Logic for exact real arithmetic

Helmut Schwichtenberg
Joint work with Ulrich Berger (Swansea), Nils Köpp (LMU), Kenyi Miyamoto (Innsbruck), Hideki Tsuiki (Kyoto) and Franziskus Wiesnet (LMU)

Mathematisches Institut, LMU, München

2018 Joint Meeting of the Korean Mathematical Society and the German Mathematical Society
Seoul, Korea, October 3-6, 2018

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. Example:

$$\forall_x A \quad \mapsto \quad \forall_x^{\mathrm{nc}}(x \in {}^{\mathrm{co}}I \to A)).$$

- Computational content of $x \in {}^{\mathrm{co}}I$ is a stream representing x.

A real number can be represented as a Cauchy sequence $(a_n)_n$ of rationals together with a Cauchy modulus M satisfying

$$|a_n - a_m| \leq \frac{1}{2^p} \quad \text{for } n, m \geq M(p).$$

Arithmetical operations on real numbers x, y are defined by

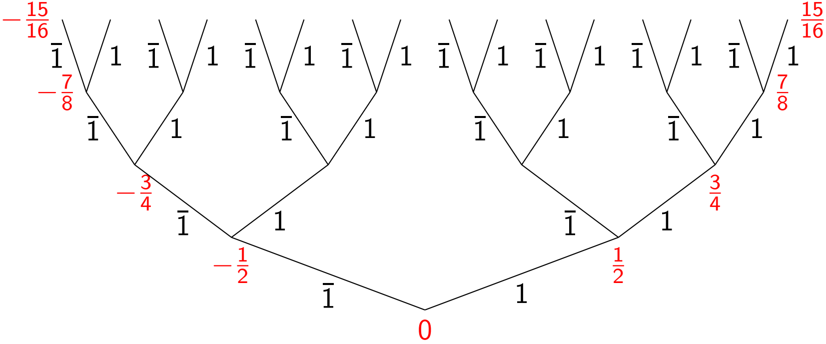
	c_n	$L(p)$
$x + y$	$a_n + b_n$	$\max\big(M(p+1), N(p+1)\big)$
$-x$	$-a_n$	$M(p)$
$\lvert x\rvert$	$\lvert a_n\rvert$	$M(p)$
$x \cdot y$	$a_n \cdot b_n$	$\max\big(M(p+1+p_y), N(p+1+p_x)\big)$
$\frac{1}{x}$ for $\lvert x\rvert \in_q \mathbb{R}^+$	$\begin{cases} \frac{1}{a_n} & \text{if } a_n \neq 0 \\ 0 & \text{if } a_n = 0 \end{cases}$	$M(2(q+1)+p)$

where 2^{p_x} is the upper bound of x provided by the Archimedian property.

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

Dyadic rationals:

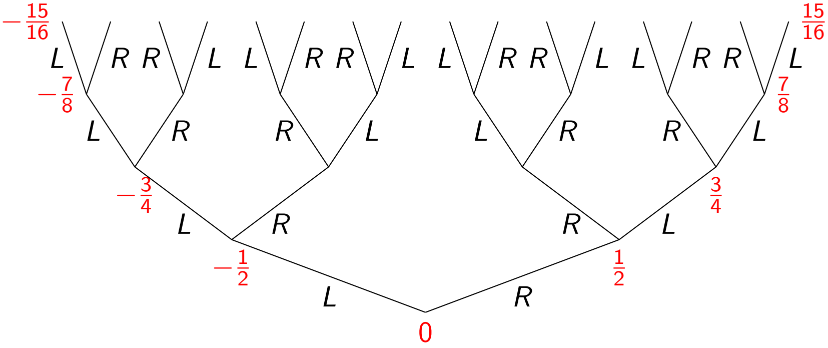
$$\sum_{n<m} \frac{k_n}{2^{n+1}} \qquad \text{with } k_n \in \{-1, 1\}.$$



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:

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

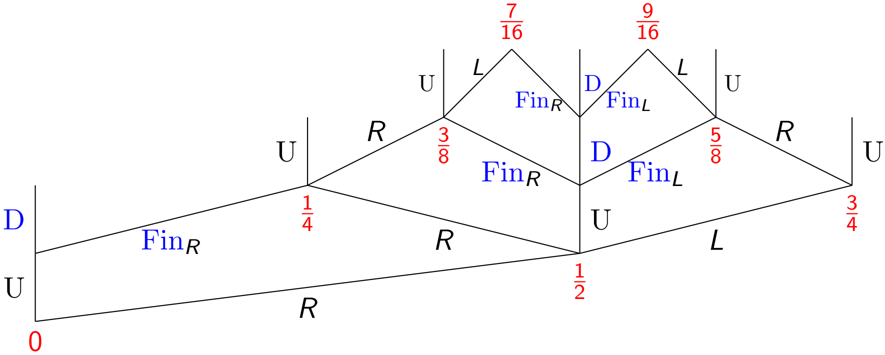
What is the first digit? Cure: delay.

- 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.

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 signed digit streams

Goal:

$$x, y \in {}^{\mathrm{co}}I \to \frac{x+y}{2} \in {}^{\mathrm{co}}I.$$

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

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

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

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

Then

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

satisfy the (strengthened) axioms

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

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

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

$$x, y \in {}^{\mathrm{co}}I \to \frac{x+y}{2} \in {}^{\mathrm{co}}I.$$

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.

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

$$i \in \mathrm{SD}_2 \to x, y \in {}^{\mathrm{co}}I \to \exists_{j \in \mathrm{SD}_2} \exists_{k \in \mathrm{SD}} \exists_{x', y' \in {}^{\mathrm{co}}I} \Big(\frac{x + y + i}{4} = \frac{\frac{x' + y' + j}{4} + k}{2} \Big).$$

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

$$i = J(i) + 4K(i), \qquad |J(i)| \le 2, \qquad |i| \le 6 \to |K(i)| \le 1.$$

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 $Q \subseteq {}^{\mathrm{co}}I$:

$$\exists_{i \in \mathrm{SD}_2} \exists_{x,y \in {}^{\mathrm{co}}I} (z = \frac{x+y+i}{4}) \to z \in {}^{\mathrm{co}}I.$$

This gives our claim

$$x, y \in {}^{\mathrm{co}}I \to \frac{x+y}{2} \in {}^{\mathrm{co}}I.$$

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 $(k,d), (l,e) \in \mathrm{SD}^{\mathbf{r}}$).

Realizability

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

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

Let

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

They satisfy the (strengthened) axioms

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

From the proof M of

$$x, y \in {}^{\mathrm{co}}I \to \frac{x+y}{2} \in {}^{\mathrm{co}}I$$

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

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

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.

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.

Method also works for multiplication and division:

$$
\begin{aligned}
&x, y \in {}^{\mathrm{co}}I \to \frac{x+y}{2} \in {}^{\mathrm{co}}I,\\
&x, y \in {}^{\mathrm{co}}I \to x \cdot y \in {}^{\mathrm{co}}I,\\
&x, y \in {}^{\mathrm{co}}I \to \frac{1}{4} \leq y \to \frac{x}{y} \in {}^{\mathrm{co}}I,
\end{aligned}
$$

both w.r.t. signed digit and Gray code.

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 relativising 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.

References

U. Berger, K. Miyamoto, H.S. and M. Seisenberger,
Minlog - A tool for program extraction supporting algebras and coalgebras.
In: Algebra and Coalgebra in Computer Science, LNCS 6859, 2011, pp. 393–399

U. Berger, K. Miyamoto, H.S. and H. Tsuiki,
Logic for Gray-code computation.
In: Concepts of Proof in Mathematics, Philosophy, and Computer Science (eds. Probst, Schuster). De Gruyter, 2016, pp. 69-110

H.S. and S.S. Wainer, *Proofs and Computations*,
Perspectives in Logic. Association for Symbolic Logic and Cambridge University Press, 2012.