

CHAPTER 5

Applications

Real numbers in the exact (as opposed to floating-point) sense can be given in different formats, for instance

- (i) as Cauchy sequences (of rationals, with a Cauchy modulus), or else
- (ii) as infinite sequences (“streams”) of “signed digits”. Intuitively, the stream $d_0, d_1, d_2 \dots$ represents the real number

$$\sum_{i=0}^{\infty} \frac{d_i}{2^{i+1}} \quad \text{with } d_i \in \{1, 0, -1\}.$$

We are interested in formally verified algorithms on real numbers in an arbitrary format. To this end we generate such algorithms as extracted terms $\text{et}(M)$ of formal existence proofs M . Recall that in our setting universal quantifiers are ignored by realizability. This makes it possible to carry out proofs using a standard representation of reals x (e.g., Cauchy sequences with modulus), and let computational content only arise by relativising x to appropriate c.r. predicates. An example is the relativization of x to a predicate ${}^{\text{co}}I$ coinductively defined in such a way that the computational content of $x \in {}^{\text{co}}I$ is a stream representing x . The required verification is provided by a formal soundness proof of the realizability interpretation.

5.1. Exact real arithmetic

5.1.1. Cauchy sequences, equality. We shall view a real as a Cauchy sequence of rationals with a separately given modulus.

DEFINITION 5.1.1. A real number x is a pair $((a_n)_{n \in \mathbb{N}}, M)$ with $a_n \in \mathbb{Q}$ and $M: \mathbb{Z}^+ \rightarrow \mathbb{N}$ such that $(a_n)_n$ is a *Cauchy sequence* with modulus M , that is

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

and M is weakly increasing (that is $M(p) \leq M(q)$ for $p \leq q$). M is called *Cauchy modulus* of x .

We shall loosely speak of a real $(a_n)_n$ if the Cauchy modulus M is clear from the context or inessential. Every rational a is tacitly understood as the

real represented by the constant sequence $a_n = a$ with the constant modulus $M(p) = 0$.

DEFINITION 5.1.2. Two reals $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$ are called *equivalent* (or *equal* and written $x = y$, if the context makes clear what is meant), if

$$|a_{M(p+1)} - b_{N(p+1)}| \leq \frac{1}{2^p} \quad \text{for all } p \in \mathbb{Z}^+.$$

We want to show that this is an equivalence relation. Reflexivity and symmetry are clear. For transitivity we use the following lemma:

LEMMA 5.1.3 (RealEqChar). *For reals $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$ the following are equivalent:*

- (a) $x = y$;
- (b) $\forall_p \exists_{n_0} \forall_{n \geq n_0} (|a_n - b_n| \leq \frac{1}{2^p})$.

PROOF. (a) implies (b). For $n \geq M(p+2), N(p+2)$ we have

$$\begin{aligned} |a_n - b_n| &\leq |a_n - a_{M(p+2)}| + |a_{M(p+2)} - b_{N(p+2)}| + |b_{N(p+2)} - b_n| \\ &\leq \frac{1}{2^{p+2}} + \frac{1}{2^{p+1}} + \frac{1}{2^{p+2}}. \end{aligned}$$

(b) implies (a). Let $q \in \mathbb{Z}^+$, and $n \geq n_0, M(p+1), N(p+1)$ with n_0 provided for q by (b). Then

$$\begin{aligned} |a_{M(p+1)} - b_{N(p+1)}| &\leq |a_{M(p+1)} - a_n| + |a_n - b_n| + |b_n - b_{N(p+1)}| \\ &\leq \frac{1}{2^{p+1}} + \frac{1}{2^q} + \frac{1}{2^{p+1}}. \end{aligned}$$

The claim follows, because this holds for every $q \in \mathbb{Z}^+$. □

REMARK 5.1.4 (RealSeqEqToEq). An immediate consequence is that any two reals with the same Cauchy sequence (but possibly different moduli) are equal.

LEMMA 5.1.5 (RealEqTrans). *Equality between reals is transitive.*

PROOF. Let $(a_n)_n, (b_n)_n, (c_n)_n$ be the Cauchy sequences for x, y, z . Assume $x = y$, $y = z$ and pick n_1, n_2 for $p+1$ according to the lemma above. Then $|a_n - c_n| \leq |a_n - b_n| + |b_n - c_n| \leq \frac{1}{2^{p+1}} + \frac{1}{2^{p+1}}$ for $n \geq n_1, n_2$. □

5.1.2. The Archimedian property. For every function on the reals we certainly want compatibility with equality. This however is not always the case; here is an important example.

LEMMA 5.1.6 (RealBound). *For every real $x := ((a_n)_n, M)$ we can find p_x such that $|a_n| \leq 2^{p_x}$ for all n .*

PROOF. Let $n_0 := M(1)$ and p_x be such that $\max\{|a_n| \mid n \leq n_0\} + \frac{1}{2} \leq 2^{p_x}$. Then $|a_n| \leq 2^{p_x}$ for all n . $\square$

Clearly this assignment of p_x to x is not compatible with equality.

5.1.3. Nonnegative and positive reals. A real $x := ((a_n)_n, M)$ is called *nonnegative* (written $x \in \mathbb{R}^{0+}$) if

$$-\frac{1}{2^p} \leq a_{M(p)} \quad \text{for all } p \in \mathbb{Z}^+.$$

It is *p-positive* (written $x \in_p \mathbb{R}^+$, or $x \in \mathbb{R}^+$ if p is not needed) if

$$\frac{1}{2^p} \leq a_{M(p+1)}.$$

We want to show that both properties are compatible with equality. First we prove a useful characterization of nonnegative reals.

LEMMA 5.1.7 (RealNNegChar). *For a real $x := ((a_n)_n, M)$ the following are equivalent:*

- (a) $x \in \mathbb{R}^{0+}$;
- (b) $\forall_p \exists_{n_0} \forall_{n \geq n_0} (-\frac{1}{2^p} \leq a_n)$.

PROOF. (a) implies (b). For $n \geq M(p+1)$ we have

$$\begin{aligned} -\frac{1}{2^p} &\leq -\frac{1}{2^{p+1}} + a_{M(p+1)} \\ &= -\frac{1}{2^{p+1}} + (a_{M(p+1)} - a_n) + a_n \\ &\leq -\frac{1}{2^{p+1}} + \frac{1}{2^{p+1}} + a_n. \end{aligned}$$

(b) implies (a). Let $q \in \mathbb{Z}^+$ and $n \geq n_0, M(p)$ with n_0 provided by (b) (for q). Then

$$\begin{aligned} -\frac{1}{2^p} - \frac{1}{2^q} &\leq -\frac{1}{2^p} + a_n \\ &= -\frac{1}{2^p} + (a_n - a_{M(p)}) + a_{M(p)} \\ &\leq -\frac{1}{2^p} + \frac{1}{2^p} + a_{M(p)}. \end{aligned}$$

The claim follows, because this holds for every q . $\square$

LEMMA 5.1.8 (RealNNegCompat). *If $x \in \mathbb{R}^{0+}$ and $x = y$, then $y \in \mathbb{R}^{0+}$.*

PROOF. Let $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$. Assume $x \in \mathbb{R}^{0+}$ and $x = y$, and let p be given. Pick n_0 according to the lemma above

and n_1 according to the characterization of equality of reals in Lemma 5.1.3 (RealEqChar) (both for $p+1$). Then for $n \geq n_0, n_1$

$$-\frac{1}{2^p} \leq -\frac{1}{2^{p+1}} + a_n \leq (b_n - a_n) + a_n.$$

Hence $y \in \mathbb{R}^{0+}$ by definition. $\square$

LEMMA 5.1.9 (RealPosChar). *For a real $x := ((a_n)_n, M)$ with $x \in_p \mathbb{R}^+$ we have*

$$\frac{1}{2^{p+1}} \leq a_n \quad \text{for } M(p+1) \leq n.$$

Conversely, from $\forall_{n \geq n_0} (\frac{1}{2^q} \leq a_n)$ we can infer $x \in_{q+1} \mathbb{R}^+$.

PROOF. Assume $x \in_p \mathbb{R}^+$, that is $\frac{1}{2^p} \leq a_{M(p+1)}$. Then

$$\frac{1}{2^{p+1}} \leq -\frac{1}{2^{p+1}} + a_{M(p+1)} = -\frac{1}{2^{p+1}} + (a_{M(p+1)} - a_n) + a_n \leq a_n$$

for $M(p+1) \leq n$. Conversely,

$$\begin{aligned} \frac{1}{2^{q+1}} &< -\frac{1}{2^{q+2}} + \frac{1}{2^q} \\ &\leq -\frac{1}{2^{q+2}} + a_n && \text{for } n_0 \leq n \\ &\leq (a_{M(q+2)} - a_n) + a_n && \text{for } M(q+2) \leq n. \end{aligned}$$

Hence $x \in_{q+1} \mathbb{R}^+$. $\square$

Positivity is compatible with equality, but only up to a shift of p :

LEMMA 5.1.10 (RealPosCompat). *If $x \in_p \mathbb{R}^+$ and $x = y$, then $y \in_{p+2} \mathbb{R}^+$.*

PROOF. Let $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$. Assume $x = y$ and $x \in_p \mathbb{R}^+$, that is $\frac{1}{2^p} \leq a_{M(p+1)}$. The goal is $\frac{1}{2^{p+2}} \leq b_{N(p+3)}$. We have

$$\frac{1}{2^{p+2}} = \frac{1}{2^{p+1}} - \frac{1}{2^{p+2}} \leq a_{M(p+3)} + (b_{N(p+3)} - a_{M(p+3)})$$

using Lemma 5.1.9 (RealPosChar) with the monotonicity of M , and the definition of $x = y$. $\square$

5.1.4. Arithmetical functions. Given real numbers $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$, we define $x + y$, $-x$, $|x|$, $x \cdot y$, and $\frac{1}{x}$ (the latter only provided that $|x| \in_q \mathbb{R}^+$) as represented by the respective sequence (c_n) of

rationals with modulus L :

	c_n	$L(p)$
$x + y$	$a_n + b_n$	$\max(M(p+1), N(p+1))$
$-x$	$-a_n$	$M(p)$
$ x $	$ a_n $	$M(p)$
$x \cdot y$	$a_n \cdot b_n$	$\max(M(p+1+p_y), N(p+1+p_x))$
$\frac{1}{x}$ for $ x \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 provided by Lemma 5.1.6 (RealBound).

LEMMA 5.1.11. *For reals x, y also $x+y$, $-x$, $|x|$, $x \cdot y$ and (provided that $|x| \in_q \mathbb{R}^+$) also $1/x$ are reals.*

PROOF. We restrict ourselves to the cases $x \cdot y$ and $1/x$.

$$\begin{aligned}
 |a_n b_n - a_m b_m| &= |a_n(b_n - b_m) + (a_n - a_m)b_m| \\
 &\leq |b_n - b_m| \cdot |a_n| + |a_n - a_m| \cdot |b_m| \\
 &\leq |b_n - b_m| \cdot 2^{p_x} + |a_n - a_m| \cdot 2^{p_y} \leq \frac{1}{2^p}
 \end{aligned}$$

for $n, m \geq \max(M(p+1+p_y), N(p+1+p_x))$.

For $1/x$ assume $|x| \in_q \mathbb{R}^+$. Then by the (proof of our) characterization of positivity in Lemma 5.1.9 (RealPosChar), $\frac{1}{2^{q+1}} \leq |a_n|$ for $n \geq M(q+1)$. Hence

$$\begin{aligned}
 \left| \frac{1}{a_n} - \frac{1}{a_m} \right| &= \frac{|a_m - a_n|}{|a_n a_m|} \\
 &\leq 2^{2(q+1)} |a_m - a_n| \quad \text{for } n, m \geq M(q+1) \\
 &\leq \frac{1}{2^p} \quad \text{for } n, m \geq M(2(q+1)+p).
 \end{aligned}$$

The claim now follows from the assumption that M is weakly increasing. $\square$

LEMMA 5.1.12. *For reals x, y, z*

$$\begin{aligned}
 x + (y + z) &= (x + y) + z & x \cdot (y \cdot z) &= (x \cdot y) \cdot z \\
 x + 0 &= x & x \cdot 1 &= x \\
 x + (-x) &= 0 & 0 < |x| \rightarrow x \cdot \frac{1}{x} &= 1 \\
 x + y &= y + x & x \cdot y &= y \cdot x \\
 x \cdot (y + z) &= x \cdot y + x \cdot z
 \end{aligned}$$

PROOF. For $0 < |x| \rightarrow x \cdot \frac{1}{x} = 1$ the Cauchy sequences are finally the same, which suffices. In all other cases both the Cauchy sequences and the moduli are the same, hence both sides are actually identical. $\square$

LEMMA 5.1.13. *The functions $x + y$, $-x$, $|x|$, $x \cdot y$ and (provided that $|x| \in_q \mathbb{R}^+$) also $1/x$ are compatible with equality.*

PROOF. Routine. For instance in case $x + y$ because of the commutativity of $+$ it suffices to prove $x = y \rightarrow x + z = y + z$. But this follows immediately from Lemma 5.1.3 (RealEqChar): the n_0 for the conclusion can be the same as for the premise. $\square$

LEMMA 5.1.14. *For reals x, y from $x \cdot y = 1$ we can infer $0 < |x|$.*

PROOF. Pick p such that $|b_n| \leq 2^p$ for all n . Pick n_0 such that $n_0 \leq n$ implies $\frac{1}{2} \leq a_n \cdot b_n$. Then $\frac{1}{2} \leq |a_n| \cdot 2^p$ for $n_0 \leq n$, and hence $\frac{1}{2^{p+1}} \leq |a_n|$. $\square$

LEMMA 5.1.15. *For reals x, y ,*

- (a) $x, y \in \mathbb{R}^{0+} \rightarrow x + y, x \cdot y \in \mathbb{R}^{0+}$,
- (b) $x, y \in \mathbb{R}^+ \rightarrow x + y, x \cdot y \in \mathbb{R}^+$,
- (c) $x \in \mathbb{R}^{0+} \rightarrow -x \in \mathbb{R}^{0+} \rightarrow x = 0$.

PROOF. (a), (b). Routine. (c). Let p be given. Pick n_0 such that $-\frac{1}{2^p} \leq a_n$ and $-\frac{1}{2^p} \leq -a_n$ for $n \geq n_0$. Then $|a_n| \leq \frac{1}{2^p}$. $\square$

5.1.5. Comparison of reals. We write $x \leq y$ for $y - x \in \mathbb{R}^{0+}$ and $x < y$ for $y - x \in \mathbb{R}^+$. Unwinding the definitions yields that $x \leq y$ is to say that for every p , $a_{L(p)} \leq b_{L(p)} + \frac{1}{2^p}$ with $L(p) := \max(M(p), N(p))$, or equivalently (using Lemma 5.1.7 (RealNNegChar)) that for every p there exists n_0 such that $a_n \leq b_n + \frac{1}{2^p}$ for all $n \geq n_0$. Furthermore, $x < y$ is a shorthand for the presence of p with $a_{L(p+1)} + \frac{1}{2^p} \leq b_{L(p+1)}$ with L the maximum of M and N , or equivalently (using Lemma 5.1.9 (RealPosChar)) for the presence of p, q with $a_n + \frac{1}{2^p} \leq b_n$ for all $n \geq q$; we then write $x <_p y$ (or $x <_{p,q} y$) whenever we want to call these witnesses.

LEMMA 5.1.16 (RealApprox). $\forall_{x,p} \exists_a (|a - x| \leq \frac{1}{2^p})$.

PROOF. Let $x = ((a_n), M)$. Given p , pick $a_{M(p)}$. We show $|a_{M(p)} - x| \leq \frac{1}{2^p}$, that is $|a_{M(p)} - a_{M(q)}| \leq \frac{1}{2^p} + \frac{1}{2^q}$ for every q . But this follows from

$$|a_{M(p)} - a_{M(q)}| \leq |a_{M(p)} - a_{M(p+q)}| + |a_{M(p+q)} - a_{M(q)}| \leq \frac{1}{2^p} + \frac{1}{2^q}. \quad \square$$

LEMMA 5.1.17. *For reals x, y, z ,*

$$\begin{array}{ll}
x \leq x & x \not\leq x \\
x \leq y \rightarrow y \leq x \rightarrow x = y & x < y \rightarrow y < z \rightarrow x < z \\
x \leq y \rightarrow y \leq z \rightarrow x \leq z & x < y \rightarrow x + z < y + z \\
x \leq y \rightarrow x + z \leq y + z & x < y \rightarrow 0 < z \rightarrow x \cdot z < y \cdot z \\
x \leq y \rightarrow 0 \leq z \rightarrow x \cdot z \leq y \cdot z &
\end{array}$$

PROOF. From Section 5.1.4. □

Here we have left out information on witnesses p for the statements proving a $<$ -formula. Such estimates can easily be given explicitly. Here are two examples.

LEMMA 5.1.18 (RealPosPlus). $0 \leq x \rightarrow 0 <_p y \rightarrow 0 <_{p+3} x + y$.

PROOF. From $0 \leq x$ we have $\forall q \exists n_0 \forall n \geq n_0 (-\frac{1}{2^q} \leq a_n)$. From $0 <_p y$ we have some n_1 such that $\forall n \geq n_1 (\frac{1}{2^{p+1}} \leq b_n)$. Pick n_0 for $p+2$. Then $n_0, n_1 \leq n$ implies $0 \leq a_n + \frac{1}{2^{p+2}}$ and $\frac{1}{2^{p+2}} \leq b_n - \frac{1}{2^{p+2}}$, hence $\frac{1}{2^{p+2}} \leq a_n + b_n$. Now Lemma 5.1.9 (RealPosChar) gives $0 <_{p+3} x + y$. □

LEMMA 5.1.19. $x \leq y \rightarrow y <_p z \rightarrow x <_{p+5} z$.

PROOF. This follows from Lemma 5.1.18 (RealPosPlus). □

As is to be expected in view of the existential and universal character of the predicates $<$ and $\leq$ on the reals, we have:

LEMMA 5.1.20 (LeIsNotGt). $x \leq y \leftrightarrow y \not< x$.

PROOF. $\rightarrow$. Assume $x \leq y$ and $y < x$. By Lemma 5.1.19 we obtain $x < x$, a contradiction.

$\leftarrow$. It clearly suffices to show $0 \not< z \rightarrow z \leq 0$, for a real z given by $(c_n)_n$. Assume $0 \not< z$. We must show $\forall p \exists n_0 \forall n \geq n_0 (c_n \leq \frac{1}{2^p})$. Let p be given. By assumption $0 \not< z$, hence $\neg \exists q (\frac{1}{2^q} \leq c_{M(q+1)})$. For $q := p+1$ this implies $c_{M(p+2)} < \frac{1}{2^{p+1}}$, hence $c_n \leq c_{M(p+2)} + \frac{1}{2^{p+2}} < \frac{1}{2^p}$ for $M(p+2) \leq n$. □

Constructively, we cannot compare two reals, but we can compare every real with a nontrivial interval.

LEMMA 5.1.21 (ApproxSplit). *Let x, y, z be given and assume $x < y$. Then either $z \leq y$ or $x \leq z$.*

PROOF. Let $x := ((a_n)_n, M)$, $y := ((b_n)_n, N)$, $z := ((c_n)_n, L)$. Assume $x <_p y$, that is (by definition) $\frac{1}{2^p} \leq b_n - a_n$ for $n := \max(M(p+2), N(p+2))$. Let $m := \max(n, L(p+2))$.

Case $c_m \leq \frac{a_n+b_n}{2}$. We show $z \leq y$. It suffices to prove $c_l \leq b_l$ for $l \geq m$. This follows from

$$c_l \leq c_m + \frac{1}{2^{p+2}} \leq \frac{a_n + b_n}{2} + \frac{b_n - a_n}{4} = b_n - \frac{b_n - a_n}{4} \leq b_n - \frac{1}{2^{p+2}} \leq b_l.$$

Case $c_m \not\leq \frac{a_n+b_n}{2}$. We show $x \leq z$. This follows from $a_l \leq c_l$ for $l \geq m$:

$$a_l \leq a_n + \frac{1}{2^{p+2}} \leq a_n + \frac{b_n - a_n}{4} = \frac{a_n + b_n}{2} - \frac{b_n - a_n}{4} \leq c_m - \frac{1}{2^{p+2}} \leq c_l. \quad \square$$

Notice that the boolean object determining whether $z \leq y$ or $x \leq z$ depends on the representation of x , y and z . In particular this assignment is *not* compatible with our equality relation.

One might think that the non-available comparison of two reals could be circumvented by using a maximum function. Indeed, such a function can easily be defined (component-wise), and it has the expected properties $x, y \leq \max(x, y)$ and $x, y \leq z \rightarrow \max(x, y) \leq z$. But what is missing is the knowledge that $\max(x, y)$ equals one of its arguments, i.e., we do not have $\max(x, y) = x \vee \max(x, y) = y$.

However, in many cases it is sufficient to pick the up to ε largest real out of finitely many given ones. This is indeed possible. We give the proof for two reals; it can be easily generalized.

LEMMA 5.1.22 (Maximum of two reals). *Let $x := ((a_n)_n, M)$ and $y := ((b_n)_n, N)$ be reals, and $p \in \mathbb{Z}^+$. Then either $x \leq y + \frac{1}{2^p}$ or else $y \leq x + \frac{1}{2^p}$.*

PROOF. Let $m := \max(M(p+1), N(p+1))$.

Case $a_m \leq b_m$. Then for $m \leq n$

$$a_n \leq a_m + \frac{1}{2^{p+1}} \leq b_m + \frac{1}{2^{p+1}} \leq b_n + \frac{1}{2^p}.$$

This holds for all $n \geq m$, therefore $x \leq y + \frac{1}{2^p}$.

Case $b_m < a_m$. Then for $m \leq n$

$$b_n \leq b_m + \frac{1}{2^{p+1}} < a_m + \frac{1}{2^{p+1}} \leq a_n + \frac{1}{2^p}.$$

This holds for all $n \geq m$, therefore $y \leq x + \frac{1}{2^p}$. $\square$

5.2. Algorithms on stream-represented real numbers

5.2.1. The predicates I and ${}^{\circ}I$. We model infinite sequences of signed digits (streams) as objects in the algebra $\mathbb{S}(\mathbb{D}) := \mu_{\xi}(\mathbb{C}: \mathbb{D} \rightarrow \xi \rightarrow \xi)$, where $\mathbb{D} := \mu_{\xi}(\text{SdR}: \xi, \text{SdM}: \xi, \text{SdL}: \xi)$ is a 3-element algebra. Such streams will appear as realizers of an inductive predicate I defined by the single clause

$$(27) \quad \forall_{d, x', x} \left(d \in \text{Sd} \rightarrow x' \in I \rightarrow x = \frac{x' + d}{2} \rightarrow x \in I \right).$$

Here (and later) x, y, z range over real numbers in $[-1, 1]$ and d over integers. Sd is a (formally inductive) predicate expressing that its integer argument d is a signed digit, i.e., $|d| \leq 1$. We have chosen (27) rather than the simpler

$$(28) \quad \forall_{d,x} \left(d \in \text{Sd} \rightarrow x \in I \rightarrow \frac{x+d}{2} \in I \right),$$

since we want I to be compatible with the defined equality $=$ on real numbers

$$(29) \quad \forall_{x,y} (x = y \rightarrow x \in I \rightarrow y \in I),$$

which easily follows from (27) (with reflexivity, symmetry and transitivity of $=$). Using (29) we then obtain (28) from (27) as a lemma.

The dual ${}^{\text{co}}I$ of I is defined by its closure axiom

$$x \in {}^{\text{co}}I \rightarrow \exists_{d,x',y} \left(d \in \text{Sd} \wedge x' \in {}^{\text{co}}I \wedge y = \frac{x'+d}{2} \wedge x = y \right).$$

Similar to what was done above it can be simplified to

$$(30) \quad x \in {}^{\text{co}}I \rightarrow \exists_{d,x'} \left(d \in \text{Sd} \wedge x' \in {}^{\text{co}}I \wedge x = \frac{x'+d}{2} \right).$$

As examples we consider proofs that

- (I) any real given in format (i) can be converted into format (ii), and
- (II) the average of two real numbers in $[-1, 1]$ is in $[-1, 1]$ again, w.r.t. format (ii) for both input and output.

5.2.2. Conversion of real numbers into streams. An essential tool in the proof for the first example is Lemma 5.1.21 (ApproxSplit) on page 81, expressing the possibility to compare a real z given as pair $((c_n)_n, M)$ with a proper rational interval $[a, b]$.

THEOREM 5.2.1. $|x| \leq 1 \rightarrow x \in {}^{\text{co}}I$.

PROOF. We use coinduction with competitor predicate $\{x \mid |x| \leq 1\}$. It suffices to prove

$$|x| \leq 1 \rightarrow \exists_{d,x'} \left(d \in \text{Sd} \wedge (x' \in {}^{\text{co}}I \vee |x'| \leq 1) \wedge x = \frac{x'+d}{2} \right).$$

Compare x with $[-\frac{1}{2}, 0]$. If $x \leq 0$, return SdL and continue with $2x + 1$. If $-\frac{1}{2} \leq x$, compare x with $[0, \frac{1}{2}]$. If $x \leq \frac{1}{2}$, return SdM and continue with $2x$. If $0 \leq x$, return SdR and continue with $2x - 1$. $\square$

More precisely, we have proven (with f of type $\mathbb{N} \rightarrow \mathbb{Q}$)

$$f \in T \rightarrow M \in T \rightarrow x \equiv (f, M) \rightarrow x \in \text{Real} \rightarrow |x| \leq 1 \rightarrow x \in {}^{\text{co}}I$$

of cotype $(\mathbb{N} \rightarrow \mathbb{Q}) \rightarrow (\mathbb{P} \rightarrow \mathbb{N}) \rightarrow {}^{\text{co}}\mathbb{S}(\mathbb{D})$. Here $x \in \text{Real}$ is an n.c. formula expressing that x is a real number in format (i). The term extracted from

this proof has type $(\mathbb{N} \rightarrow \mathbb{Q}) \rightarrow (\mathbb{P} \rightarrow \mathbb{N}) \rightarrow \mathbb{S}(\mathbb{D})$ and is built by the corecursion operator with step function

$$x \mapsto \begin{cases} (\text{SdL}, 2x + 1) & \text{if } g(-\frac{1}{2}, 0, x) = \mathbf{tt} \\ (\text{SdM}, 2x) & \text{if } g(-\frac{1}{2}, 0, x) = \mathbf{ff} \text{ and } g(0, \frac{1}{2}, x) = \mathbf{tt} \\ (\text{SdR}, 2x - 1) & \text{if } g(0, \frac{1}{2}, x) = \mathbf{ff}. \end{cases}$$

Here g is a function of type $\mathbb{Q} \rightarrow \mathbb{Q} \rightarrow \mathbb{R} \rightarrow \mathbb{B}$ representing the computational content of Lemma 5.1.21 (ApproxSplit).

5.2.3. Average of real numbers. In our second example we consider a proof that the average of two real numbers in $[-1, 1]$ is in $[-1, 1]$ again:

$$x, y \in {}^{\text{co}}I \rightarrow \frac{x + y}{2} \in {}^{\text{co}}I.$$

Following Berger and Seisenberger (2010) we begin with an informal proof. The computational content of this proof will be the desired algorithm.

Consider two sets of averages, the second one with a “carry” $i \in \mathbb{Z}$

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

where Sd_2 is a (formally inductive) predicate expressing that the integer i is an extended signed digit, i.e., $|i| \leq 2$. It suffices to show that Q satisfies

$$x \in Q \rightarrow \exists_{d, x'} (d \in \text{Sd} \wedge x' \in Q \wedge x = \frac{x' + d}{2}),$$

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

Below we will need functions $J, K: \mathbb{Z} \rightarrow \mathbb{Z}$ such that

$$(31) \quad \forall_i (i = J(i) + 4K(i)) \quad (\text{with } \forall_i (|J(i)| \leq 2), \forall_i (|i| \leq 6 \rightarrow |K(i)| \leq 1)).$$

We use the following notation for streams u of type $\mathbb{S}(\mathbb{D})$:

$$(u)_n := n\text{-th entry in } u,$$

$$Tu := \text{rest of } u \text{ after removal of its first entry.}$$

Clearly $(T^n u)_m = (u)_{n+m}$, where T^n denotes the n -th iteration of T .

LEMMA 5.2.2 (CoIAvToAvc).

$$x, y \in {}^{\text{co}}I \rightarrow \exists_{i, x', y'} (i \in \text{Sd}_2 \wedge x', y' \in {}^{\text{co}}I \wedge \frac{x + y}{2} = \frac{x' + y' + i}{4}).$$

PROOF. By the closure axiom (30) for ${}^{\text{co}}I$ we can write $x = \frac{x' + d}{2}$ and $y = \frac{y' + e}{2}$ for some $d, e \in \text{Sd}$ and $x', y' \in {}^{\text{co}}I$. Then

$$\frac{x + y}{2} = \frac{x' + y' + d + e}{4}. \quad \square$$

The computational content this proof is a function

$$\begin{aligned} \text{Av}_{\text{init}} &: \mathbb{S}(\mathbb{D}) \rightarrow \mathbb{S}(\mathbb{D}) \rightarrow \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D}) \\ \text{Av}_{\text{init}}(u, v) &:= \langle (u)_0 + (v)_0, Tu, Tv \rangle. \end{aligned}$$

LEMMA 5.2.3 (CoIAvcSatCoICl).

$$i \in \text{Sd}_2 \wedge x, y \in {}^{\text{co}I} \rightarrow \exists d \in \text{Sd} \exists j \in \text{Sd}_2 \exists x', y' \in {}^{\text{co}I} \left(\frac{x+y+i}{4} = \frac{\frac{x'+y'+j}{4} + d}{2} \right).$$

PROOF. By the closure axiom (30) for ${}^{\text{co}I}$ we can write $x = \frac{x'+d}{2}$ and $y = \frac{y'+e}{2}$ for some $d, e \in \text{Sd}$ and $x', y' \in {}^{\text{co}I}$. Then

$$\frac{x+y+i}{4} = \frac{x'+y'+d+e+2i}{8}.$$

Since $|d+e+2i| \leq 6$ we can write $d+e+2i = j+4k$ with $|j| \leq 2$ and $|k| \leq 1$ by the JK-property (31). Therefore

$$\frac{x+y+i}{4} = \frac{x'+y'+j+4k}{8} = \frac{\frac{x'+y'+j}{4} + k}{2}. \quad \square$$

The computational content of this proof is a function

$$\begin{aligned} \text{Av}_{\text{step}} &: \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D}) \rightarrow \mathbb{D} \times \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D}) \\ \text{Av}_{\text{step}} \langle i, u, v \rangle &:= \langle K((u)_0 + (v)_0 + 2i), J((u)_0 + (v)_0 + 2i), Tu, Tv \rangle. \end{aligned}$$

By coinduction from Lemma 5.2.3 we obtain

$$\text{LEMMA 5.2.4. } \forall z (\exists i, x, y (i \in \text{Sd}_2 \wedge x, y \in {}^{\text{co}I} \wedge z = \frac{x+y+i}{4}) \rightarrow z \in {}^{\text{co}I}).$$

THEOREM 5.2.5. *The average of two real numbers x, y in ${}^{\text{co}I}$ is in ${}^{\text{co}I}$:*

$$x, y \in {}^{\text{co}I} \rightarrow \frac{x+y}{2} \in {}^{\text{co}I}.$$

PROOF. Immediate from Lemma 5.2.2 and Lemma 5.2.4. $\square$

The extracted term is short (19 lines in `minlog/examples/analysis/`, file `sdavaux.scm`), and involves the corecursion operator. It represents the function

$$\text{cCoIAverage}: \mathbb{S}(\mathbb{D}) \rightarrow \mathbb{S}(\mathbb{D}) \rightarrow \mathbb{S}(\mathbb{D})$$

defined using corecursion, as follows.

- (i) From $u, v \in \mathbb{S}(\mathbb{D})$ form an initial triple $\text{Av}_{\text{init}}(u, v) \in \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D})$.
- (ii) Iterate $\text{Av}_{\text{step}}: \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D}) \rightarrow \mathbb{D} \times \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D})$ starting with $\text{Av}_{\text{init}}(u, v)$.
- (iii) Return the stream of the generated $d \in \mathbb{D}$.

5.3. Lookahead

Recall that real numbers in $[-1.1]$ can be represented in the form

$$\sum_{n=0}^{\infty} \frac{d_n}{2^{n+1}} \quad (d_n \in \{-1, 0, 1\}).$$

We are interested in algorithms for arithmetical functions on real numbers operating on such stream representations $(d_n)_n$. In particular we want to verify lookahead properties of such algorithms.

To this end we inductively define a binary predicate L of arity $(\mathbb{R}, \mathbb{N})$. The intended property of L is

a realizer of $x \in L_n$ is a list $(d_m)_{m < n}$ of signed digits which approximates x with error bound $\frac{1}{2^n}$, i.e., such that

$$\left| \sum_{m=0}^{n-1} \frac{d_m}{2^{m+1}} - x \right| \leq \frac{1}{2^n}.$$

Here we have written $x \in L_n$ for $L(x, n)$. Let x, y, z range over real numbers and d over integers. Sd is a (formally inductive) predicate expressing that its integer argument d is a signed digit, i.e., $|d| \leq 1$. L is defined by the two clauses

$$L_0^+ : \forall x (|x| \leq 1 \rightarrow x \in L_0),$$

$$L_1^+ : \forall_{x,y,n,d} \left(d \in \text{Sd} \rightarrow x \in L_n \rightarrow y = \frac{x+d}{2} \rightarrow y \in L_{n+1} \right).$$

L_1^+ says that if we know the first n digits of a representation of x and that $y = \frac{x+d}{2}$, then we know the first $n+1$ digits of a representation of y .

The induction or least-fixed-point (lfp) axiom for L is

$$\begin{aligned} & \forall_x (|x| \leq 1 \rightarrow Y(x, 0)) \rightarrow \\ & \forall_{x,y,n,d} \left(d \in \text{Sd} \rightarrow x \in L_n \rightarrow Y(x, n) \rightarrow y = \frac{x+d}{2} \rightarrow Y(y, n+1) \right) \rightarrow L \subseteq Y. \end{aligned}$$

The algebra associated with L is $\mathbb{L} := \mu_{\xi}(U : \xi, C : \mathbb{D} \rightarrow \xi \rightarrow \xi)$, i.e., finite lists of signed digits $-1, 0, 1$. We write u, v for objects of type $\mathbb{L}$, and $d :: u$ for Cdu .

We will need some properties of L .

LEMMA 5.3.1 (**LCompat**). $x = y \rightarrow x \in L_n \rightarrow y \in L_n$.

PROOF. Use the lfp-axiom for L . □

The term extracted from this proof is the identity on $\mathbb{L}$; it will be omitted in the sequel.

LEMMA 5.3.2 (**LToBd**). $x \in L_n \rightarrow |x| \leq 1$.

PROOF. Use induction on n . $\square$

Parallel to the (simplified) closure axiom (30) for ${}^{\text{co}}I$ (page 83) we have

LEMMA 5.3.3 (LClosure). $x \in L_{n+1} \rightarrow \exists_{d,x'} (d \in \text{Sd} \wedge x' \in L_n \wedge x = \frac{x'+d}{2})$.

PROOF. Use the lfp-axiom for L . $\square$

The extracted term **cLClosure** has type $\mathbb{L} \rightarrow \mathbb{D} \times \mathbb{L}$. It satisfies

$$\text{cLClosure}(d :: u) = \langle d, u \rangle.$$

We now proceed as before, but with L instead of ${}^{\text{co}}I$. As in Section 5.2.3 (page 84) we show

$$\left\{ \frac{x+y}{2} \mid x, y \in L_{n+1} \right\} \subseteq \left\{ \frac{x+y+i}{4} \mid x, y \in L_n, i \in \text{Sd}_2 \right\} \subseteq L_n,$$

where this time the final conclusion is proved by induction.

LEMMA 5.3.4 (LAvToAvc).

$$x, y \in L_{n+1} \rightarrow \exists_{i,x',y'} \left(i \in \text{Sd}_2 \wedge x', y' \in L_n \wedge \frac{x+y}{2} = \frac{x'+y'+i}{4} \right).$$

PROOF. By Lemma 5.3.3 we can write $x = \frac{x'+d}{2}$ and $y = \frac{y'+e}{2}$ for some $d, e \in \text{Sd}$ and $x', y' \in L_n$. Then

$$\frac{x+y}{2} = \frac{x'+y'+d+e}{4}. \quad \square$$

The extracted term **cLAvToAvc** has type $\mathbb{L} \rightarrow \mathbb{L} \rightarrow \mathbb{D}_2 \times \mathbb{L} \times \mathbb{L}$ and satisfies

$$\text{cLAvToAvc}(d :: u, e :: v) = \langle d+e, u, v \rangle.$$

LEMMA 5.3.5 (LAvcSatLC1).

$$i \in \text{Sd}_2 \wedge x, y \in L_{n+1} \rightarrow \exists_{d \in \text{Sd}} \exists_{j \in \text{Sd}_2} \exists_{x', y' \in L_n} \left(\frac{x+y+i}{4} = \frac{\frac{x'+y'+j}{4} + d}{2} \right).$$

PROOF. Let $i \in \text{Sd}_2$ and $x, y \in L_{n+1}$. By Lemma 5.3.3 we can write $x = \frac{x'+d}{2}$ and $y = \frac{y'+e}{2}$ for some $d, e \in \text{Sd}$ and $x', y' \in L_n$. Then

$$\frac{x+y+i}{4} = \frac{x'+y'+d+e+2i}{8}.$$

Since $|d+e+2i| \leq 6$ we can write $d+e+2i = j+4k$ with $|j| \leq 2$ and $|k| \leq 1$ by the JK-property (31). Therefore

$$\frac{x+y+i}{4} = \frac{x'+y'+j+4k}{8} = \frac{\frac{x'+y'+j}{4} + k}{2}. \quad \square$$

The extracted term **cLAvcSatLC1** has type $\mathbb{D}_2 \times \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{D} \times \mathbb{D}_2 \times \mathbb{L} \times \mathbb{L}$ and satisfies

$$\mathbf{cLAvcSatLC1}\langle i, d :: u, e :: v \rangle = \langle K(d + e + 2i), J(d + e + 2i), u, v \rangle.$$

By induction from Lemma 5.3.5 we obtain

LEMMA 5.3.6 (LAvcToL). $n \in T_{\mathbb{N}} \rightarrow i \in \text{Sd}_2 \wedge x, y \in L_n \rightarrow \frac{x+y+i}{4} \in L_n$.

PROOF. By induction on n . *Base.* Assume $i \in \text{Sd}_2$ and $x, y \in L_0$. Then $|x|, |y| \leq 1$ by Lemma 5.3.2, hence $\frac{x+y+i}{4} \in L_0$ by the first clause of L . *Step.* Assume $i \in \text{Sd}_2$ and $x, y \in L_{n+1}$. By Lemma 5.3.5 we can write

$$\frac{x + y + i}{4} = \frac{\frac{x' + y' + j}{4} + d}{2}$$

with $x', y' \in L_n$, $j \in \text{Sd}_2$ and $d \in \text{Sd}$. Now we can apply the second clause of L , using the IH to obtain $x', y' \in L_n$ and then compatibility of L . $\square$

The extracted term **cLAvcToL** has type $\mathbb{N} \rightarrow \mathbb{D}_2 \times \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L}$ and is defined by recursion over $\mathbb{N}$. It satisfies

$$\begin{aligned} \mathbf{cLAvcToL}(0, \langle i, u, v \rangle) &= U, \\ \mathbf{cLAvcToL}(n + 1, \langle i, u, v \rangle) &= d :: \mathbf{cLAvcToL}(n, w) \end{aligned}$$

where

$$\langle d, w \rangle = \mathbf{cLAvcSatLC1}\langle i, u, v \rangle.$$

THEOREM 5.3.7 (LAverage). $n \in T_{\mathbb{N}} \rightarrow x, y \in L_{n+1} \rightarrow \frac{x+y}{2} \in L_n$.

PROOF. Immediate by Lemma 5.3.4 and Lemma 5.3.6. $\square$

The extracted term **cLAverage** has type $\mathbb{N} \rightarrow \mathbb{L} \rightarrow \mathbb{L} \rightarrow \mathbb{L}$. It satisfies

$$\mathbf{cLAverage}(n, u, v) = \mathbf{cLAvcToL}(n, \mathbf{cLAvToAvc}(u, v)).$$

The way **cLAverage** operates can be understood as follows.

- From $u, v \in \mathbb{L}$ form the initial triple $\mathbf{cLAvToAvc}(u, v) \in \mathbb{D}_2 \times \mathbb{L} \times \mathbb{L}$.
- Recall that **cLAvcSatLC1** has type $\mathbb{D}_2 \times \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{D} \times \mathbb{D}_2 \times \mathbb{L} \times \mathbb{L}$. Iterate it n times, starting with $\mathbf{cLAvToAvc}(u, v)$.
- Return the list of generated $d \in \mathbb{D}$.

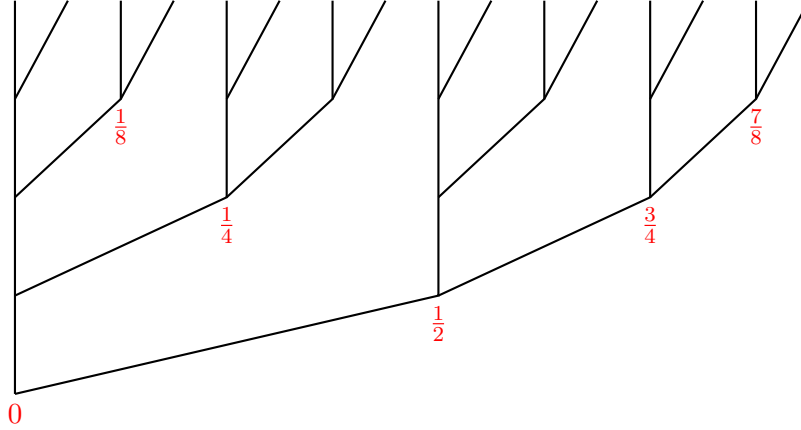
The soundness proof is within TCF and can be automatically generated with **add-sound**; see **sdindav.scm** (on the webpage of the course).

With the same method one can also treat other functions in exact real arithmetic. For instance, recently Nils Köpp proved

$$\begin{aligned} x \in L_{n+5} &\rightarrow x^2 \in L_n, \\ x, y \in L_{n+6} &\rightarrow xy \in L_n. \end{aligned}$$

REMARK. For a lookahead result like Theorem 5.3.7 it is essential to work with *signed* digits $-1, 0, 1$ rather than ordinary digits $0, 1$. To see this we sketch an attempt to only consider real numbers $x \geq 0$ and their stream representations with ordinary digits.

It will be helpful to work with *dyadic* rationals, whose denominator is a power of two. Dyadic rationals in $[0, 1]$ can be easily pictured:



Real numbers in $[0, 1]$ can be seen as infinite paths in this tree.

Note that this representation is unique if we forbid trailing 1's: replace $d_0 \dots d_{n-1} 01^\infty$ by $d_0 \dots d_{n-1} 10^\infty$. However, to identify trailing 1's requires the "Limited Principle of Omniscience" (LPO) and hence is not possible constructively.

A more severe problem is the lack of "productivity": what is the first digit when forming say the average of two such streams? As an example consider stream representations of $1/3$ and $2/3$. The task is to compute the first digit of their average.

```
;; Approximation of (1#3) from below:
(pp (nt (pt "DyToSds(05#16)"))) ;SdM::SdR::SdM::SdR:
;; Approximation of (1#3) from above:
(pp (nt (pt "DyToSds(11#32)"))) ;SdM::SdR::SdM::SdR::SdR:
```

The representations of the two approximations of $1/3$ have 4 common digits.

```
;; Approximation of (2#3) from below:
(pp (nt (pt "DyToSds(21#32)"))) ;SdR::SdM::SdR::SdM::SdR:
;; Approximation of (2#3) from above:
(pp (nt (pt "DyToSds(43#64)"))) ;SdR::SdM::SdR::SdM::SdR::SdR:
```

The representations of the two approximations of $2/3$ have 5 common digits.

Form the average of the two approximations from below:

```
(pp (nt (pt "DyToSds((1#2)*((05#16)+(21#32)))"))) ;SdM::...
```

Form the average of the two approximations from above:

```
(pp (nt (pt "DyToSds((1#2)*((11#32)+(43#64)))")) ;SdR::...
```

The representations of the averages of the approximations differ in the first digit already.