

Logic for exact real arithmetic

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

Second CORE meeting, January 27, 2017

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
- ▶ $\{-1, 1, \perp\}$ with at most one \perp (“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**:

$$\forall_x A \quad \mapsto \quad \forall_x^{\text{nc}}(x \in {}^{\text{co}}I \rightarrow A) \quad (\text{abbreviated } \forall_{x \in {}^{\text{co}}I}^{\text{nc}} A).$$

- ▶ Computational content of $x \in {}^{\text{co}}I$ 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
- ▶ $\{-1, 1, \perp\}$ with at most one \perp (“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**:
 $\forall_x A \quad \mapsto \quad \forall_x^{\text{nc}}(x \in {}^{\text{co}}I \rightarrow A)$ (abbreviated $\forall_{x \in {}^{\text{co}}I}^{\text{nc}} A$).
- ▶ Computational content of $x \in {}^{\text{co}}I$ 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
- ▶ $\{-1, 1, \perp\}$ with at most one \perp (“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**:

$$\forall_x A \quad \mapsto \quad \forall_x^{\text{nc}}(x \in \text{cof} \rightarrow A) \quad (\text{abbreviated } \forall_{x \in \text{cof}}^{\text{nc}} A).$$

- ▶ Computational content of $x \in \text{cof}$ 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
- ▶ $\{-1, 1, \perp\}$ with at most one \perp (“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**:

$$\forall_x A \quad \mapsto \quad \forall_x^{\text{nc}}(x \in \text{coI} \rightarrow A) \quad (\text{abbreviated } \forall_{x \in \text{coI}}^{\text{nc}} A).$$

- ▶ Computational content of $x \in \text{coI}$ 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
- ▶ $\{-1, 1, \perp\}$ with at most one \perp (“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**:

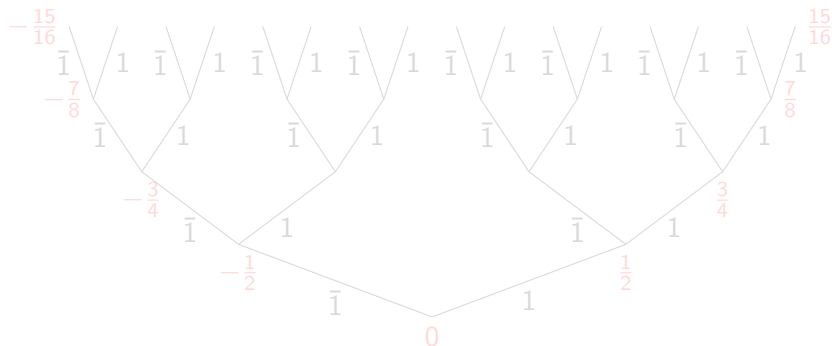
$$\forall_x A \quad \mapsto \quad \forall_x^{\text{nc}}(x \in \text{coI} \rightarrow A) \quad (\text{abbreviated } \forall_{x \in \text{coI}}^{\text{nc}} A).$$

- ▶ Computational content of $x \in \text{coI}$ is a stream representing x .

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

Dyadic rationals:

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



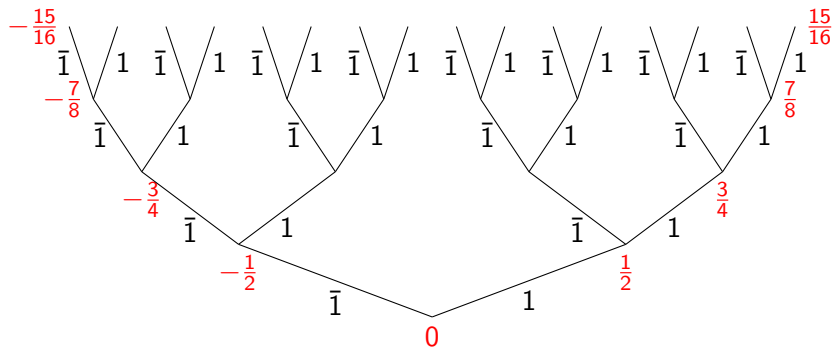
with $\bar{1} := -1$. Adjacent dyadics can differ in many digits:

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

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

Dyadic rationals:

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



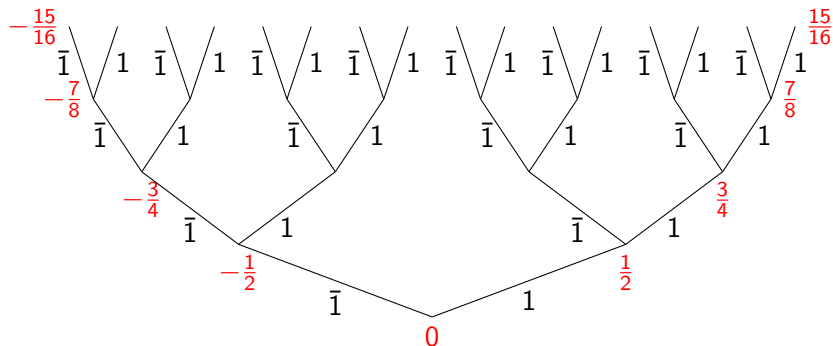
with $\bar{1} := -1$. Adjacent dyadics can differ in many digits:

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

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

Dyadic rationals:

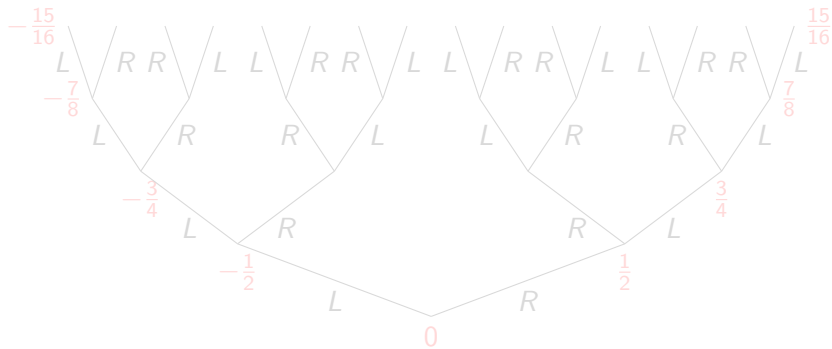
$$\sum_{n < m} \frac{k_n}{2^{n+1}} \quad \text{with } k_n \in \{-1, 1\}.$$



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

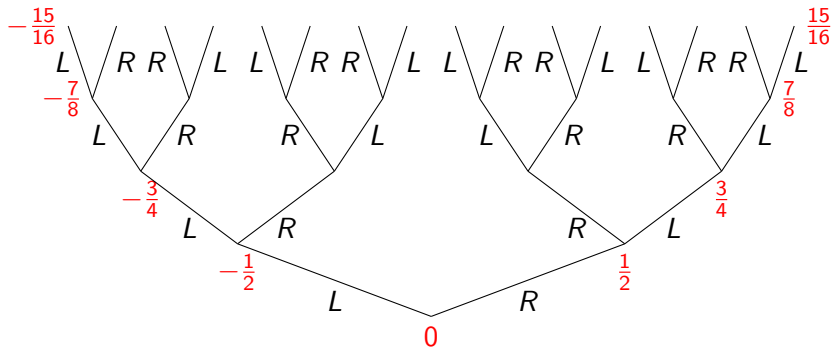
$$\frac{7}{16} \sim 1\bar{1}11, \quad \frac{9}{16} \sim 11\bar{1}\bar{1}.$$

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



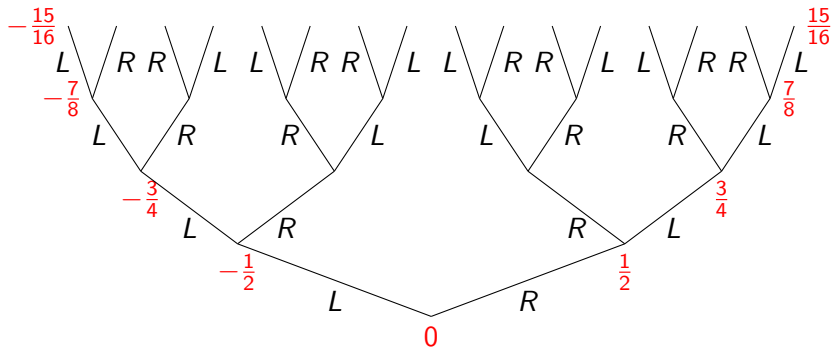
$$\frac{7}{16} \sim \text{RRRL}, \quad \frac{9}{16} \sim \text{RLRL}.$$

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



$$\frac{7}{16} \sim \text{RRRL}, \quad \frac{9}{16} \sim \text{RLRL}.$$

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



$$\frac{7}{16} \sim \text{RRRL}, \quad \frac{9}{16} \sim \text{RLRL}.$$

Problem with productivity:

$$\bar{1}111 + 1\bar{1}\bar{1}\bar{1}\dots = ? \quad (\text{or } \text{LRL}\dots + \text{RRRL}\dots = ?)$$

What is the first digit? Cure: delay.

- ▶ For binary code: add 0. Signed digit code

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

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), Fin_{L/R} (finally left / right). Pre-Gray code.

Problem with productivity:

$$\bar{1}111 + 1\bar{1}\bar{1}\bar{1}\dots = ? \quad (\text{or } LRL\bar{L}\dots + RRRL\dots = ?)$$

What is the first digit? Cure: delay.

- ▶ For binary code: add 0. **Signed digit code**

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

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), Fin_{L/R} (finally left / right). **Pre-Gray code**.

Problem with productivity:

$$\bar{1}111 + 1\bar{1}\bar{1}\bar{1}\dots = ? \quad (\text{or } LRL\bar{L}\dots + RRRL\dots = ?)$$

What is the first digit? Cure: delay.

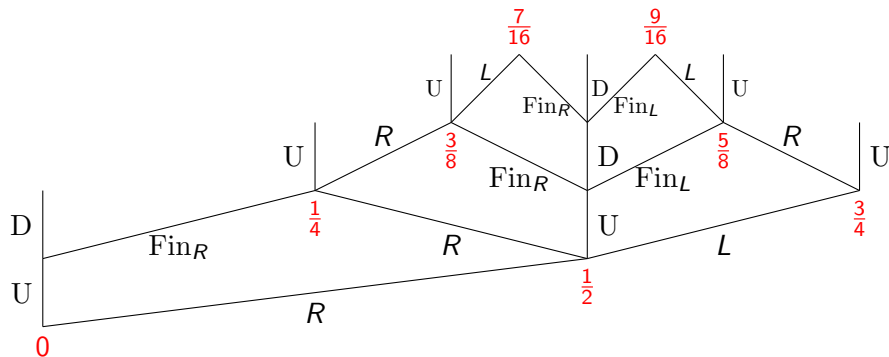
- ▶ For binary code: add 0. **Signed digit code**

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

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), Fin_{L/R} (finally left / right). **Pre-Gray code**.

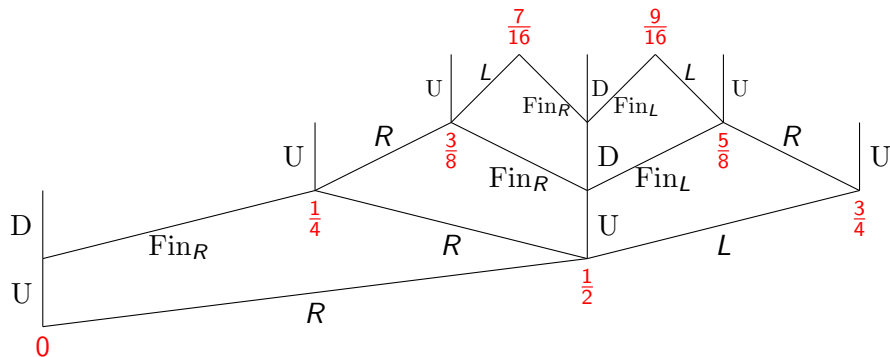
Pre-Gray code



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

$$U \circ \text{Fin}_a \mapsto a \circ R, \quad D \circ \text{Fin}_a \mapsto \text{Fin}_a \circ L.$$

Pre-Gray code



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

$$U \circ \text{Fin}_a \mapsto a \circ R, \quad D \circ \text{Fin}_a \mapsto \text{Fin}_a \circ L.$$

RRRLLL... RLRLLL... RUDDDD...

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**.

RRRLLL... RLRLLL... RUDDDD...

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**.

RRRLLL... RLRLLL... RUDDDD...

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**.

RRRLLL... RLRLLL... RUDDDD...

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**.

RRRLLL... RLRLLL... RUDDDD...

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**.

Average for pre-Gray code

Pre-Gray code: “cototal objects” in the (simultaneously defined) free algebras \mathbf{G} and \mathbf{H} given by the constructors

$$\text{Lr}: \mathbf{B} \rightarrow \mathbf{G} \rightarrow \mathbf{G}$$

$$\text{U}: \mathbf{H} \rightarrow \mathbf{G}$$

$$\text{Fin}: \mathbf{B} \rightarrow \mathbf{G} \rightarrow \mathbf{H}$$

$$\text{D}: \mathbf{H} \rightarrow \mathbf{H}$$

with $\mathbf{B} = \{\text{tt}, \text{ff}\}$

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

Let

$$\Gamma(X, Y) := \left\{ x \mid \exists_{x' \in X}^r \exists_{a \in \text{Psd}}^r \left(x = -a \frac{x' - 1}{2} \right) \vee \exists_{x' \in Y}^r \left(x = \frac{x'}{2} \right) \right\},$$

$$\Delta(X, Y) := \left\{ x \mid \exists_{x' \in X}^r \exists_{a \in \text{Psd}}^r \left(x = a \frac{x' + 1}{2} \right) \vee \exists_{x' \in Y}^r \left(x = \frac{x'}{2} \right) \right\}$$

and define

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

Consequences:

$$\forall_{x \in {}^{\text{co}}G}^{\text{nc}} \left(\exists_{x' \in {}^{\text{co}}G}^r \exists_{a \in \text{Psd}}^r \left(x = -a \frac{x' - 1}{2} \right) \vee \exists_{x' \in {}^{\text{co}}H}^r \left(x = \frac{x'}{2} \right) \right)$$

$$\forall_{x \in {}^{\text{co}}H}^{\text{nc}} \left(\exists_{x' \in {}^{\text{co}}G}^r \exists_{a \in \text{Psd}}^r \left(x = a \frac{x' + 1}{2} \right) \vee \exists_{x' \in {}^{\text{co}}H}^r \left(x = \frac{x'}{2} \right) \right)$$

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

Let

$$\Gamma(X, Y) := \left\{ x \mid \exists_{x' \in X}^r \exists_{a \in \text{Psd}}^r \left(x = -a \frac{x' - 1}{2} \right) \vee \exists_{x' \in Y}^r \left(x = \frac{x'}{2} \right) \right\},$$

$$\Delta(X, Y) := \left\{ x \mid \exists_{x' \in X}^r \exists_{a \in \text{Psd}}^r \left(x = a \frac{x' + 1}{2} \right) \vee \exists_{x' \in Y}^r \left(x = \frac{x'}{2} \right) \right\}$$

and define

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

Consequences:

$$\forall_{x \in {}^{\text{co}}G}^{\text{nc}} \left(\exists_{x' \in {}^{\text{co}}G}^r \exists_{a \in \text{Psd}}^r \left(x = -a \frac{x' - 1}{2} \right) \vee \exists_{x' \in {}^{\text{co}}H}^r \left(x = \frac{x'}{2} \right) \right)$$

$$\forall_{x \in {}^{\text{co}}H}^{\text{nc}} \left(\exists_{x' \in {}^{\text{co}}G}^r \exists_{a \in \text{Psd}}^r \left(x = a \frac{x' + 1}{2} \right) \vee \exists_{x' \in {}^{\text{co}}H}^r \left(x = \frac{x'}{2} \right) \right)$$

Lemma (CoGMinus)

$$\begin{aligned}\forall_x^{\text{nc}}(\text{coG}(-x) \rightarrow \text{coG}x), \\ \forall_x^{\text{nc}}(\text{coH}(-x) \rightarrow \text{coH}x).\end{aligned}$$

Implicit algorithm. $f: \mathbf{G} \rightarrow \mathbf{G}$ and $f': \mathbf{H} \rightarrow \mathbf{H}$ defined by

$$\begin{aligned}f(\text{Lr}_a(u)) &= \text{Lr}_{-a}(u), & f'(\text{Fin}_a(u)) &= \text{Fin}_{-a}(u), \\ f(\text{U}(v)) &= \text{U}(f'(v)), & f'(\text{D}(v)) &= \text{D}(f'(v)).\end{aligned}$$

Lemma (CoGMinus)

$$\begin{aligned}\forall_x^{\text{nc}}(\text{coG}(-x) \rightarrow \text{coG}x), \\ \forall_x^{\text{nc}}(\text{coH}(-x) \rightarrow \text{coH}x).\end{aligned}$$

Implicit algorithm. $f: \mathbf{G} \rightarrow \mathbf{G}$ and $f': \mathbf{H} \rightarrow \mathbf{H}$ defined by

$$\begin{aligned}f(\text{Lr}_a(u)) &= \text{Lr}_{-a}(u), & f'(\text{Fin}_a(u)) &= \text{Fin}_{-a}(u), \\ f(\text{U}(v)) &= \text{U}(f'(v)), & f'(\text{D}(v)) &= \text{D}(f'(v)).\end{aligned}$$

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

Lemma (CoHToCoG)

$$\begin{aligned} & \forall_x^{\text{nc}} (x \in {}^{\text{co}}H \rightarrow x \in {}^{\text{co}}G), \\ & \forall_x^{\text{nc}} (x \in {}^{\text{co}}G \rightarrow x \in {}^{\text{co}}H). \end{aligned}$$

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

$$\begin{aligned} g(\text{Fin}_a(u)) &= \text{Lr}_a(f^-(u)), & h(\text{Lr}_a(u)) &= \text{Fin}_a(f^-(u)), \\ g(\text{D}(v)) &= \text{U}(v), & h(\text{U}(v)) &= \text{D}(v) \end{aligned}$$

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

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

Lemma (CoHToCoG)

$$\begin{aligned} \forall_x^{\text{nc}}(x \in {}^{\text{co}}H \rightarrow x \in {}^{\text{co}}G), \\ \forall_x^{\text{nc}}(x \in {}^{\text{co}}G \rightarrow x \in {}^{\text{co}}H). \end{aligned}$$

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

$$\begin{aligned} g(\text{Fin}_a(u)) &= \text{Lr}_a(f^-(u)), & h(\text{Lr}_a(u)) &= \text{Fin}_a(f^-(u)), \\ g(\text{D}(v)) &= \text{U}(v), & h(\text{U}(v)) &= \text{D}(v) \end{aligned}$$

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

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

Lemma (CoHToCoG)

$$\begin{aligned} \forall_x^{\text{nc}}(x \in {}^{\text{co}}H \rightarrow x \in {}^{\text{co}}G), \\ \forall_x^{\text{nc}}(x \in {}^{\text{co}}G \rightarrow x \in {}^{\text{co}}H). \end{aligned}$$

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

$$\begin{aligned} g(\text{Fin}_a(u)) &= \text{Lr}_a(f^-(u)), & h(\text{Lr}_a(u)) &= \text{Fin}_a(f^-(u)), \\ g(\text{D}(v)) &= \text{U}(v), & h(\text{U}(v)) &= \text{D}(v) \end{aligned}$$

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

Informal proof

To prove

$$\forall_{x,y \in {}^{\text{co}}G}^{\text{nc}} \left(\frac{x+y}{2} \in {}^{\text{co}}G \right)$$

consider two sets of averages, the second one with a “carry”:

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

Suffices: Q satisfies the clause coinductively defining ${}^{\text{co}}G$.

- ▶ By the greatest-fixed-point axiom for ${}^{\text{co}}G$ we have $Q \subseteq {}^{\text{co}}G$.
- ▶ Since also $P \subseteq Q$ we obtain $P \subseteq {}^{\text{co}}G$, which is our claim.

Informal proof

To prove

$$\forall_{x,y \in {}^{\text{co}}G}^{\text{nc}} \left(\frac{x+y}{2} \in {}^{\text{co}}G \right)$$

consider two sets of averages, the second one with a “carry”:

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

Suffices: Q satisfies the clause coinductively defining ${}^{\text{co}}G$.

- ▶ By the greatest-fixed-point axiom for ${}^{\text{co}}G$ we have $Q \subseteq {}^{\text{co}}G$.
- ▶ Since also $P \subseteq Q$ we obtain $P \subseteq {}^{\text{co}}G$, which is our claim.

Informal proof

To prove

$$\forall_{x,y \in {}^{\text{co}}G}^{\text{nc}} \left(\frac{x+y}{2} \in {}^{\text{co}}G \right)$$

consider two sets of averages, the second one with a “carry”:

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

Suffices: Q satisfies the clause coinductively defining ${}^{\text{co}}G$.

- ▶ By the greatest-fixed-point axiom for ${}^{\text{co}}G$ we have $Q \subseteq {}^{\text{co}}G$.
- ▶ Since also $P \subseteq Q$ we obtain $P \subseteq {}^{\text{co}}G$, which is our claim.

Lemma (CoGAvToAvc)

$$\forall_{x,y \in \text{coG}}^{\text{nc}} \exists_{i \in \text{Sd}_2}^{\text{r}} \exists_{x',y' \in \text{coG}}^{\text{r}} \left(\frac{x+y}{2} = \frac{x'+y'+i}{4} \right).$$

Proof needs CoGPsdTimes: $\forall_{a \in \text{Psd}}^{\text{nc}} \forall_{x \in \text{coG}}^{\text{nc}} (ax \in \text{coG})$. Rest easy, using CoGClause.

Implicit algorithm.

Write f^* for cCoGPsdTimes and s for cCoHToCoG.

$$f(\text{Lr}_a(u), \text{Lr}_{a'}(u')) = (a + a', f^*(-a, u), f^*(-a', u')),$$

$$f(\text{Lr}_a(u), \text{U}(v)) = (a, f^*(-a, u), s(v)),$$

$$f(\text{U}(v), \text{Lr}_a(u)) = (a, s(v), f^*(-a, u)),$$

$$f(\text{U}(v), \text{U}(v')) = (0, s(v), s(v')).$$

Lemma (CoGAvToAvc)

$$\forall_{x,y \in \text{coG}}^{\text{nc}} \exists i \in \text{Sd}_2^r \exists_{x',y' \in \text{coG}}^r \left(\frac{x+y}{2} = \frac{x'+y'+i}{4} \right).$$

Proof needs CoGPsdTimes: $\forall_{a \in \text{Psd}}^{\text{nc}} \forall_{x \in \text{coG}}^{\text{nc}} (ax \in \text{coG})$. Rest easy, using CoGClause.

Implicit algorithm.

Write f^* for cCoGPsdTimes and s for cCoHToCoG.

$$f(\text{Lr}_a(u), \text{Lr}_{a'}(u')) = (a + a', f^*(-a, u), f^*(-a', u')),$$

$$f(\text{Lr}_a(u), \text{U}(v)) = (a, f^*(-a, u), s(v)),$$

$$f(\text{U}(v), \text{Lr}_a(u)) = (a, s(v), f^*(-a, u)),$$

$$f(\text{U}(v), \text{U}(v')) = (0, s(v), s(v')).$$

Lemma (CoGAvToAvc)

$$\forall_{x,y \in \text{coG}}^{\text{nc}} \exists i \in \text{Sd}_2^r \exists_{x',y' \in \text{coG}}^r \left(\frac{x+y}{2} = \frac{x'+y'+i}{4} \right).$$

Proof needs CoGPsdTimes: $\forall_{a \in \text{Psd}}^{\text{nc}} \forall_{x \in \text{coG}}^{\text{nc}} (ax \in \text{coG})$. Rest easy, using CoGClause.

Implicit algorithm.

Write f^* for cCoGPsdTimes and s for cCoHToCoG.

$$f(\text{Lr}_a(u), \text{Lr}_{a'}(u')) = (a + a', f^*(-a, u), f^*(-a', u')),$$

$$f(\text{Lr}_a(u), \text{U}(v)) = (a, f^*(-a, u), s(v)),$$

$$f(\text{U}(v), \text{Lr}_a(u)) = (a, s(v), f^*(-a, u)),$$

$$f(\text{U}(v), \text{U}(v')) = (0, s(v), s(v')).$$

Lemma (CoGAvcSatColCI)

$$\forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{x, y \in \text{coG}}^{\text{nc}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{k \in \text{Sd}}^{\text{r}} \exists_{x', y' \in \text{coG}}^{\text{r}} \left(\frac{x + y + i}{4} = \frac{\frac{x' + y' + j}{4} + k}{2} \right).$$

Proof. Define $J, K: \mathbb{Z} \rightarrow \mathbb{Z}$ such that

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

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

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

Implicit algorithm.

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

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

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

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

Lemma (CoGAvcSatColCI)

$$\forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{x, y \in \text{coG}}^{\text{nc}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{k \in \text{Sd}}^{\text{r}} \exists_{x', y' \in \text{coG}}^{\text{r}} \left(\frac{x + y + i}{4} = \frac{\frac{x' + y' + j}{4} + k}{2} \right).$$

Proof. Define $J, K: \mathbb{Z} \rightarrow \mathbb{Z}$ such that

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

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

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

Implicit algorithm.

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

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

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

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

Lemma (CoGAvcSatColCI)

$$\forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{x, y \in \text{coG}}^{\text{nc}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{k \in \text{Sd}}^{\text{r}} \exists_{x', y' \in \text{coG}}^{\text{r}} \left(\frac{x + y + i}{4} = \frac{\frac{x' + y' + j}{4} + k}{2} \right).$$

Proof. Define $J, K: \mathbb{Z} \rightarrow \mathbb{Z}$ such that

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

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

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

Implicit algorithm.

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

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

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

$$f(i, U(v), U(v')) = (J(2i), K(2i), s(v), s(v')).$$

Lemma (CoGAvcToCoG)

$$\forall_z^{\text{nc}} (\exists_{x,y \in \text{coG}}^r \exists_{i \in \text{Sd}_2}^r (z = \frac{x + y + i}{4}) \rightarrow z \in \text{coG}),$$
$$\forall_z^{\text{nc}} (\exists_{x,y \in \text{coG}}^r \exists_{i \in \text{Sd}_2}^r (z = \frac{x + y + i}{4}) \rightarrow z \in \text{coH}).$$

Proof (by coinduction) uses CoGAvcSatColCl. We need a lemma:

$$\text{SdDisj}: \forall_{d \in \text{Sd}}^{\text{nc}} (d = 0 \vee^r \exists_{a \in \text{Psd}}^r (d = a)).$$

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

Lemma (CoGAvcToCoG)

$$\forall_z^{\text{nc}} (\exists_{x,y \in \text{coG}}^r \exists_{i \in \text{Sd}_2}^r (z = \frac{x + y + i}{4}) \rightarrow z \in \text{coG}),$$
$$\forall_z^{\text{nc}} (\exists_{x,y \in \text{coG}}^r \exists_{i \in \text{Sd}_2}^r (z = \frac{x + y + i}{4}) \rightarrow z \in \text{coH}).$$

Proof (by coinduction) uses CoGAvcSatColCl. We need a lemma:

$$\text{SdDisj}: \forall_{d \in \text{Sd}}^{\text{nc}} (d = 0 \vee^r \exists_{a \in \text{Psd}}^r (d = a)).$$

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

Implicit algorithm.

$g(i, u, u') = \text{let } (i_1, k, u_1, u'_1) = \text{cCoGAvcSatCoICl}(i, u, u')$ in
case $\text{cSdDisj}(k)$ of

$$0 \rightarrow U(h(i_1, u_1, u'_1))$$

$$a \rightarrow \text{Lr}_a(g(-ai_1, f^*(-a, u_1), f^*(-a, u'_1))),$$

$h(j, u, u') = \text{let } (i_1, k, u_1, u'_1) = \text{cCoGAvcSatCoICl}(i, u, u')$ in
case $\text{cSdDisj}(k)$ of

$$0 \rightarrow D(h(i_1, u_1, u'_1))$$

$$a \rightarrow \text{Fin}_a(g(-ai_1, f^*(-a, u_1), f^*(-a, u'_1))).$$

Theorem (CoGAverage)

$$\forall_{x,y \in \text{coG}}^{\text{nc}} \left(\frac{x+y}{2} \in \text{coG} \right).$$

Implicit algorithm. Compose cCoGAvToAvc with cCoGAvcToCoG .

Theorem (CoGAverage)

$$\forall_{x,y \in \text{coG}}^{\text{nc}} \left(\frac{x+y}{2} \in \text{coG} \right).$$

Implicit algorithm. Compose cCoGAvToAvc with cCoGAvcToCoG .

Multiplication for pre-Gray code

To prove

$$\forall_{x,x'}^{\text{nc}} (x, x' \in {}^{\text{co}}G \rightarrow x \cdot x' \in {}^{\text{co}}G),$$

consider the two sets

$$P := \{ x \cdot y \mid x, y \in {}^{\text{co}}G \},$$

$$Q := \left\{ \frac{x \cdot y + z + i}{4} \mid x, y, z \in {}^{\text{co}}G, i \in \text{Sd}_2 \right\}.$$

Suffices: Q satisfies the clause coinductively defining ${}^{\text{co}}G$.

- ▶ By the greatest-fixed-point axiom for ${}^{\text{co}}G$ we have $Q \subseteq {}^{\text{co}}G$.
- ▶ Since also $P \subseteq Q$ we obtain $P \subseteq {}^{\text{co}}G$, which is our claim.

Multiplication for pre-Gray code

To prove

$$\forall_{x,x'}^{\text{nc}}(x, x' \in {}^{\text{co}}G \rightarrow x \cdot x' \in {}^{\text{co}}G),$$

consider the two sets

$$P := \{x \cdot y \mid x, y \in {}^{\text{co}}G\},$$

$$Q := \left\{ \frac{x \cdot y + z + i}{4} \mid x, y, z \in {}^{\text{co}}G, i \in \text{Sd}_2 \right\}.$$

Suffices: Q satisfies the clause coinductively defining ${}^{\text{co}}G$.

- ▶ By the greatest-fixed-point axiom for ${}^{\text{co}}G$ we have $Q \subseteq {}^{\text{co}}G$.
- ▶ Since also $P \subseteq Q$ we obtain $P \subseteq {}^{\text{co}}G$, which is our claim.

Lemma (CoGMultToMultc)

$$\forall_{x,y \in {}^{\text{co}}G}^{\text{nc}} \exists_{i \in \text{Sd}_2}^r \exists_{x',y',z \in {}^{\text{co}}G}^r (xy = \frac{x'y' + z + i}{4}).$$

Proof. Case

$$x = -a \frac{x' - 1}{2} \quad y = -b \frac{y' - 1}{2} \quad \text{with } x', y' \in {}^{\text{co}}G \text{ and } a, b \in \text{Psd.}$$

By CoGAverage $\frac{-abx' - aby'}{2} =: z \in {}^{\text{co}}G$. Subcase Lrz. Then

$$z = -c \frac{z' - 1}{2} \quad \text{with } z' \in {}^{\text{co}}G \text{ and } c \in \text{Psd.}$$

Hence

$$\begin{aligned} xy &= \frac{(ax' - a)(by' - b)}{4} = \frac{ax'by' - ab(x' + y') + ab}{4} \\ &= \frac{ax'by' - cz' + (c + ab)}{4}, \end{aligned}$$

which is of the required form.

Lemma (CoGMultToMultc)

$$\forall_{x,y \in {}^{\text{co}}G}^{\text{nc}} \exists_{i \in \text{Sd}_2}^r \exists_{x',y',z \in {}^{\text{co}}G}^r (xy = \frac{x'y' + z + i}{4}).$$

Proof. Case

$$x = -a \frac{x' - 1}{2} \quad y = -b \frac{y' - 1}{2} \quad \text{with } x', y' \in {}^{\text{co}}G \text{ and } a, b \in \text{Psd.}$$

By CoGAverage $\frac{-abx' - aby'}{2} =: z \in {}^{\text{co}}G$. Subcase Lrz. Then

$$z = -c \frac{z' - 1}{2} \quad \text{with } z' \in {}^{\text{co}}G \text{ and } c \in \text{Psd.}$$

Hence

$$\begin{aligned} xy &= \frac{(ax' - a)(by' - b)}{4} = \frac{ax'by' - ab(x' + y') + ab}{4} \\ &= \frac{ax'by' - cz' + (c + ab)}{4}, \end{aligned}$$

which is of the required form.

Lemma (CoGMultToMultc)

$$\forall_{x,y \in \text{coG}}^{\text{nc}} \exists_{i \in \text{Sd}_2}^{\text{r}} \exists_{x',y',z \in \text{coG}}^{\text{r}} (xy = \frac{x'y' + z + i}{4}).$$

Implicit algorithm. We use s for cCoHToCoG , and au for $f^*(a, u)$.

$$\begin{aligned} g(\text{Lr}_a(u), \text{Lr}_b(u')) &= \text{case cCoGAverage}(-abu, -abu') \text{ of} \\ &\quad \text{Lr}_c(u'') \rightarrow (c + ab, au, bu', -cu'') \\ &\quad \text{U}(v) \rightarrow (ab, au, bu', s(v)) \end{aligned}$$

$$g(\text{Lr}_a(u), \text{U}(v)) = (0, -au, s(v), as(v))$$

$$g(\text{U}(v), \text{Lr}_a(u)) = (0, s(v), -au, as(v))$$

$$g(\text{U}(v), \text{U}(v')) = (0, s(v), s(v'), \text{cCoGZero}).$$

Lemma (CoGMultcSatColCI)

$$\forall_{y \in {}^{\text{co}}G}^{\text{nc}} \forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{x, z \in {}^{\text{co}}G} \exists_{d \in \text{Sd}}^r \exists_{j \in \text{Sd}_2}^r \exists_{x', z' \in {}^{\text{co}}G}^r \left(\frac{xy + z + i}{4} = \frac{\frac{x'y + z' + j}{4} + d}{2} \right).$$

Proof. Case

$$x = -a_1 \frac{x_1 - 1}{2} \quad z = -a_0 \frac{z_1 - 1}{2} \quad \text{with } x_1, z_1 \in {}^{\text{co}}G, a_1, a_0 \in \text{Psd}.$$

Then

$$\begin{aligned} \frac{xy + z + i}{4} &= \frac{(-a_1 x_1 + a_1)y - a_0 z_1 + a_0 + 2i}{8} \\ &= \frac{-a_1 x_1 y + (a_1 y - a_0 z_1 + i) + a_0 + i}{8}. \end{aligned}$$

By CoGAvcToCoG $\frac{a_1 y - a_0 z_1 + i}{4} =: v \in {}^{\text{co}}G$. Hence we can continue

$$= \frac{-a_1 x_1 y + 4v + a_0 + i}{8} = \frac{\frac{-a_1 x_1 y}{4} + v + \frac{a_0 + i}{4}}{2} = \frac{\frac{-a_1 x_1 y + z + j}{4} + d}{2}$$

with $z \in {}^{\text{co}}G, j \in \text{Sd}_2$ and $d \in \text{Sd}$, by Lemma JKLr (below).

Lemma (CoGMultcSatColCI)

$$\forall_{y \in {}^{\text{co}}G}^{\text{nc}} \forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{x, z \in {}^{\text{co}}G}^{\text{nc}} \exists_{d \in \text{Sd}}^r \exists_{j \in \text{Sd}_2}^r \exists_{x', z' \in {}^{\text{co}}G}^r \left(\frac{xy + z + i}{4} = \frac{\frac{x'y + z' + j}{4} + d}{2} \right).$$

Proof. Case

$$x = -a_1 \frac{x_1 - 1}{2} \quad z = -a_0 \frac{z_1 - 1}{2} \quad \text{with } x_1, z_1 \in {}^{\text{co}}G, a_1, a_0 \in \text{PsD}.$$

Then

$$\begin{aligned} \frac{xy + z + i}{4} &= \frac{(-a_1 x_1 + a_1)y - a_0 z_1 + a_0 + 2i}{8} \\ &= \frac{-a_1 x_1 y + (a_1 y - a_0 z_1 + i) + a_0 + i}{8}. \end{aligned}$$

By CoGAvcToCoG $\frac{a_1 y - a_0 z_1 + i}{4} =: v \in {}^{\text{co}}G$. Hence we can continue

$$= \frac{-a_1 x_1 y + 4v + a_0 + i}{8} = \frac{-a_1 x_1 y}{4} + v + \frac{a_0 + i}{4} = \frac{-a_1 x_1 y + z + j}{4} + d$$

with $z \in {}^{\text{co}}G$, $j \in \text{Sd}_2$ and $d \in \text{Sd}$, by Lemma JKLr (below).

Lemma (CoGMultcSatCoICI)

$$\forall_{y \in \text{coG}}^{\text{nc}} \forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{x, z \in \text{coG}}^{\text{nc}} \exists_{d \in \text{Sd}}^{\text{r}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{x', z' \in \text{coG}}^{\text{r}} \left(\frac{xy + z + i}{4} = \frac{\frac{x'y + z' + j}{4} + d}{2} \right).$$

Implicit algorithm. We use h for cCoGAvcToCoG , w_0 for cCoGZero

$$g(u_0, i, \text{Lr}_a(u), \text{Lr}_b(u')) =$$

$$\text{let } (j, d, w) = \text{cJKLr}(i, b, h(i, au_0, -bu')) \text{ in } (d, j, -au, w)$$

$$g(u_0, i, \text{Lr}_a(u), \text{U}(v)) =$$

$$\text{let } (j, d, w) = \text{cJKU}(i, h(i, au_0, s(v))) \text{ in } (d, j, -au, w)$$

$$g(u_0, i, \text{U}(v), \text{Lr}_a(u)) =$$

$$\text{let } (j, d, w) = \text{cJKLr}(i, a, h(i, w_0, -au)) \text{ in } (d, j, s(v), w)$$

$$g(u_0, i, \text{U}(v), \text{U}(v')) =$$

$$\text{let } (j, d, w) = \text{cJKU}(i, h(i, w_0, s(v'))) \text{ in } (d, j, s(v), w)$$

Lemma (JKLr)

$$\forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{a \in \text{Psd}}^{\text{nc}} \forall_{v \in {}^{\text{co}}G}^{\text{nc}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{d \in \text{Sd}}^{\text{r}} \exists_{z \in {}^{\text{co}}G}^{\text{r}} (v + \frac{a+i}{4} = \frac{z+j}{4} + d).$$

Proof. Case $v = -b_0 \frac{w-1}{2}$ with $w \in {}^{\text{co}}G$ and $b_0 \in \text{Psd}$. Subcase

$$v = -b_0 \frac{w-1}{2} = -b_0 \frac{-b \frac{z-1}{2} - 1}{2} \quad \text{with } w, z \in {}^{\text{co}}G, b_0, b \in \text{Psd}.$$

Then

$$\begin{aligned} v + \frac{a+i}{4} &= \frac{b_0 b z - b_0 b + 2b_0 + a + i}{4} \\ &= \frac{b_0 b z + j + 4d}{4} \\ &= \frac{b_0 b z + j}{4} + d \end{aligned}$$

with

$$\begin{aligned} j &:= J(-b_0 b + 2b_0 + a + i), \\ d &:= K(-b_0 b + 2b_0 + a + i). \end{aligned}$$

Lemma (JKLr)

$$\forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{a \in \text{Psd}}^{\text{nc}} \forall_{v \in {}^{\text{co}}G}^{\text{nc}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{d \in \text{Sd}}^{\text{r}} \exists_{z \in {}^{\text{co}}G}^{\text{r}} (v + \frac{a+i}{4} = \frac{z+j}{4} + d).$$

Proof. Case $v = -b_0 \frac{w-1}{2}$ with $w \in {}^{\text{co}}G$ and $b_0 \in \text{Psd}$. Subcase

$$v = -b_0 \frac{w-1}{2} = -b_0 \frac{-b \frac{z-1}{2} - 1}{2} \quad \text{with } w, z \in {}^{\text{co}}G, b_0, b \in \text{Psd}.$$

Then

$$\begin{aligned} v + \frac{a+i}{4} &= \frac{b_0 b z - b_0 b + 2b_0 + a + i}{4} \\ &= \frac{b_0 b z + j + 4d}{4} \\ &= \frac{b_0 b z + j}{4} + d \end{aligned}$$

with

$$\begin{aligned} j &:= J(-b_0 b + 2b_0 + a + i), \\ d &:= K(-b_0 b + 2b_0 + a + i). \end{aligned}$$

Lemma (JKLr)

$$\forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{a \in \text{Psd}}^{\text{nc}} \forall_{v \in \text{coG}}^{\text{nc}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{d \in \text{Sd}}^{\text{r}} \exists_{z \in \text{coG}}^{\text{r}} (v + \frac{a+i}{4} = \frac{z+j}{4} + d).$$

Implicit algorithm We use s for cCoHToCoG .

$$g(i, a, \text{Lr}_{b_0}(\text{Lr}_b(w))) = (J(-b_0b+2b_0+a+i), K(-b_0b+2b_0+a+i), b_0bw)$$

$$g(i, a, \text{Lr}_{b_0}(U(w))) = (J(2b_0 + a + i), K(2b_0 + a + i), -b_0s(w))$$

$$g(i, a, U(\text{Lr}_b(w))) = (J(b + a + i), K(b + a + i), bw)$$

$$g(i, a, U(U(w))) = (J(a + i), K(a + i), s(w))$$

Lemma (JKU)

$$\forall_{i \in \text{Sd}_2}^{\text{nc}} \forall_{v \in \text{coG}}^{\text{nc}} \exists_{j \in \text{Sd}_2}^{\text{r}} \exists_{d \in \text{Sd}}^{\text{r}} \exists_{z \in \text{coG}}^{\text{r}} (v + \frac{i}{4} = \frac{z+j}{4} + d)$$

Lemma (CoGMultcToCoG)

$$\forall_{z_0}^{\text{nc}} (\exists_{i \in \text{Sd}_2}^{\text{r}} \exists_{x,y,z \in \text{coG}}^{\text{r}} (z_0 = \frac{xy + z + i}{4}) \rightarrow z_0 \in {}^{\text{co}}\mathbf{G}),$$

$$\forall_{z_0}^{\text{nc}} (\exists_{i \in \text{Sd}_2}^{\text{r}} \exists_{x,y,z \in \text{coG}}^{\text{r}} (z_0 = \frac{xy + z + i}{4}) \rightarrow z_0 \in {}^{\text{co}}\mathbf{H}).$$

Proof (by coinduction) uses CoGMultcSatCoCI. We need SdDisj.

Lemma (CoGMultcToCoG)

$$\forall_{z_0}^{\text{nc}} (\exists_{i \in \text{Sd}_2}^{\text{r}} \exists_{x,y,z \in \text{coG}}^{\text{r}} (z_0 = \frac{xy + z + i}{4}) \rightarrow z_0 \in {}^{\text{co}}\mathbf{G}),$$

$$\forall_{z_0}^{\text{nc}} (\exists_{i \in \text{Sd}_2}^{\text{r}} \exists_{x,y,z \in \text{coG}}^{\text{r}} (z_0 = \frac{xy + z + i}{4}) \rightarrow z_0 \in {}^{\text{co}}\mathbf{H}).$$

Proof (by coinduction) uses CoGMultcSatCoI. We need SdDisj.

Implicit algorithm.

$g(i, u, u', u'') = \text{let } (d, j, u_1, u'_1) = \text{cCoGMultcSatCoICl}(u', i, u, u'')$ in
case $\text{cSdDisj}(d)$ of

$$0 \rightarrow U(h(j, u_1, u', u'_1))$$

$$a \rightarrow \text{Lr}_a(g(-aj, u_1, f^*(-a, u'), f^*(-a, u'_1))),$$

$h(i, u, u', u'') = \text{let } (d, j, u_1, u'_1) = \text{cCoGMultcSatCoICl}(u', i, u, u'')$ in
case $\text{cSdDisj}(d)$ of

$$0 \rightarrow D(h(j, u_1, u', u'_1))$$

$$a \rightarrow \text{Fin}_a(g(aj, u_1, f^*(a, u'), f^*(a, u'_1))).$$

```

[iggg](CoRec sdtwo yprod ag yprod ag yprod ag=>ag
      sdtwo yprod ag yprod ag yprod ag=>ah)iggg
([iggg0][let djgg (cCoGMultcSatCoICl
                  clft crht crht iggg0 clft iggg0
                  clft crht iggg0 crht crht crht iggg0)
[case (cSdDisj clft djgg)
  (DummyL -> InR(InR(clft crht djgg pair
                    clft crht crht djgg pair
                    clft crht crht iggg0 pair
                    crht crht crht djgg)))
  (Inr boole -> InL(boole pair
                    InR(cIntTimesSdtwoPsdToSdtwo
                        clft crht djgg(cPsdUMinus boole)pair
                        clft crht crht djgg pair
                        cCoGPsdTimes clft crht crht iggg0
                                      (cPsdUMinus boole)pair
                        cCoGPsdTimes crht crht crht djgg
                                      (cPsdUMinus boole))))))]
([iggg0][let djgg ...])

```

Theorem (CoGMult)

$$\forall_{x,y \in \text{coG}}^{\text{nc}} (xy \in \text{coG}).$$

Implicit algorithm.

Compose `cCoGMultToMultc` with `cCoGMultcToCoG`.

Theorem (CoGMult)

$$\forall_{x,y \in \text{co}G}^{\text{nc}} (xy \in \text{co}G).$$

Implicit algorithm.

Compose `cCoGMultToMultc` with `cCoGMultcToCoG`.

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^{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 $et(M)$ of the proof M .
- ▶ Verification by (automatically generated) formal soundness proof of the realizability interpretation.