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 $d_0, d_1, d_2 \ldots$ represents the real number

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

We are interested in formally verified algorithms on real numbers in an arbitrary format. To this end we generate such algorithms as extracted terms $\mathrm{et}(M)$ 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 ${}^{\mathrm{co}}I$ coinductively defined in such a way that the computational content of $x \in {}^{\mathrm{co}}I$ 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 $M\colon \mathbb{Z}^+ \to \mathbb{N}$ such that $(a_n)_n$ is a *Cauchy sequence* with modulus M, that is

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

and M is weakly increasing (that is $M(p) \le M(q)$ for $p \le q$). 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 $\max\{\, |a_n| \mid n \le n_0 \,\} + \frac{1}{2} \le 2^{p_x}$. Then $|a_n| \le 2^{p_x}$ for all n. □

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

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

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

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

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) $\forall_p \exists_{n_0} \forall_{n \ge n_0} (-\frac{1}{2^p} \le a_n)$.

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

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

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

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

The claim follows, because this holds for every q. □

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. □

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

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

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 $x \in_{q+1} \mathbb{R}^+$. □

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 $x = y$. □

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	$L(p)$
$x + y$	$a_n + b_n$	$\max\big(M(p+1), N(p+1)\big)$
$-x$	$-a_n$	$M(p)$
$\lvert x\rvert$	$\lvert a_n\rvert$	$M(p)$
$x \cdot y$	$a_n \cdot b_n$	$\max\big(M(p+1+p_y), N(p+1+p_x)\big)$
$\frac{1}{x}$ 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 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 $n, m \geq \max\big(M(p+1+p_y), N(p+1+p_x)\big)$.

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

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

The claim now follows from the assumption that M is weakly increasing. □

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

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

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

PROOF. For $0 < |x| \to x \cdot \frac{1}{x} = 1$ 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. □

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 $x = y \to x + z = y + z$. But this follows immediately from Lemma 5.1.3 (RealEqChar): the n_0 for the conclusion can be the same as for the premise. □

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 $\frac{1}{2^{p+1}} \leq |a_n|$. □

LEMMA 5.1.15. *For reals x, y,*

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

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 $|a_n| \leq \frac{1}{2^p}$. □

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,*

$$x \le x \qquad x \not< x$$
$$x \le y \to y \le x \to x = y \qquad x < y \to y < z \to x < z$$
$$x \le y \to y \le z \to x \le z \qquad x < y \to x + z < y + z$$
$$x \le y \to x + z \le y + z \qquad x < y \to 0 < z \to x \cdot z < y \cdot z$$
$$x \le y \to 0 \le z \to x \cdot z \le y \cdot z$$

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 explicitely. Here are two examples.

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

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

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

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 $\le$ on the reals, we have:

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

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

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

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 $z \le y$ or $x \le z$.*

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) $\frac{1}{2^p} \le b_n - a_n$ 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 $l \geq m$:

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

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 $x, y \leq z \to \max(x, y) \leq z$. 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 $m := \max\big(M(p+1), N(p+1)\big)$.

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 ${}^{\mathrm{co}}I$. We model infinite sequences of signed digits (streams) as objects in the algebra $\mathbb{S}(\mathbb{D}) := \mu_\xi(\mathrm{C}\colon \mathbb{D} \to \xi \to \xi)$, where $\mathbb{D} := \mu_\xi(\mathrm{SdR}\colon \xi, \mathrm{SdM}\colon \xi, \mathrm{SdL}\colon \xi)$ is a 3-element variant of the booleans $\mathbb{B}$. Such streams will appear as realizers of an inductive predicate I defined by the single clause

$$\forall_{d,x',x}(d \in \mathrm{Sd} \to x' \in I \to x = \frac{x'+d}{2} \to x \in I). \tag{17}$$

Here (and later) x ranges 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., $|d| \le 1$. We have chosen (17) rather than the simpler

$$\forall_{d,x}(d \in \mathrm{Sd} \to x \in I \to \frac{x+d}{2} \in I), \tag{18}$$

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

$$\forall_{x,y}(x = y \to x \in I \to y \in I), \tag{19}$$

which easily follows from (17) (with reflexivity, symmetry and transitivity of $=$). Using (19) we then obtain (18) from (17) as a lemma.

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

$$x \in {}^{\mathrm{co}}I \to \exists_{d,x',y}(d \in \mathrm{Sd} \land x' \in {}^{\mathrm{co}}I \land y = \frac{x'+d}{2} \land x = y).$$

Similar to what was done above it can be simplified to

$$x \in {}^{\mathrm{co}}I \to \exists_{d,x'}(d \in \mathrm{Sd} \land x' \in {}^{\mathrm{co}}I \land x = \frac{x'+d}{2}). \tag{20}$$

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 89, 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. $|x| \le 1 \to x \in {}^{\mathrm{co}}I$.

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

$$|x| \le 1 \to \exists_{d,x'}(d \in \mathrm{Sd} \land (x' \in {}^{\mathrm{co}}I \lor |x'| \le 1) \land x = \frac{x'+d}{2}).$$

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

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

$$f \in T \to M \in T \to x \equiv (f, M) \to x \in \mathrm{Real} \to |x| \le 1 \to x \in {}^{\mathrm{co}}I$$

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

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

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

Here g is a function of type $\mathbb{Q} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{B}$ 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. Following Berger and Seisenberger (2010) we begin with an informal proof of Theorem 5.2.2 below. The computational content of this proof will be the desired algorithm.

THEOREM 5.2.2. *The average of two real numbers x, y in ${}^{\mathrm{co}}I$ is in ${}^{\mathrm{co}}I$:*

$$\forall_{x,y \in {}^{\mathrm{co}}I}\Big(\frac{x+y}{2} \in {}^{\mathrm{co}}I\Big).$$

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

$$P := \{\, \frac{x+y}{2} \mid x, y \in {}^{\mathrm{co}}I \,\}, \qquad Q := \{\, \frac{x+y+i}{4} \mid x, y \in {}^{\mathrm{co}}I, i \in \mathrm{Sd}_2 \,\},$$

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

$$x \in Q \to \exists_{d,x'}(d \in \mathrm{Sd} \land x' \in Q \land x = \frac{x'+d}{2}),$$

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

LEMMA 5.2.3. $x, y \in {}^{\mathrm{co}}I \to \exists_{i,x',y'}(i \in \mathrm{Sd}_2 \land x', y' \in {}^{\mathrm{co}}I \land \frac{x+y}{2} = \frac{x'+y'+i}{4})$.

PROOF. By (20). The extracted term has type $\mathbb{S}(\mathbb{D}) \to \mathbb{S}(\mathbb{D}) \to \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D})$; it maps $(\mathrm{C}_d(u), \mathrm{C}_e(v))$ into $(d+e, u, v)$. □

The main part of the proof consists in showing

$$\begin{aligned} &i \in \mathrm{Sd}_2 \to x, y \in {}^{\mathrm{co}}I \to \\ &\exists_{j,d,x',y'}(j \in \mathrm{Sd}_2 \land d \in \mathrm{Sd} \land x', y' \in {}^{\mathrm{co}}I \land \frac{x+y+i}{4} = \frac{\frac{x'+y'+j}{4} + d}{2}). \end{aligned} \tag{21}$$

PROOF. By (20) we can write $x = \frac{x'+d}{2}$ and $y = \frac{y'+e}{2}$ with $d, e \in \mathrm{Sd}$ and $x', y' \in {}^{\mathrm{co}}I$. Then $\frac{x+y+i}{4} = \frac{x'+y'+d+e+2i}{8}$. Since $|d+e+2i| \le 6$ we can write

$d+e+2i = j+4k$ with $|j| \le 2$ and $|k| \le 1$. Therefore

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

Hence we have $q\colon \mathbb{D}_2 \to \mathbb{S}(\mathbb{D}) \to \mathbb{S}(\mathbb{D}) \to \mathbb{D}_2 \times \mathbb{D} \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D})$ defined by $q(i, \mathrm{C}_d(u), \mathrm{C}_e(v)) := (J(d+e+2i), K(d+e+2i), u, v)$, where $J, K\colon \mathbb{Z} \to \mathbb{Z}$ with $\forall_i(|J(i)| \le 2)$, $\forall_i(|i| \le 6 \to |K(i)| \le 1))$ and $\forall_i(i = J(i) + 4K(i))$. □

By coinduction from (21) we obtain

LEMMA 5.2.4. $\exists_{i,x,y}(i \in \mathrm{Sd}_2 \land x, y \in {}^{\mathrm{co}}I \land z = \frac{x+y+i}{4}) \to z \in {}^{\mathrm{co}}I$.

Theorem 5.2.2 is an immediate consequence of Lemmata 5.2.3 and 5.2.4. Its proof gives a function $\mathrm{Av}\colon \mathbb{D}_2 \times \mathbb{S}(\mathbb{D}) \times \mathbb{S}(\mathbb{D}) \to \mathbb{S}(\mathbb{D})$ defined corecursively by $\mathrm{Av}(i, \mathrm{C}_d(v), \mathrm{C}_e(w)) = \mathrm{C}_{K(d+e+2i)}(\mathrm{Av}(J(d+e+2i), v, w))$. More precisely, Lemma 5.2.3 computes the first "carry" $i \in \mathrm{Sd}_2$ and the tails of the inputs. Then Av is called repeatedly, computing the average step by step. For the first n digits in the Sd-representation of $\frac{x+y}{2}$ we need the first $n+1$ digits in the Sd-representations of x and y.

5.2.4. Division for signed digit streams. We finally prove that $[-1, 1]$ is closed under division, w.r.t. the representation of reals as signed digit streams. Using ideas from Ciaffaglione and Gianantonio (2006), we will reduce this problem to the one for the average function.

For division $\frac{x}{y}$ we clearly need a restriction on the denominator y to stay in the interval $[-1, 1]$, and must assume that $|y|$ is strictly positive. For simplicity we assume $\frac{1}{4} \le y$; this can easily be extended to the case $2^{-p} \le y$ (using induction on p and Lemma 5.2.6 below). The main idea of the algorithm and also of the proof consists in three representations of $\frac{x}{y}$:

$$\frac{x}{y} = \frac{1+\frac{x_1}{y}}{2} = \frac{0+\frac{x_0}{y}}{2} = \frac{-1+\frac{x_{-1}}{y}}{2}$$

where

$$x_1 = 4\frac{x+\frac{-y}{2}}{2}, \quad x_0 = 2x, \quad x_{-1} = 4\frac{x+\frac{y}{2}}{2}.$$

Depending on what we know about x we choose one of these representations of $\frac{x}{y}$ to obtain its first digit. This will give us a corecursive definition of $\frac{x}{y}$.

LEMMA 5.2.5 (CoINegToCoIPlusOne, CoIPosToCoIMinusOne). *${}^{\mathrm{co}}I$ is closed under shifting a real $x \le 0$ ($x \ge 0$) by $+1$ (-1):*

$$\forall_{x \in {}^{\mathrm{co}}I}(x \le 0 \to x+1 \in {}^{\mathrm{co}}I),$$
$$\forall_{x \in {}^{\mathrm{co}}I}(0 \le x \to x-1 \in {}^{\mathrm{co}}I).$$

PROOF. We only consider the first claim; the second is proved similarly. The proof uses coinduction on ${}^{\mathrm{co}}I$ with $P := \{\, x \mid \exists_{y\in{}^{\mathrm{co}}I}(y \le 0 \land x = y+1)\,\}$ the competitor predicate. It suffices to prove the step formula

$$\forall_x\Big(\exists_{y\in{}^{\mathrm{co}}I}(y \le 0 \land x = y+1) \to \exists_{d\in\mathrm{Sd},x'\in{}^{\mathrm{co}}I\cup P}\Big(|x| \le 1 \land x = \frac{d+x'}{2}\Big)\Big).$$

Let x, y be given with $y \in {}^{\mathrm{co}}I$, $y \le 0$ and $x = y+1$. From $y \in {}^{\mathrm{co}}I$ we know $|y| \le 1$ and with $y \le 0$ also $|x| \le 1$. We need $d \in \mathrm{Sd}$ and x' such that

$$(x' \in {}^{\mathrm{co}}I \vee \exists_{y\in{}^{\mathrm{co}}I}(y \le 0 \land x' = y+1)) \land x = \frac{d+x'}{2}.$$

Again from $y \in {}^{\mathrm{co}}I$ we obtain $e \in \mathrm{Sd}$ and $z \in {}^{\mathrm{co}}I$ with $y = \frac{e+z}{2}$. We now distinguish cases on $e \in \mathrm{Sd}$.

Case $e = 1$. Then $0 \ge y = \frac{1+z}{2} \ge \frac{1}{2} - \frac{1}{2} = 0$ and hence $x = y+1 = 1$. Picking $d = 1$ and $x' = 1$ gives the claim. Here we need a lemma `CoIOne` stating that 1 is in ${}^{\mathrm{co}}I$. The proof of this lemma (by coinduction) is omitted.

Case $e = 0$. Pick $d = 1$ and $x' = z+1$. Then $z = 2y \le 0$ and hence the r.h.s. of the disjunction above holds with z for y. Also $x = 2y = \frac{1+2y+1}{2}$.

Case $e = -1$. Pick $d = 1$ and $x' = z$. Then the l.h.s. of the disjunction above holds, and $\frac{d+x'}{2} = \frac{1+z}{2} = \frac{-1+z}{2} + 1 = y+1 = x$. □

We have formalized this proof M in the Minlog[1] proof assistant. Minlog has a tool to extract from the proof M the term $\mathrm{et}(M)$ representing the computational content of the proof M. This term is displayed as

```
[u](CoRec ai=>ai)u
 ([u0][case (DesYprod u0)
     (s pair u1 -> [case s
       (SdR -> SdR pair InL cCoIOne)
       (SdM -> SdR pair InR u1)
       (SdL -> SdR pair InL u1)])])
```

Here `[u]` means lambda abstraction λ_u, and `(CoRec ai=>ai)` is the corecursion operator ${}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbb{I}}$ defined above, where τ is $\mathbb{I}$ again. The type of ${}^{\mathrm{co}}\mathcal{R}^{\mathbb{I}}_{\mathbb{I}}$ is $\mathbb{I} \to (\mathbb{I} \to \mathbb{D} \times (\mathbb{I} + \mathbb{I})) \to \mathbb{I}$. The first argument of the corecursion operator is the abstracted variable `u` of type $\mathbb{I}$, and the second `([u0][case ...])` is the "step" function, which first destructs its argument `u0` into a pair of a signed digit `s` and another stream `u1`, and then distinguishes cases on `s`. In the `SdR` case the returned pair of type $\mathbb{D} \times (\mathbb{I} + \mathbb{I})$ has `SdR` again as its left component, and as right component the InL (left embedding into a sum

[1]The development described here resides in the dev branch of Minlog, in the directory `minlog/examples/analysis`, files `sddiv.scm` and `graydiv.scm`

type) of a certain stream denoted `cCoIOne`. This is the computational content (hence the "`c`") of `CoIOne`, essentially an infinite sequence of the digit SdR (written $\vec{1}$).

The algorithm represented by $\mathrm{et}(M)$ can be understood as follows. If $s = \mathrm{SdR}$, then y must be non-negative. Hence $y = 0$, and a stream-representation of $y + 1$ is $\vec{1}$. Here we do not need a corecursive call, and hence the result is $\langle \mathrm{SdR}, \mathrm{InL}(\vec{1}\,)\rangle$. The same happens in case $s = \mathrm{SdL}$. Here $y + 1$ can be determined easily by changing the first digit from SdL to SdR and leaving the tail as it is. Hence the result is $\langle \mathrm{SdR}, \mathrm{InL}(u')\rangle$. Only in case $s = \mathrm{SdM}$ we have a corecursive call. Here we change the first digit from SdM to SdR, which however amounts to adding $\frac{1}{2}$ only. Therefore the procedure continues with the tail. Hence the result is $\langle \mathrm{SdR}, \mathrm{InR}(u')\rangle$. Using the computation rule for ${}^{\mathrm{co}}\mathcal{R}^{\mathbb{I}}_{\mathbb{I}}$ we can now describe the computational content as a function $f\colon \mathbb{I} \to \mathbb{I}$ defined by

$$\begin{aligned} f(\mathrm{SdR} :: u) &:= [\mathrm{SdR}, \mathrm{SdR}, \dots], \\ f(\mathrm{SdM} :: u) &:= \mathrm{SdR} :: f(u), \\ f(\mathrm{SdL} :: u) &:= \mathrm{SdR} :: u. \end{aligned}$$

A similar argument for the second part of the lemma gives $g\colon \mathbb{I} \to \mathbb{I}$ with

$$\begin{aligned} g(\mathrm{SdR} :: u) &:= \mathrm{SdL} :: u, \\ g(\mathrm{SdM} :: u) &:= \mathrm{SdL} :: g(u), \\ g(\mathrm{SdL} :: u) &:= [\mathrm{SdL}, \mathrm{SdL}, \dots]. \end{aligned}$$

LEMMA 5.2.6. *For x in ${}^{\mathrm{co}}I$ with $|x| \le \frac{1}{2}$ we have $2x$ in ${}^{\mathrm{co}}I$:*

$$\forall_{x \in {}^{\mathrm{co}}I}\Big(|x| \le \frac{1}{2} \to 2x \in {}^{\mathrm{co}}I\Big).$$

PROOF. Let $x \in {}^{\mathrm{co}}I$ be given. From the closure axiom for ${}^{\mathrm{co}}I$ we obtain $d \in \mathrm{Sd}$ and $x' \in {}^{\mathrm{co}}I$ such that $x = \frac{d+x'}{2}$. We distinguish cases on $d \in \mathrm{Sd}$.

Case $d = 1$. Then $x = \frac{1+x'}{2}$ and hence $2x = 1 + x'$. Since $|x| \le \frac{1}{2}$ we have $x' \le 0$. Now the first part of Lemma 5.2.5 gives the claim.

Case $d = 0$. Then $x = \frac{0+x'}{2}$ and hence $2x = x' \in {}^{\mathrm{co}}I$.

Case $d = -1$. Then $x = \frac{-1+x'}{2}$ and hence $2x = -1 + x'$. Since $|x| \le \frac{1}{2}$ we have $0 \le x'$. Now the second part of Lemma 5.2.5 gives the claim. □

Using arguments similar to those in the remark after Lemma 5.2.5 we can see that the corresponding algorithm can be written as a function

Double: $\mathbb{I} \to \mathbb{I}$ with

$$\begin{aligned}\mathrm{Double}(\mathrm{SdR} :: u) &:= f(u),\\ \mathrm{Double}(\mathrm{SdM} :: u) &:= u,\\ \mathrm{Double}(\mathrm{SdL} :: u) &:= g(u)\end{aligned}$$

where f and g are the functions from this remark.

LEMMA 5.2.7. *For x, y in ${}^{\mathrm{co}}I$ with $\frac{1}{4} \le y$, $|x| \le y$ and $0 \le x$ ($x \le 0$) we have $2x - y$ ($2x + y$) in ${}^{\mathrm{co}}I$:*

$$\forall_{x,y\in{}^{\mathrm{co}}I}\Big(\frac{1}{4} \le y \to |x| \le y \to 0 \le x \to 4\frac{x + \frac{-y}{2}}{2} \in {}^{\mathrm{co}}I\Big),$$
$$\forall_{x,y\in{}^{\mathrm{co}}I}\Big(\frac{1}{4} \le y \to |x| \le y \to x \le 0 \to 4\frac{x + \frac{y}{2}}{2} \in {}^{\mathrm{co}}I\Big).$$

PROOF. We essentially use the function $\mathrm{Av}\colon \mathbb{I} \to \mathbb{I} \to \mathbb{I}$ extracted from the proof of Theorem 5.2.2. In the formulas above instead of $2x \pm y$ we have written $4\frac{x+(\pm y/2)}{2}$ to make Theorem 5.2.2 applicable. We also use two lemmas stating that ${}^{\mathrm{co}}I$ is closed under $x \mapsto \frac{x}{2}$ and $x \mapsto -x$. To prove the first claim, let x, y in ${}^{\mathrm{co}}I$ with $\frac{1}{4} \le y$, $|x| \le y$ and $0 \le x$. Then clearly $\frac{-y}{2} \in {}^{\mathrm{co}}I$, and $\frac{x+\frac{-y}{2}}{2} \in {}^{\mathrm{co}}I$ by Theorem 5.2.2. We have

$$\Big|\frac{x + \frac{-y}{2}}{2}\Big| = \Big|\frac{2x - y}{4}\Big| \le \Big|\frac{2y - y}{4}\Big| = \Big|\frac{y}{4}\Big| \le \frac{1}{4}. \tag{22}$$

Hence we can apply Lemma 5.2.6 twice and obtain $4\frac{x+\frac{-y}{2}}{2} \in {}^{\mathrm{co}}I$. The proof of the second claim is similar. □

The computational content of the proofs is $\mathrm{AuxL}, \mathrm{AuxR}\colon \mathbb{I} \to \mathbb{I} \to \mathbb{I}$:

$$\begin{aligned}\mathrm{AuxL}(u, v) &:= \mathrm{Double}(\mathrm{Double}(\mathrm{Av}(u, h(n(v))))),\\ \mathrm{AuxR}(u, v) &:= \mathrm{Double}(\mathrm{Double}(\mathrm{Av}(u, h(v)))).\end{aligned}$$

Here $h, n\colon \mathbb{I} \to \mathbb{I}$ represent the computational content of the two lemmas used in the proof; both are proved by coinduction. The function h prepends SdM to the stream, and n negates all digits:

$$h(u) := \mathrm{SdM} :: u, \qquad \begin{aligned} n(\mathrm{SdR} :: u) &:= \mathrm{SdL} :: n(u),\\ n(\mathrm{SdM} :: u) &:= \mathrm{SdM} :: n(u),\\ n(\mathrm{SdL} :: u) &:= \mathrm{SdR} :: n(u).\end{aligned}$$

THEOREM 5.2.8. *For x, y in ${}^{\mathrm{co}}I$ with $\frac{1}{4} \le y$ and $|x| \le y$ we have $\frac{x}{y}$ in ${}^{\mathrm{co}}I$:*

$$\forall_{x,y\in{}^{\mathrm{co}}I}\Big(\frac{1}{4} \le y \to |x| \le y \to \frac{x}{y} \in {}^{\mathrm{co}}I\Big).$$

PROOF. The proof uses coinduction on ${}^{\mathrm{co}}I$ with $P := \{\, z \mid \exists_{x,y\in{}^{\mathrm{co}}I}(|x| \le y \land \frac{1}{4} \le y \land z = \frac{x}{y})\,\}$. It suffices to prove the step formula

$$\forall_z\Big(\exists_{x,y\in{}^{\mathrm{co}}I}\Big(|x| \le y \land \frac{1}{4} \le y \land z{=}\frac{x}{y}\Big) \to \exists_{d\in\mathrm{Sd},z'\in{}^{\mathrm{co}}I\cup P}\Big(|z| \le 1 \land z{=}\frac{d+z'}{2}\Big)\Big).$$

Let x, y, z be given with $x, y \in {}^{\mathrm{co}}I$, $|x| \le y$, $\frac{1}{4} \le y$ and $z = \frac{x}{y}$. From $|x| \le y$ we have $z \le 1$. By a trifold application of the closure axiom to x we obtain $d_1, d_2, d_3 \in \mathrm{Sd}$ and $\tilde{x} \in {}^{\mathrm{co}}I$ such that $x = \frac{4d_1+2d_2+d_3+\tilde{x}}{8}$ or $x = d_1d_2d_3\tilde{x}$ for short. We now distinguish three cases.

If $x = 1d_2d_3\tilde{x}$, $x = 01d_3\tilde{x}$ or $x = 001\tilde{x}$, then $0 \le x$. Pick $d = 1$ and $z' = \frac{x'}{y}$ with $x' = 4\frac{x+\frac{-y}{2}}{2}$. Then $x' \in {}^{\mathrm{co}}I$ by Lemma 5.2.7. From (22) we also obtain $|x'| \le y$ and hence $z' \in P$. One can easily check that $z = \frac{1+z'}{2}$.

If $x = \bar{1}d_2d_3\tilde{x}$, $x = 0\bar{1}d_3\tilde{x}$ or $x = 00\bar{1}\tilde{x}$, then $x \le 0$. Pick $d = -1$ and $z' = \frac{x'}{y}$ with $x' = 4\frac{x+\frac{y}{2}}{2}$. We can then proceed as in the first case.

The final case is $x = 000\tilde{x}$. Then $|x| \le \frac{1}{8}$; pick $d = 0$ and $z' = \frac{x'}{y}$ with $x' = 2x$. We obtain $|x'| \le \frac{1}{4} \le y$ and with Lemma 5.2.6 also $x' \in {}^{\mathrm{co}}I$. Therefore $z' \in P$, and $z = \frac{z'}{2}$ is easily checked. □

The term Minlog extracts is displayed in Figure 2.

```
[u,u0](CoRec ai=>ai)u
 ([u1][case (cCoIClosure u1)
   (s pair u2 -> [case s
     (SdR -> SdR pair InR(cCoIDivSatCoIClAuxR u1 u0))
     (SdM -> [case (cCoIClosure u2)
       (s0 pair u3 -> [case s0
        (SdR -> SdR pair InR(cCoIDivSatCoIClAuxR u1 u0))
        (SdM -> [case (cCoIClosure u3)
         (s1 pair u4 -> [case s1
          (SdR -> SdR pair InR(cCoIDivSatCoIClAuxR u1 u0))
          (SdM -> SdM pair InR(cCoIToCoIDouble u1))
          (SdL -> SdL pair InR(cCoIDivSatCoIClAuxL u1 u0))])])
        (SdL -> SdL pair InR(cCoIDivSatCoIClAuxL u1 u0))])])
     (SdL -> SdL pair InR(cCoIDivSatCoIClAuxL u1 u0))])])
```

FIGURE 1. Extracted term for Theorem 5.2.8.

The three occurrences of `cCoIClosure` correspond to the trifold application of the closure axioms to x. The seven cases $x = 1d_2d_3\tilde{x}$, $x = 01d_3\tilde{x}$, $x =$

$001\tilde{x}$, $x = 000\tilde{x}$, $x = \bar{1}d_2d_3\tilde{x}$, $x = 0\bar{1}d_3\tilde{x}$ and $x = 00\bar{1}\tilde{x}$ are clearly visible. In the first three cases `SdR` corresponds to picking $d = 1$ and usage of the AuxR function from Lemma 5.2.7, and similarly in the last three cases `SdL` corresponds to picking $d = -1$ and usage of AuxL. In the middle case `SdM` corresponds to $d = 0$; there we use the computational content of Lemma 5.2.6. We can describe the extracted term by a function $\mathrm{Div}\colon \mathbb{I} \to \mathbb{I} \to \mathbb{I}$ corecursively defined by

$$\mathrm{Div}(u,v) := \begin{cases} \mathrm{SdR} :: \mathrm{Div}(\mathrm{AuxR}(u,v),v) & \text{if } u = 1\tilde{u} \vee u = 01\tilde{u} \vee u = 001\tilde{u}, \\ \mathrm{SdM} :: \mathrm{Div}(\mathrm{Double}(u),v) & \text{if } u = 000\tilde{u}, \\ \mathrm{SdL} :: \mathrm{Div}(\mathrm{AuxL}(u,v),v) & \text{if } u = \bar{1}\tilde{u} \vee u = 0\bar{1}\tilde{u} \vee u = 00\bar{1}\tilde{u}. \end{cases}$$

We use this description of the extracted term to see how far we have to look into u and v to determine the first n entries of $\mathrm{Div}(u,v)$. To this end we write the above equation as

$$\mathrm{Div}(u,v) = d(u) :: \mathrm{Div}(G(u,v),v),$$

where $d(u)$ depends on the first three digits of u, and $G(u,v)$ is one of $\mathrm{AuxR}(u,v)$, $\mathrm{Double}(u)$ or $\mathrm{AuxL}(u,v)$, according to the present case. Recall

$$\begin{aligned} \mathrm{AuxL}(u,v) &:= \mathrm{Double}(\mathrm{Double}(\mathrm{Av}(u,h(n(v))))), \\ \mathrm{AuxR}(u,v) &:= \mathrm{Double}(\mathrm{Double}(\mathrm{Av}(u,h(v)))). \end{aligned}$$

By the equations for n, h, Av and Double we see that the first n entries of

$n(u)$	need the first n entries of u,
$h(u)$	need the first $n-1$ entries of u,
$\mathrm{Av}(u,v)$	need the first $n+1$ entries of u and v,
$\mathrm{Double}(u)$	need the first $n+1$ entries of u.

Hence $\mathrm{AuxR}(u,v)$, $\mathrm{AuxL}(u,v)$ and $G(u,v)$ all need at most the first $n+3$ entries of u and $n+2$ entries of v. Iterating the above equation for G gives for $\mathrm{Div}(u,v)$ the representation

$$d(u) :: d(G(u,v)) :: d(G(G(u,v),v)) :: d(G(G(G(u,v),v),v),v) \ldots$$

Therefore the first n entries of $\mathrm{Div}(u,v)$ depend on at most the first $3n$ entries of u and the first $3n-1$ entries of v.