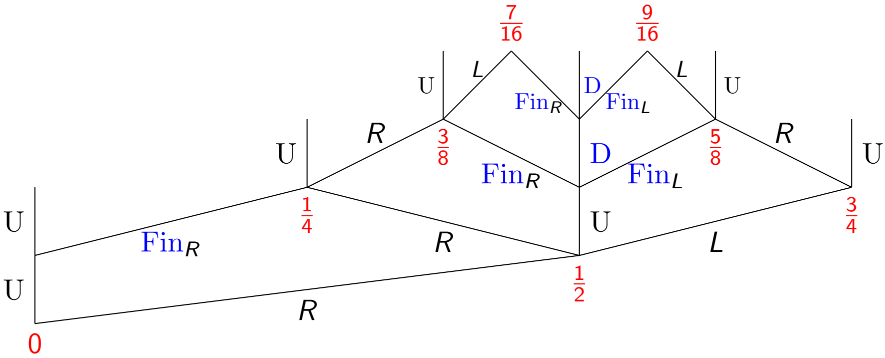
What is the first digit? Cure: delay.

- For binary code: add 0. Signed digit code

$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 0, 1\}.$$

  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.

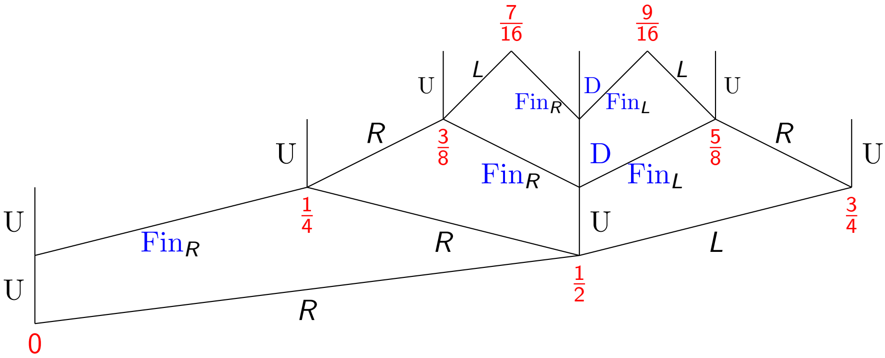
Pre-Gray code



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

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

Pre-Gray code



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

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

$$\text{RRRLLL}\ldots \qquad \text{RLRLLL}\ldots \qquad \text{RUDDDD}\ldots$$

all denote $\frac{1}{2}$. Only keep the latter to denote $\frac{1}{2}$. Then, generally,

- U occurs in a context UDDDD . . . only, and
- U appears iff we have a dyadic rational.

Result: unique representation, called pure Gray code.

$$\mathrm{RRRLLL}\ldots \qquad \mathrm{RLRLLL}\ldots \qquad \mathrm{RU{\color{blue}DDDD}}\ldots$$

all denote $\frac{1}{2}$. Only keep the latter to denote $\frac{1}{2}$. Then, generally,

- U occurs in a context UDDDD . . . only, and
- U appears iff we have a dyadic rational.

Result: unique representation, called pure Gray code.

$$\mathrm{RRRLLL}\ldots \qquad \mathrm{RLRLLL}\ldots \qquad \mathrm{RU{\color{blue}DDDD}}\ldots$$

all denote $\frac{1}{2}$. Only keep the latter to denote $\frac{1}{2}$. Then, generally,

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

Result: unique representation, called pure Gray code.

$$\mathrm{RRRLLL}\ldots \qquad \mathrm{RLRLLL}\ldots \qquad \mathrm{RUDDDD}\ldots$$

all denote $\frac{1}{2}$. Only keep the latter 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, called pure Gray code.

$$\mathrm{RRRLLL}\ldots \qquad \mathrm{RLRLLL}\ldots \qquad \mathrm{RU}\mathrm{DDDD}\ldots$$

all denote $\frac{1}{2}$. Only keep the latter 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, called pure Gray code.

Average for signed digit streams

Goal:

$$\forall^{\mathrm{nc}}_{x,y}(\underbrace{x, y \in {}^{\mathrm{co}}I}_{x,y\in[-1,1]} \to \underbrace{\frac{x+y}{2} \in {}^{\mathrm{co}}I}_{\frac{x+y}{2}\in[-1,1]}).$$

- Need to accomodate streams in our logical framework.
- Model streams as "cototal objects" in the (free) algebra **I** given by the constructor $\mathrm{C}\colon \mathbf{SD} \to \mathbf{I} \to \mathbf{I}$.

Intuitively, $k_0, k_1, k_2 \dots$ represents

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

Average for signed digit streams

Goal:

$$\forall^{\mathrm{nc}}_{x,y}(\underbrace{x, y \in {}^{\mathrm{co}}I}_{x,y\in[-1,1]} \to \underbrace{\frac{x+y}{2} \in {}^{\mathrm{co}}I}_{\frac{x+y}{2}\in[-1,1]}).$$

- Need to accomodate streams in our logical framework.
- Model streams as "cototal objects" in the (free) algebra **I** given by the constructor $\mathrm{C}\colon \mathbf{SD} \to \mathbf{I} \to \mathbf{I}$.

Intuitively, $k_0, k_1, k_2 \ldots$ represents

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

Average for signed digit streams

Goal:

$$\forall^{\mathrm{nc}}_{x,y}(\underbrace{x, y \in {}^{\mathrm{co}}I}_{x,y\in[-1,1]} \to \underbrace{\frac{x+y}{2} \in {}^{\mathrm{co}}I}_{\frac{x+y}{2}\in[-1,1]}).$$

- Need to accomodate streams in our logical framework.
- Model streams as "cototal objects" in the (free) algebra **I** given by the constructor C: **SD** $\to$ **I** $\to$ **I**.

Intuitively, $k_0, k_1, k_2 \ldots$ represents

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

Average for signed digit streams

Goal:

$$\forall^{\mathrm{nc}}_{x,y}(\underbrace{x, y \in {}^{\mathrm{co}}I}_{x,y \in [-1,1]} \to \underbrace{\frac{x+y}{2} \in {}^{\mathrm{co}}I}_{\frac{x+y}{2} \in [-1,1]}).$$

- Need to accomodate streams in our logical framework.
- Model streams as "cototal objects" in the (free) algebra **I** given by the constructor $\mathrm{C} \colon \mathbf{SD} \to \mathbf{I} \to \mathbf{I}$.

Intuitively, $k_0, k_1, k_2 \ldots$ represents

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

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

Then

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

satisfy the (strengthened) axioms

$$\Phi(I \cap X) \subseteq X \to I \subseteq X \qquad \text{induction}$$
$$X \subseteq \Phi(^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I \qquad \text{coinduction}$$

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

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

Then

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

satisfy the (strengthened) axioms

$$\Phi(I \cap X) \subseteq X \to I \subseteq X \qquad \text{induction}$$
$$X \subseteq \Phi(^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I \qquad \text{coinduction}$$

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

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

Then

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

satisfy the (strengthened) axioms

$$\Phi(I \cap X) \subseteq X \to I \subseteq X \qquad \text{induction}$$
$$X \subseteq \Phi(^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I \qquad \text{coinduction}$$

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

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

Then

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

satisfy the (strengthened) axioms

$$\Phi(I \cap X) \subseteq X \to I \subseteq X \qquad \text{induction}$$
$$X \subseteq \Phi(^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I \qquad \text{coinduction}$$

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

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

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

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" $i \in \mathbb{Z}$:

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

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

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

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

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" $i \in \mathbb{Z}$:

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

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

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

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

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" $i \in \mathbb{Z}$:

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

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

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

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

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

$$\forall_i(i=J(i)+4K(i))\quad\forall_i(|J(i)|\leq 2)\quad\forall_i(|i|\leq 6\to|K(i)|\leq 1)$$

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

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

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

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

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

$$\forall_i (i = J(i) + 4K(i)) \quad \forall_i (|J(i)| \leq 2) \quad \forall_i (|i| \leq 6 \to |K(i)| \leq 1)$$

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

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

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

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

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

$$\forall_i (i = J(i) + 4K(i)) \quad \forall_i (|J(i)| \leq 2) \quad \forall_i (|i| \leq 6 \to |K(i)| \leq 1)$$

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

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

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

$$f(i, \mathrm{C}_d(u), \mathrm{C}_e(v)) = \mathrm{C}_{K(k+l+2i)}(f(J(k+l+2i), u, v))$$

is called repeatedly and computes the average step by step. (Here $(d,k),(e,l) \in \mathrm{SD}^{\mathbf{r}}$).

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

$$f(i, \mathrm{C}_d(u), \mathrm{C}_e(v)) = \mathrm{C}_{K(k+l+2i)}(f(J(k+l+2i), u, v))$$

is called repeatedly and computes the average step by step. (Here $(d,k),(e,l) \in \mathrm{SD}^{\mathbf{r}}$).

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

$$f(i, \mathrm{C}_d(u), \mathrm{C}_e(v)) = \mathrm{C}_{K(k+l+2i)}(f(J(k+l+2i), u, v))$$

is called repeatedly and computes the average step by step. (Here $(d,k), (e,l) \in \mathrm{SD}^{\mathbf{r}}$).

Realizability

Define the realizability extension $\Phi^{\mathbf{r}}$ of Φ by

$$\Phi^{\mathbf{r}}(Y) := \{\, (u,x) \mid \exists^{\mathrm{nc}}_{(d,k)\in \mathrm{SD}^{\mathbf{r}}} \exists^{\mathrm{nc}}_{(u',x')\in Y}(x = \frac{x'+k}{2} \wedge u = \mathrm{C}_d(u'))\,\}$$

Let

$$\begin{aligned} I^{\mathbf{r}} &:= \mu_Y \Phi^{\mathbf{r}}(Y) && \text{least fixed point} \\ ({}^{\mathrm{co}}I)^{\mathbf{r}} &:= \nu_Y \Phi^{\mathbf{r}}(Y) && \text{greatest fixed point} \end{aligned}$$

satisfying the (strengthened) axioms

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

From the proof

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

extract a term $\mathrm{et}(M)$. The Soundness theorem gives a proof of

$$\mathrm{et}(M) \;\mathbf{r}\; \forall^{\mathrm{nc}}_{x,y \in {}^{\mathrm{co}}I} \left(\frac{x+y}{2} \in {}^{\mathrm{co}}I\right)$$

Brouwer-Heyting-Kolmogorov interpretation:

$$u \;\mathbf{r}\; (x \in {}^{\mathrm{co}}I) \to v \;\mathbf{r}\; (y \in {}^{\mathrm{co}}I) \to \mathrm{et}(M)(u,v) \;\mathbf{r}\; \left(\frac{x+y}{2} \in {}^{\mathrm{co}}I\right)$$

This is a formal verification that $\mathrm{et}(M)$ computes the average w.r.t. signed digit streams.

From the proof

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

extract a term $\mathrm{et}(M)$. The Soundness theorem gives a proof of

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

Brouwer-Heyting-Kolmogorov interpretation:

$$u\ \mathbf{r}\ (x\in {}^{\mathrm{co}}I)\to v\ \mathbf{r}\ (y\in {}^{\mathrm{co}}I)\to \mathrm{et}(M)(u,v)\ \mathbf{r}\ (\frac{x+y}{2}\in {}^{\mathrm{co}}I)$$

This is a formal verification that $\mathrm{et}(M)$ computes the average w.r.t. signed digit streams.

From the proof

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

extract a term $\mathrm{et}(M)$. The Soundness theorem gives a proof of

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

Brouwer-Heyting-Kolmogorov interpretation:

$$u\ \mathbf{r}\ (x\in {}^{\mathrm{co}}I)\to v\ \mathbf{r}\ (y\in {}^{\mathrm{co}}I)\to \mathrm{et}(M)(u,v)\ \mathbf{r}\ (\frac{x+y}{2}\in {}^{\mathrm{co}}I)$$

This is a formal verification that $\mathrm{et}(M)$ computes the average w.r.t. signed digit streams.

From the proof

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

extract a term $\mathrm{et}(M)$. The Soundness theorem gives a proof of

$$\mathrm{et}(M)\ \mathbf{r}\ \forall^{\mathrm{nc}}_{x,y\in {}^{\mathrm{co}}I}\Big(\frac{x+y}{2} \in {}^{\mathrm{co}}I\Big)$$

Brouwer-Heyting-Kolmogorov interpretation:

$$u\ \mathbf{r}\ (x \in {}^{\mathrm{co}}I) \to v\ \mathbf{r}\ (y \in {}^{\mathrm{co}}I) \to \mathrm{et}(M)(u,v)\ \mathbf{r}\ \Big(\frac{x+y}{2} \in {}^{\mathrm{co}}I\Big)$$

This is a formal verification that $\mathrm{et}(M)$ computes the average w.r.t. signed digit streams.

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" in pre-Gray code.

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" in pre-Gray code.

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" in pre-Gray code.

Algebras G and H

We model pre-Gray codes as "cotatal 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

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

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

and define

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

Consequences:

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

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

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

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

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

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

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 $h\colon \mathbf{G} \to \mathbf{H}$:

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

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

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 $h\colon \mathbf{G} \to \mathbf{H}$:

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

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

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 $h\colon \mathbf{G} \to \mathbf{H}$:

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

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

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

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.

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

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

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.

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

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

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)

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

Proof needs CoGPsdTimes: $\forall^{\mathrm{nc}}_{a \in \mathrm{PSD}} \forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}G} (ax \in {}^{\mathrm{co}}G)$. Rest easy, using CoGClause.

Implicit algorithm.
Write f^* for cCoGPsdTimes and s for cCoHToCoG.

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

Lemma (CoGAvToAvc)

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

Proof needs CoGPsdTimes: $\forall^{\mathrm{nc}}_{a \in \mathrm{PSD}} \forall^{\mathrm{nc}}_{x \in {}^{\mathrm{co}}G} (ax \in {}^{\mathrm{co}}G)$. Rest easy, using CoGClause.

Implicit algorithm.

Write f^* for cCoGPsdTimes and s for cCoHToCoG.

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

Lemma (CoGAvToAvc)

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

Proof needs CoGPsdTimes: $\forall^{\mathrm{nc}}_{a\in \mathrm{PSD}}\forall^{\mathrm{nc}}_{x\in {}^{\mathrm{co}}G}(ax\in {}^{\mathrm{co}}G)$. Rest easy, using CoGClause.

Implicit algorithm.
Write f^* for cCoGPsdTimes and s for cCoHToCoG.

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

Lemma (CoGAvcSatCoICl)

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

(As in CoIAvcSatCoICl we need functions J, K with

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

Then CoGClause gives the claim.)

Implicit algorithm.

$$f(i, \mathrm{LR}_a(u), \mathrm{LR}_{a'}(u')) = (J(a+a'+2i), K(a+a'+2i), f^*(-a,u), f^*(-a',u'))$$

$$f(i, \mathrm{LR}_a(u), \mathrm{U}(v)) = (J(a+2i), K(a+2i), f^*(-a,u), s(v)),$$

$$f(i, \mathrm{U}(v), \mathrm{LR}_a(u)) = (J(a+2i), K(a+2i), s(v), f^*(-a,u)),$$

$$f(i, \mathrm{U}(v), \mathrm{U}(v')) = (J(2i), K(2i), s(v), s(v')).$$

Lemma (CoGAvcSatCoICl)

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

(As in CoIAvcSatCoICl we need functions J, K with

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

Then CoGClause gives the claim.)

Implicit algorithm.

$$f(i,\mathrm{LR}_a(u),\mathrm{LR}_{a'}(u'))=(J(a+a'+2i),K(a+a'+2i),f^*(-a,u),f^*(-a',u'))$$
$$f(i,\mathrm{LR}_a(u),\mathrm{U}(v))=(J(a+2i),K(a+2i),f^*(-a,u),s(v)),$$
$$f(i,\mathrm{U}(v),\mathrm{LR}_a(u))=(J(a+2i),K(a+2i),s(v),f^*(-a,u)),$$
$$f(i,\mathrm{U}(v),\mathrm{U}(v'))=(J(2i),K(2i),s(v),s(v')).$$

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:

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

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

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:

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

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

Implicit algorithm.

$$\begin{aligned}
g(i, u, u') = {} & \text{let } (i_1, k, u_1, u_1') = \mathrm{cCoGAvcSatCoICl}(i, u, u') \text{ in} \\
& \quad \text{case } \mathrm{cSdDisj}(k) \text{ of} \\
& \qquad 0 \to \mathrm{U}(h(i_1, u_1, u_1')) \\
& \qquad a \to \mathrm{LR}_a(g(-ai_1, f^*(-a, u_1), f^*(-a, u_1'))),
\end{aligned}$$

$$\begin{aligned}
h(i, u, u') = {} & \text{let } (i_1, k, u_1, u_1') = \mathrm{cCoGAvcSatCoICl}(i, u, u') \text{ in} \\
& \quad \text{case } \mathrm{cSdDisj}(k) \text{ of} \\
& \qquad 0 \to \mathrm{D}(h(i_1, u_1, u_1')) \\
& \qquad a \to \mathrm{Fin}_a(g(-ai_1, f^*(-a, u_1), f^*(-a, u_1'))).
\end{aligned}$$

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.

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

- Want formally verified algorithms on real numbers given as streams (signed digits or pre-Gray code).
- Consider formal 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 proof M.
- Verification by (automatically generated) formal soundness proof of the realizability interpretation.