Logic for real number computation

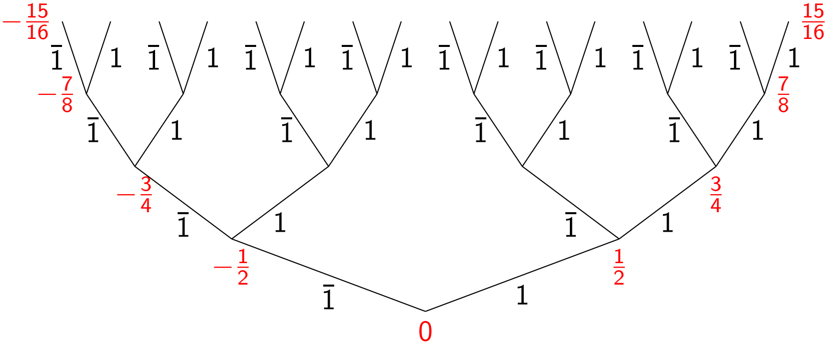
Helmut Schwichtenberg
(j.w.w. Ulrich Berger, Kenji Miyamoto and Hideki Tsuiki)

Mathematisches Institut, LMU, München

Trends in Proof Theory, Hamburg, 20. - 21. September 2015

Dyadic rationals:

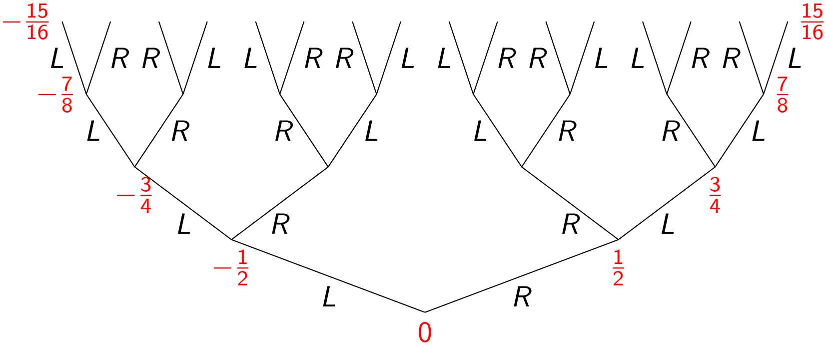
$$\sum_{i<k} \frac{a_i}{2^{i+1}}. \qquad \text{with } a_i \in \{-1, 1\} =: \textbf{PSD}.$$



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:

$$\bar{1}111 + 1\bar{1}\bar{1}\bar{1} = ? \qquad \text{(what is the first digit?)}$$

Cure: delay.

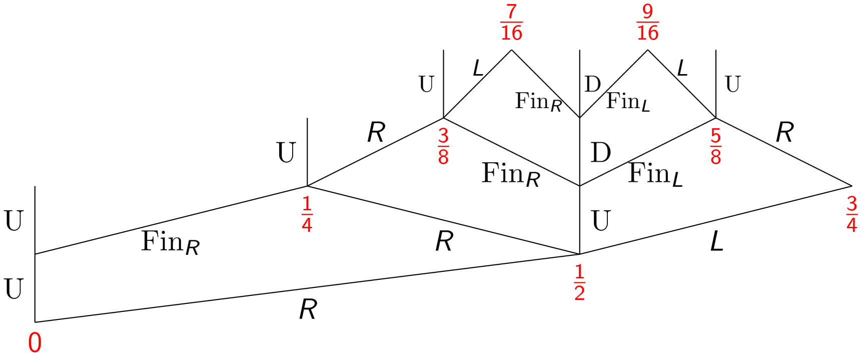
- For binary code: add 0. Signed digit code

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

  Widely used for real number computation.

- For Gray-code: add U, D, $\mathrm{Fin}_{L/R}$. Pre-Gray code.

Pre-Gray code



After computation in pre-Gray code, one can remove Fin_a up to $\frac{1}{2^k}$:

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

Goal: extract algorithms on infinite objects from proofs, in a simple framework (TCF). Example:

- Infinite objects: streams, in pre-Gray code.
- Algorithm: average.

Framework:

- Constructive logic
- Types: only function types (Scott/Ershov partial continuous functionals), over base types given by constructors (may contain infinite objects).
- Inductive & coinductive predicates, with their least & greatest fixed point axioms (i.e., induction & coinduction).

We will coinductively define a predicate ${}^{\mathrm{co}}G$ and prove

$$\forall^{\mathrm{nc}}_{x,x'}({}^{\mathrm{co}}G(x) \to {}^{\mathrm{co}}G(x') \to {}^{\mathrm{co}}G(\frac{x+x'}{2})) \tag{1}$$

($\forall^{\mathrm{nc}}_{x,x'}$: the reals x, x' have no computational significance).
Associated with ${}^{\mathrm{co}}G$ is its realizability extension $({}^{\mathrm{co}}G)^{\mathbf{r}}(p, x)$ (p is a stream representation of x witnessing ${}^{\mathrm{co}}G(x)$).

Soundness theorem:

$$({}^{\mathrm{co}}G)^{\mathbf{r}}(p, x) \to ({}^{\mathrm{co}}G)^{\mathbf{r}}(p', x') \to ({}^{\mathrm{co}}G)^{\mathbf{r}}(f(p, p'), \frac{x+x'}{2})$$

for some stream transformer f extracted from the proof of (1), which never mentions streams.

What is ${}^{\mathrm{co}}G$? Need simultaneously ${}^{\mathrm{co}}H$.

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

($\exists^{\mathrm{r}}_x$: the real x has no computational significance)
Define $({}^{\mathrm{co}}G, {}^{\mathrm{co}}H) := \nu_{(X,Y)}(\Gamma(X,Y), \Delta(X,Y))$.
Coinduction:

$$(X,Y) \subseteq (\Gamma({}^{\mathrm{co}}G \cup X, {}^{\mathrm{co}}H \cup Y), \Delta({}^{\mathrm{co}}G \cup X, {}^{\mathrm{co}}H \cup Y)) \to (X,Y) \subseteq ({}^{\mathrm{co}}G, {}^{\mathrm{co}}H).$$

Associated to Γ, Δ are algebras $\mathbf{G}, \mathbf{H}$ with constructors

$$\begin{aligned} \mathrm{LR}&\colon \mathbf{PSD} \to \mathbf{G} \to \mathbf{G}, \\ \mathrm{U}&\colon \mathbf{H} \to \mathbf{G} \qquad \text{(for "undefined")}, \\ \mathrm{Fin}&\colon \mathbf{PSD} \to \mathbf{G} \to \mathbf{H}, \\ \mathrm{D}&\colon \mathbf{H} \to \mathbf{H} \qquad \text{(for "delay")}. \end{aligned}$$

Realizability extensions $({}^{\mathrm{co}}G)^{\mathbf{r}}$ and $({}^{\mathrm{co}}H)^{\mathbf{r}}$:

$$\begin{aligned}
\Gamma^{\mathbf{r}}(Z,W) &:= \{\,(p,x) \mid \exists_{(p',x')\in Z}\exists_a\Big(x = -a\frac{x'-1}{2} \wedge p = \mathrm{LR}_a(p')\Big) \vee^{\mathrm{u}} \\
&\qquad\qquad\qquad \exists^{\mathrm{u}}_{(q',x')\in W}\Big(x = \frac{x'}{2} \wedge p = \mathrm{U}(q')\Big)\,\}, \\
\Delta^{\mathbf{r}}(Z,W) &:= \{\,(q,x) \mid \exists_{(p',x')\in Z}\exists_a\Big(x = a\frac{x'+1}{2} \wedge q = \mathrm{Fin}_a(p')\Big) \vee^{\mathrm{u}} \\
&\qquad\qquad\qquad \exists^{\mathrm{u}}_{(q',x')\in W}\Big(x = \frac{x'}{2} \wedge q = \mathrm{D}(q')\Big)\,\}
\end{aligned}$$

($\vee^{\mathrm{u}}$: the whole formula has no computational significance).
Define

$$(({}^{\mathrm{co}}G)^{\mathbf{r}}, ({}^{\mathrm{co}}H)^{\mathbf{r}}) := \nu_{(Z,W)}(\Gamma^{\mathbf{r}}(Z,W), \Delta^{\mathbf{r}}(Z,W))$$

CoGAverage:

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

Consider two sets of averages, the second one with a "carry" $i \in \mathbf{SD}_2 := \{-2,-1,0,1,2\}$:

$$\mathrm{Av} := \{\, \frac{x+y}{2} \mid x, y \in {}^{\mathrm{co}}G \,\},$$
$$\mathrm{Avc} := \{\, \frac{x+y+i}{4} \mid x, y \in {}^{\mathrm{co}}G,\ i \in \mathbf{SD}_2 \,\}.$$

Suffices: Avc satisfies the clause coinductively defining ${}^{\mathrm{co}}G$, for then by the greatest-fixed-point axiom for ${}^{\mathrm{co}}G$ we have $\mathrm{Avc} \subseteq {}^{\mathrm{co}}G$. Since we also have $\mathrm{Av} \subseteq \mathrm{Avc}$ we obtain $\mathrm{Av} \subseteq {}^{\mathrm{co}}G$, i.e., our claim.

CoGAvToAvc:

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

Implicit algorithm. $f^* :=$ cCoGPsdTimes, and $s :=$ cCoHToCoG.
cL denotes the function extracted from the proof of a lemma L.
CoGPsdTimes: $\forall^{\mathrm{nc}}_x \forall_a ({}^{\mathrm{co}}G(x) \to {}^{\mathrm{co}}G(a * x))$.

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

Need J: $\mathbf{SD} \to \mathbf{SD} \to \mathbf{SD}_2 \to \mathbf{SD}_2$, K: $\mathbf{SD} \to \mathbf{SD} \to \mathbf{SD}_2 \to \mathbf{SD}$ with $d + e + 2i = J(d, e, i) + 4K(d, e, i)$ (cases on d, e, i). Then

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

CoGAvcSatColCl:

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

Implicit algorithm.

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

CoGAvcToCoG:

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

Implicit algorithm. Proof uses SdDisj: $\forall_d(d=0\vee\exists_a(d=a))$.

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

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

Composing CoGAvToAvc and CoGAvcToCoG gives CoGAverage.

Extracted term for CoGAvcToCoG:

```
[ipp](CoRec sdtwo@@ag@@ag=>ag sdtwo@@ag@@ag=>ah)ipp
 ([ipp0][let idpp (cCoGAvcSatCoICl
         left ipp0 left right ipp0 right right ipp0)
     [case (cSdDisj left right idpp)
      (DummyL -> InR(InR(left idpp@right right idpp)))
      (Inr a -> InL(a@InR
       (a times inv left idpp@
        cCoGPsdTimes inv a left right right idpp@
        cCoGPsdTimes inv a right right right idpp))))]])
 ([ipp0][let idpp ...] ...)
```

`ipp`	variable of type $\mathbf{SD}_2 \times \mathbf{G} \times \mathbf{G}$
`idpp`	variable of type $\mathbf{SD}_2 \times \mathbf{SD} \times \mathbf{G} \times \mathbf{G}$
`[ipp]r`	lambda abstraction $\lambda_{ipp} r$
`sdtwo@@ag@@ag=>ah`	function type $\mathbf{SD}_2 \times \mathbf{G} \times \mathbf{G} \to \mathbf{H}$
`r@s`, `left r`, `right r`	product term, components
`cL`	realizer for lemma L

Corecursion $\sim$ coinduction.

$$ {}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)} \colon \sigma \to \delta_{\mathbf{G}} \to \delta_{\mathbf{H}} \to \mathbf{G} $$
$$ {}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)} \colon \tau \to \delta_{\mathbf{G}} \to \delta_{\mathbf{H}} \to \mathbf{H} $$

with step types

$$ \delta_{\mathbf{G}} := \sigma \to \mathbf{PSD} \times (\mathbf{G} + \sigma) + (\mathbf{H} + \tau), $$
$$ \delta_{\mathbf{H}} := \tau \to \mathbf{PSD} \times (\mathbf{G} + \sigma) + (\mathbf{H} + \tau). $$

$\mathbf{PSD} \times (\mathbf{G} + \sigma) + (\mathbf{H} + \tau)$ appears since $\mathbf{G}$ has constructors

$$ \mathrm{LR} \colon \mathbf{PSD} \to \mathbf{G} \to \mathbf{G} \text{ and } \mathrm{U} \colon \mathbf{H} \to \mathbf{G}, $$

and $\mathbf{H}$ has constructors

$$ \mathrm{Fin} \colon \mathbf{PSD} \to \mathbf{G} \to \mathbf{H} \text{ and } \mathrm{D} \colon \mathbf{H} \to \mathbf{H}. $$

- Analyzing the step terms gives the "implicit algorithm".
- Extracted terms are in an extension T^+ of Gödel's T, the term language of TCF. They denote partial continuous functionals (Scott/Ershov).
- Verification is automatic (soundness theorem).
- Minlog provides a translation to Haskell for (lazy) evaluation.
- "Code carrying proof" can be a reasonable alternative to "Proof carrying code" (Necula).