Logic for exact real arithmetic

Helmut Schwichtenberg

Mathematisches Institut, LMU, München

Oberwolfach, November 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
- $\{-1, 1, \bot\}$ with at most one $\bot$ ("undefined"): Gray code.

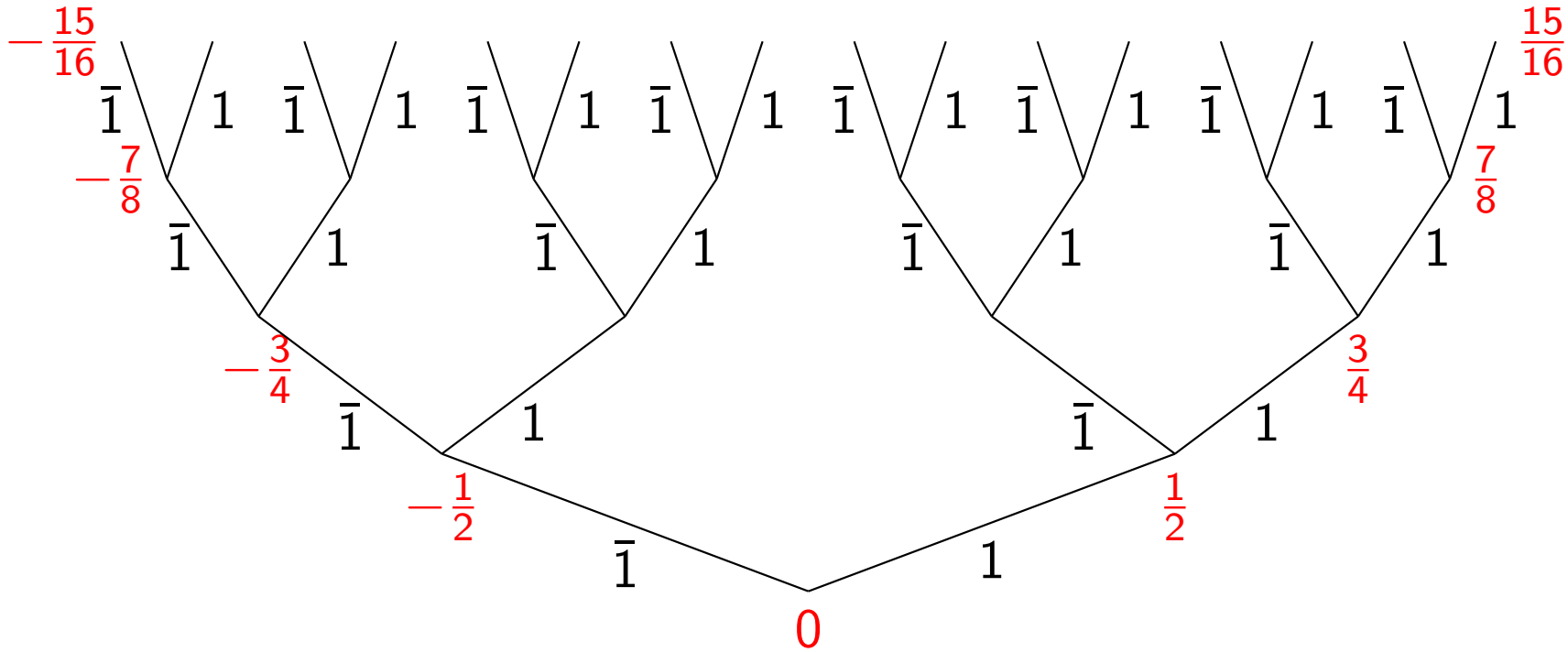
Want formally verified algorithms on reals given as streams.

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

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

Dyadic rationals:

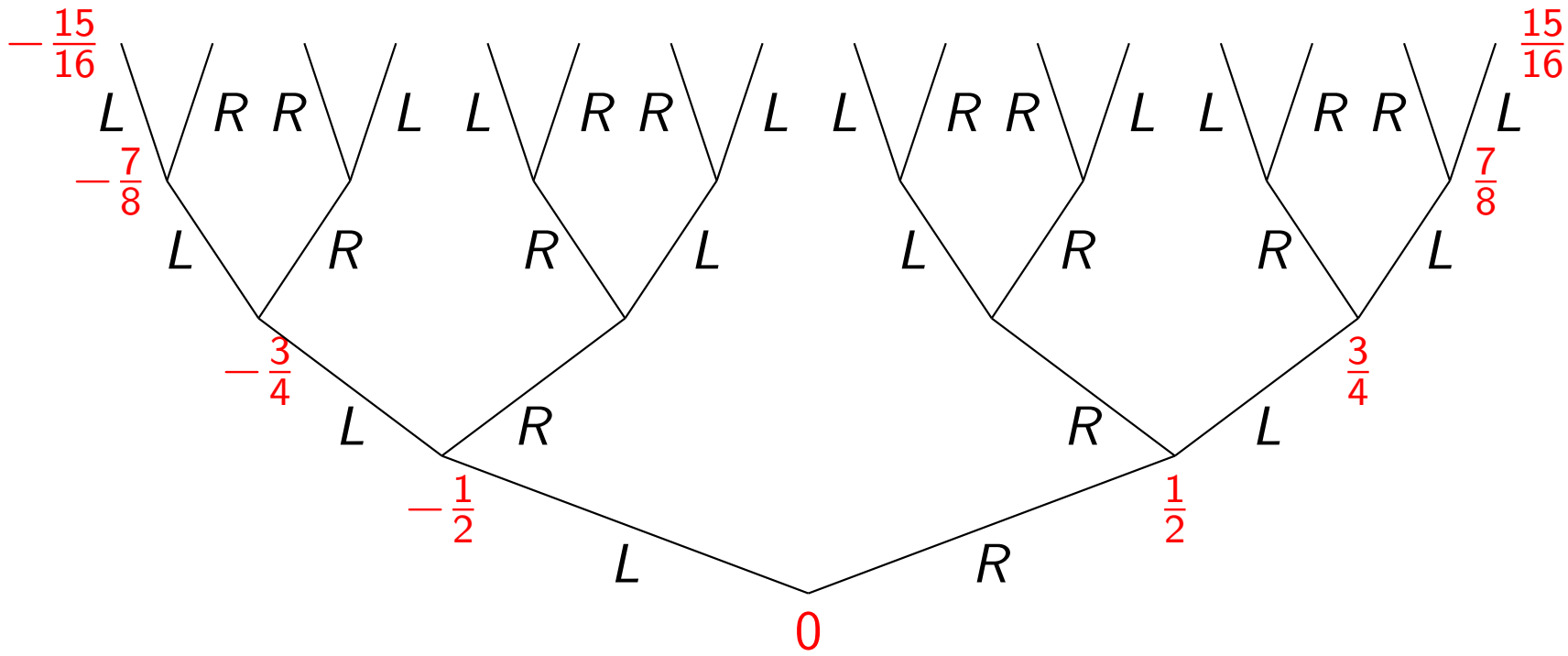
$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 1\}.$$



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

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

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:

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

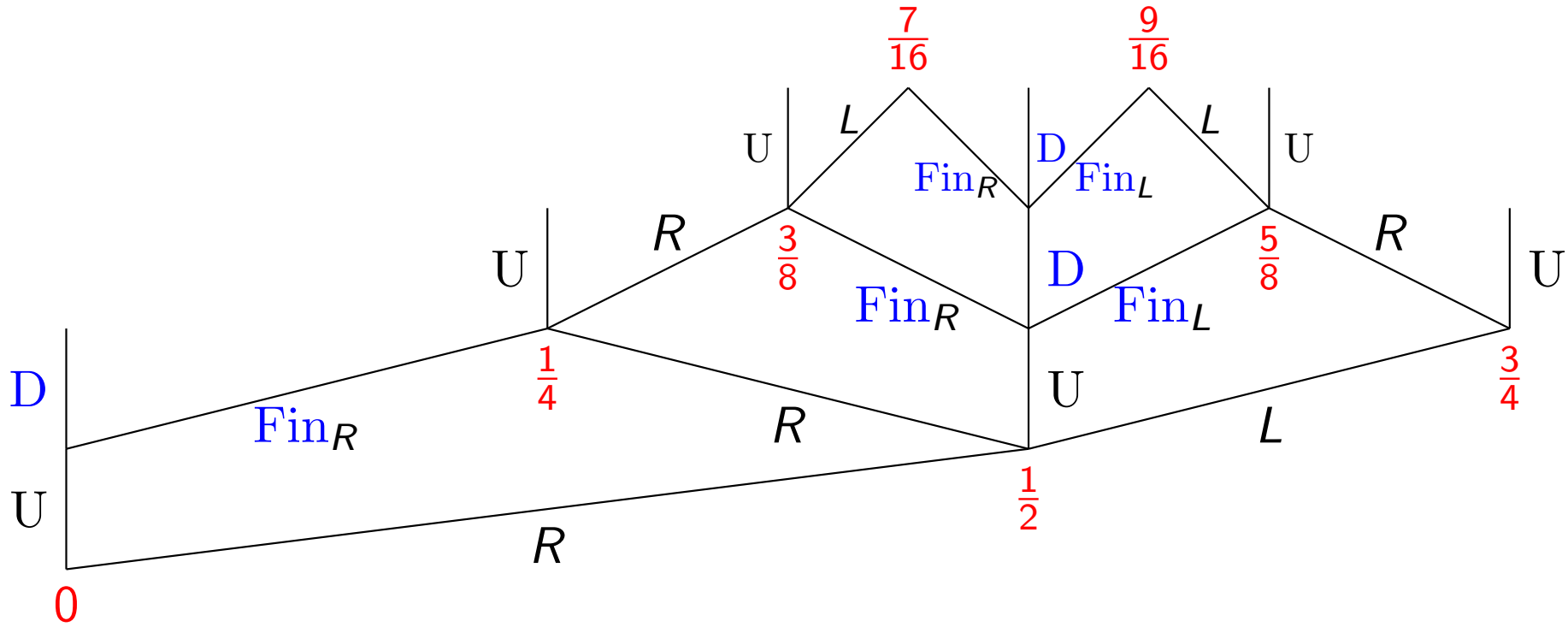
What is the first digit? Cure: delay.

- 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



Can remove Fin_a (by $\mathrm{U} \circ \mathrm{Fin}_a \mapsto a \circ \mathrm{R}$, $\mathrm{D} \circ \mathrm{Fin}_a \mapsto \mathrm{Fin}_a \circ \mathrm{L}$)

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

all denote $\frac{1}{2}$. Only keep the latter to denote $\frac{1}{2}$.
Result: unique representation, called pure Gray code.

Average for pre-Gray code

Pre-Gray code: "cototal objects" in the (simultaneously defined) free algebras **G** and **H** given by the constructors

$$\mathrm{Lr} : \mathbf{B} \to \mathbf{G} \to \mathbf{G}$$
$$\mathrm{U} : \mathbf{H} \to \mathbf{G}$$

$$\mathrm{Fin} : \mathbf{B} \to \mathbf{G} \to \mathbf{H}$$
$$\mathrm{D} : \mathbf{H} \to \mathbf{H}$$

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

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 (CoGUMinus)

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

Proof by coinduction (:= Gfp-axiom), using properties of the unary minus functions.

Implicit algorithm. $f : \mathbf{G} \to \mathbf{G}$ and $f' : \mathbf{H} \to \mathbf{H}$ 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 CoGUMinus we prove that ${}^{\mathrm{co}}G$ and ${}^{\mathrm{co}}H$ are equivalent.

Lemma (CoHToCoG)

$$\forall_x^{\mathrm{nc}}(x \in {}^{\mathrm{co}}H \to x \in {}^{\mathrm{co}}G),$$
$$\forall_x^{\mathrm{nc}}(x \in {}^{\mathrm{co}}G \to x \in {}^{\mathrm{co}}H).$$

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

Informal proof

U. Berger and M. Seisenberger 2010. To prove

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

consider 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 ${}^{\mathrm{co}}G$.

- 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)

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

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)

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

Proof. Define $J, K : \mathbb{Z} \to \mathbb{Z}$ 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 $\frac{x+d}{2}$ 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.

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

Lemma (CoGAvcToCoG)

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

Proof (by coinduction) uses CoGAvcSatCoICl. 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.

$$g(i,u,u') = \text{let } (i_1,k,u_1,u_1') = \text{cCoGAvcSatCoICl}(i,u,u') \text{ in}$$
$$\text{case cSdDisj}(k) \text{ of}$$
$$0 \to \text{U}(h(i_1,u_1,u_1'))$$
$$a \to \text{Lr}_a(g(-ai_1, f^*(-a,u_1), f^*(-a,u_1'))),$$

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

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.

Multiplication for pre-Gray code

To prove

$$\forall^{\mathrm{nc}}_{x,x'}(x, x' \in {}^{\mathrm{co}}G \to x \cdot x' \in {}^{\mathrm{co}}G),$$

consider the two sets

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

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

- 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 (CoGMultToMultc)

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

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

$$\begin{aligned}
g(\mathrm{Lr}_a(u),\mathrm{Lr}_b(u')) &= \mathrm{case}\ \mathrm{cCoGAverage}(-abu,-abu')\ \mathrm{of}\\
&\qquad \mathrm{Lr}_c(u'')\to(c+ab,au,bu',-cu'')\\
&\qquad \mathrm{U}(v)\to(ab,au,bu',s(v))\\
g(\mathrm{Lr}_a(u),\mathrm{U}(v)) &= (0,-au,s(v),as(v))\\
g(\mathrm{U}(v),\mathrm{Lr}_a(u)) &= (0,s(v),-au,as(v))\\
g(\mathrm{U}(v),\mathrm{U}(v')) &= (0,s(v),s(v'),\mathrm{cCoGZero}).
\end{aligned}$$

Lemma (JKLr)

$$\forall^{\mathrm{nc}}_{i\in \mathrm{Sd}_2}\forall^{\mathrm{nc}}_{a\in \mathrm{Psd}}\forall^{\mathrm{nc}}_{v\in {}^{\mathrm{co}}G}\exists^{\mathrm{r}}_{j\in \mathrm{Sd}_2}\exists^{\mathrm{r}}_{d\in \mathrm{Sd}}\exists^{\mathrm{r}}_{z\in {}^{\mathrm{co}}G}(v+\frac{a+i}{4}=\frac{z+j}{4}+d).$$

Implicit algorithm We use s for cCoHToCoG.

$$\begin{aligned}
g(i,a,\mathrm{Lr}_{b_0}(\mathrm{Lr}_b(w))) &= (J(-b_0b+2b_0+a+i),K(-b_0b+2b_0+a+i),b_0bw)\\
g(i,a,\mathrm{Lr}_{b_0}(\mathrm{U}(w))) &= (J(2b_0+a+i),K(2b_0+a+i),-b_0s(w))\\
g(i,a,\mathrm{U}(\mathrm{Lr}_b(w))) &= (J(b+a+i),K(b+a+i),bw)\\
g(i,a,\mathrm{U}(\mathrm{U}(w))) &= (J(a+i),K(a+i),s(w))
\end{aligned}$$

Lemma (JKU)

$$\forall^{\mathrm{nc}}_{i\in \mathrm{Sd}_2}\forall^{\mathrm{nc}}_{v\in {}^{\mathrm{co}}G}\exists^{\mathrm{r}}_{j\in \mathrm{Sd}_2}\exists^{\mathrm{r}}_{d\in \mathrm{Sd}}\exists^{\mathrm{r}}_{z\in {}^{\mathrm{co}}G}(v+\frac{i}{4}=\frac{z+j}{4}+d)$$

Lemma (CoGMultcSatCoICl)

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

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

$$\begin{aligned}
&g(u_0,i,\mathrm{Lr}_a(u),\mathrm{Lr}_b(u')) = \\
&\quad \text{let } (j,d,w)=\mathrm{cJKLr}(i,b,h(i,au_0,-bu')) \text{ in } (d,j,-au,w)\\
&g(u_0,i,\mathrm{Lr}_a(u),\mathrm{U}(v)) = \\
&\quad \text{let } (j,d,w)=\mathrm{cJKU}(i,h(i,au_0,s(v))) \text{ in } (d,j,-au,w)\\
&g(u_0,i,\mathrm{U}(v),\mathrm{Lr}_a(u)) = \\
&\quad \text{let } (j,d,w)=\mathrm{cJKLr}(i,a,h(i,w_0,-au)) \text{ in } (d,j,s(v),w)\\
&g(u_0,i,\mathrm{U}(v),\mathrm{U}(v')) = \\
&\quad \text{let } (j,d,w)=\mathrm{cJKU}(i,h(i,w_0,s(v'))) \text{ in } (d,j,s(v),w)
\end{aligned}$$

Lemma (CoGMultcToCoG)

$$\forall^{\mathrm{nc}}_{z_0}(\exists^{\mathrm{r}}_{i\in \mathrm{Sd}_2}\exists^{\mathrm{r}}_{x,y,z\in {}^{\mathrm{co}}G}(z_0 = \frac{xy+z+i}{4}) \to z_0 \in {}^{\mathrm{co}}G),$$

$$\forall^{\mathrm{nc}}_{z_0}(\exists^{\mathrm{r}}_{i\in \mathrm{Sd}_2}\exists^{\mathrm{r}}_{x,y,z\in {}^{\mathrm{co}}G}(z_0 = \frac{xy+z+i}{4}) \to z_0 \in {}^{\mathrm{co}}H).$$

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

Implicit algorithm.

$$g(i,u,u',u'') = \text{let } (d,j,u_1,u_1') = \text{cCoGMultcSatCoICl}(u',i,u,u'') \text{ in}$$
$$\text{case cSdDisj}(d) \text{ of}$$
$$0 \to \text{U}(h(j,u_1,u',u_1'))$$
$$a \to \text{Lr}_a(g(-aj,u_1,f^*(-a,u'),f^*(-a,u_1'))),$$

$$h(i,u,u',u'') = \text{let } (d,j,u_1,u_1') = \text{cCoGMultcSatCoICl}(u',i,u,u'') \text{ in}$$
$$\text{case cSdDisj}(d) \text{ of}$$
$$0 \to \text{D}(h(j,u_1,u',u_1'))$$
$$a \to \text{Fin}_a(g(aj,u_1,f^*(a,u'),f^*(a,u_1'))).$$

```
[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)

$$\forall^{\mathrm{nc}}_{x,y\in{}^{\mathrm{co}}G}(xy \in {}^{\mathrm{co}}G).$$

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 $\forall_x^{\mathrm{nc}}$ 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.