Abstract

Digital computers permeate our physical world. This phenomenon creates a pressing need for tools that help us understand a priori how digital computers can affect their physical environment. In principle, simulation can be a powerful tool for animating models of the world. Today, however, there is not a single simulation environment that comes with a guarantee that the results of the simulation are determined purely by a real-valued model and not by artifacts of the digitized implementation. As such, simulation with guaranteed fidelity does not yet exist.

Towards addressing this problem, we offer an expository account of what is known about exact real arithmetic. We argue that this technology, which has roots that are over 200 years old, bears significant promise as offering exactly the right technology to build simulation environments with guaranteed fidelity. And while it has only been sparsely studied in this large span of time, there are reasons to believe that the time is right to accelerate research in this direction.

1. Introduction

In the embedded systems community it is widely recognized that digital computers are permeating our physical world. Recently, there has been a growing consensus that this phenomenon of cyber-physical systems may require not only new tools but also new foundations to enable an effective understanding of such systems. In particular, there is a pressing need for methods that can provide us with useful, a priori accounts of how digital computers would affect a physical environment in which they are embedded.

In principle, simulation can serve as a powerful stride towards this goal. Unfortunately, no mainstream simulation environment available today comes with a clear, rigorous guarantee that would assure us that the results of the simulation are determined purely by a real-valued model and not by artifacts of the digitized implementation. Simulation tools with guaranteed fidelity do not yet exist.

The absence of such fidelity is a concern both in engineering and in science. When building safety critical systems, one would like to know that a behavior that appears possible in a simulation is indeed physically possible and not a result of numerical anomalies. In science, fidelity is absolutely essential for scientists to quickly determine whether an artifact in a physical simulation is a true phenomenon in the model or merely an artifact of the underlying implementation. Fidelity is also essential for the reproducibility of results.

For a simulation tool to provide fidelity guarantees it must be grounded in the mathematical study of real num-
bers, namely real analysis. This is, in essence, implied by the definition of what we want: To specify the correctness of an implementation, we need to use ideas from real analysis about approximations of increasing precision. Then, once we get into the details of the computation, and as we will get to see in some of the examples in this paper, we find that some fundamental truths about real-numbers (such as the undecidability of equality) cannot be avoided when we talk about high fidelity guarantees.

Exact real computation can be approached in several ways. A direct approach would be to compute explicitly with intervals representing precisely what we know about a certain real value. Such intervals can be represented, for example, by a pair of rationals. Then we can imagine all other operations being defined as working on intervals and producing answers that represent all possible answers for any given exact reals. We can call this method interval arithmetic [17, 19, 20, 1, 7].

While this approach can be effective for a wide range of applications, we believe that it can suffer from a particular type of computational inefficiency. Imagine a situation where we run a large computation and we get a result of unsatisfactory precision. What input do we need to provide in greater accuracy for the precision of the output to be improved? We expect that, in general, as we compose computation, the variance of needed precisions among inputs is likely to grow more dramatically, and as a result, only a very small number of inputs will really need to be provided in high-precision. This means that it becomes increasingly more wasteful to assume that all computation needs to be done in higher precision.

As such, we postulate that the most likely approaches to succeed in providing efficient real arithmetic computation will be based on lazy, explicit, and co-inductive (“infinite”) representations of real numbers. Because this approach only computes to the precision needed, it avoids the problem with the direct approach.

Interestingly, it appears that the lazy approach has a long history going back at least to the work of Leslie and Cauchy in the 1800s [8]. At the same time, while exact real arithmetic may have seemed too expensive and too impractical in the past, a confluence of developments makes this an appropriate time to reconsider this judgment:

- Parallel computing resources: Multi-core, grid, and cloud computing systems all offer resources that can be employed effectively by highly parallelizable computations. Exact real arithmetic computations have the same purely functional properties as many other computations that are derived directly from mathematical computations. Furthermore, the granularity of individual operations in such a setting can be sufficiently large to take up non-trivial computing units.
- Feasibility of specialized hardware: FPGA, ASICS, and a wide range of technologies make it possible, today, to experiment with new architectural designs. At the same time, there is a growing consensus that it may be time to reconsider some very basic architectural aspects of microprocessor design. A better understanding of the needs of exact real arithmetic can provide critical guidance in this process.

- More than ever, a pressing need for accuracy: Today, even though some numerical libraries may have reasonable properties in terms of accuracy, it is rare that a library comes with any formal guarantees about accuracy. Even if that is the case, there are not methods for ensuring any properties when such libraries are composed (or even iterated!) For example, it is well known that the precision of transcendental functions can be very poor and vary greatly from system to system. Not only does this make it hard to have any basis for trusting the results of such computations, it makes it virtually impossible to use such computations to evaluate analytical models.

The question, then, is what are the right principle for designing lazy representation of exact real numbers?

### 1.1 Contributions

Towards addressing this problem, we offer an expository account of what is known about exact real arithmetic.

- We explain why the standard Base-2 representation for real numbers is not satisfactory, even for addition operation. We offer an intuitive explanation for why addition is not computable in this representation (Section 2).
- We explain two methods for solving this problem. The first method is to change the meaning of zero and one (Section 3). The second method is to add extra digits (Section 4).
- We show for the two representations how can +, × and > be defined. We formalize theorems which state the soundness and effectiveness of the definitions.

Proofs of propositions and theorems can be found in Appendix.

### 2. Base-2 Representation Doesn’t Work

A real number \( r \) in \([0, 1]\) has its integer part be 0 and every digit after the binary point be either 0 or 1. The traditional interpretation takes the \( n \)-th digit \( d \) after the binary point
2.1. Expressible Intervals

In the traditional interpretation, for a finite sequence of digits \( A \), the infinite sequence 0.\( A \) ranges from 0.\( A(0)^\omega \) to 0.\( A(1)^\omega \). For example, the sequence 0.0 means \([0, \frac{1}{2}]\), the sequence 0.1 means \([\frac{1}{2}, 1]\), and the sequence 0.00 means \([0, \frac{1}{2}]\) (Figure 1). When adding two numbers where only the first few digits of the inputs are known, we add the intervals corresponding to both inputs. The sum of the interval is guaranteed to include any possible results of the addition of input numbers. For example, we have 0.000 + 0.011 \(\in\) \([\frac{3}{8}, \frac{5}{8}]\), 0.0000 + 0.0111 \(\in\) \([\frac{7}{16}, \frac{9}{16}]\). The left most digits of the result can be inferred by finding a sequence of digits, where the interval it corresponded to must contain the sum of the intervals from the input.

Recall the problem of computing the result of adding two real numbers which start as:

- 0.0000000... and 0.0111111...

If 0 keeps appearing in the first input and 1 keeps appearing in the second input, then after \( n \) pairs of 0 and 1, we would have the sum be lying in \([\frac{1}{2} - \frac{1}{2^n\pi}, \frac{1}{2} + \frac{1}{2^n\pi}]\). Now with the first digit be 0 ranges from 0 to \(\frac{1}{2}\) and 1 ranges from \(\frac{1}{2}\) to 1, the sum cannot have either 0 or 1 be its first digit. This makes the addition not computable. And the reason is because the intervals represented by 0 and 1 have only overlapped at one point. If there is a small overlap between the intervals represented by 0 and 1, a sufficient small interval should always be able to be included in one of the intervals.

2.2. Semantics

To better understand the Base-2 real representation and its operations, we give a formal definition for this representation and its interpretation. We also formally define the traditional addition operation and show that the operation is guaranteed to be correct but in many cases incomplete.

Definition 2.1 (Base-2 Real Numbers).

Let \( \mathbb{N} \) denote the set of naturals, and \( \mathbb{Q} \) denote the set of rationals. Let \( \mathbb{B} = \{0, 1\} \). Then a Base-2 real number in \([0, 1]\) can be represented as an infinite stream of type \( \mathbb{N} \rightarrow \mathbb{B} \).

Definition 2.2 (Semantics of Base-2 Real Numbers).

The semantics of any finite prefix of a real number is a function \([\cdot] : (\exists n \in \mathbb{N}. \mathbb{B}^n) \rightarrow \mathbb{Q} \) defined as follows:

\[
\begin{align*}
[x] & = [0, 1] \\
[A0] & = \text{let } [x, y] = [A] \text{ in } [x, x + \frac{1}{2}(y - x)] \\
[A1] & = \text{let } [x, y] = [A] \text{ in } [x + \frac{1}{2}(y - x), y]
\end{align*}
\]

We will use the following interval operations and relations throughout the paper:

Definition 2.3 (Basics for interval operations and relations).

\[
\begin{align*}
[x_1, y_1] + [x_2, y_2] & = [x_1 + x_2, y_1 + y_2] \\
[x_1, y_1] - [x_2, y_2] & = [x_1 - y_2, y_1 - x_2] \\
[x, y]/z & = [x/z, y/z] \\
[x_1, y_1] \subseteq [x_2, y_2] & \iff x_1 \geq x_2 \text{ and } y_1 \leq y_2 \\
[x_1, y_1] < [x_2, y_2] & \iff y_1 < x_2 \\
|x, y| \leq z & \iff \max(|x|, |y|) \leq z
\end{align*}
\]

where \(|x|\) is the absolute value of \(x\).

We can show that this interpretation converges to a real number as we look at a longer prefix:

Proposition 2.1. For any \(A \in \mathbb{B}^n\):
\[ |A| \text{ is the length of prefix } A. \]

We now define the addition operation \( \oplus \). Since we are considering real numbers in \([0, 1]\), we define \( A + B \) such that \( |A + B| \approx \frac{|A| + |B|}{2} \), where \( A, B \in (\forall n \in \mathbb{N}, \mathbb{B}^n) \). The conventional addition is defined by left shifting the results.

**Definition 2.4 (Addition of Base-2 Real Numbers).**

For any digit \( d \in \mathbb{B} \) and finite prefix \( A, B \in (\forall n \in \mathbb{N}, \mathbb{B}^n) \):

\[
\begin{align*}
A & \oplus \epsilon = \epsilon \\
\epsilon & \oplus B = \epsilon \\
dA & \oplus dB = d(A \oplus B) \\
dA & \oplus (1 - d)B = \text{add_one}(A \oplus B) \\
\text{add_one}(\epsilon) & = \epsilon \\
\text{add_one}(A) & = 10A \\
\text{add_one}(0A) & = 01A
\end{align*}
\]

**Theorem 2.1 (Correctness of Addition).**

If \( A + B \) is defined, then \( \frac{|A| + |B|}{2} \leq |A + B| \).

Theorem 2.1 says that any digits produced from the addition operation is guaranteed to be correct. In other words, when more digits are available in the input sequences, there is no need to change the digits produced before.

**Theorem 2.2.** Let \( A = A_1dA_2 \) and \( B = B_1dB_2, |A_1| = |B_1| = l \). Then \( |A + B| \geq |A| + |B| \).

Theorem 2.2 says that addition on Base-2 real numbers can generate results of certain length if we consider any natural number \( n \); the \( n \)-th digit in both input sequences are the same. Otherwise, the length of the result has no lower limit. The problem of deciding first digit in the result of \( 0.000000 \ldots + 0.01111111 \ldots \) is one such example.

### 3. Proportional Relaxation

We now formalize binary numbers with proportional relaxation (Brouwer 1920, Turing 1937). The formalization has base 0 and 1. Digit 0 means zero and digit 1 means \( \frac{1}{3} \) when it appears as the \( n \)-th digit after the binary point. The number of the real number is to add values of all the digits. Again, for a finite sequence of digits \( A \), the infinite sequence \( A \) ranges from \( 0.A(0)^{\infty} \) to \( 0.A(1)^{\infty} \). For example, the sequence 0.0 means \([0, 0\frac{2}{3})\), the sequence 0.1 means \([\frac{1}{3}, 1]\), and the sequence 0.0 means \([0, \frac{2}{3})\) (Figure 2). When adding two numbers where only their finite prefixes are known, we add the intervals corresponding to both inputs. The sum of the interval is guaranteed to include any possible results of the addition of input numbers. For example, we have 0.00 + 0.011 ∈ \([0, \frac{8}{27}] + [\frac{10}{27}, \frac{18}{27}]\). The latter one is contained in \([\frac{3}{1}, 1]\), so the result of 0.000 + 0.011 must start with 0.1.

![Figure 2. Binary Numbers with Proportional Relaxation](image)

We formally define the representation described above as follows:

**Definition 3.1 (Semantics of Binary Numbers with Proportional Relaxation).**

The semantics of any finite prefix of a real number is a function \( \lfloor . \rfloor : (\forall n \in \mathbb{N}, \mathbb{B}^n) \rightarrow \mathbb{Q} \times \mathbb{Q} \) defined as follows:

\[
\begin{align*}
\lfloor c \rfloor & = [0, 1] \\
\lfloor A \rfloor & = \text{let } [x, y] = \lfloor A \rfloor \text{ in } [x, x + \frac{1}{3}(y - x)] \\
\lfloor A \rfloor & = \text{let } [x, y] = \lfloor A \rfloor \text{ in } [x + \frac{1}{3}(y - x), y]
\end{align*}
\]

Again, this interpretation converges to a real number as we look at a longer prefix.

**Proposition 3.1.** For any \( A \in \mathbb{B}^n \):

\[
\begin{align*}
\lfloor A \rfloor & \subseteq [0, 1] \\
|\lfloor A \rfloor| & = (\frac{1}{3})^{|A|}
\end{align*}
\]

In the definition of addition of Base-2 real numbers, even the first digit of the result may not be decidable regardless of how many digits we known in the inputs. This is because some intervals cannot be expressed. If the interval stride ranges represented by 0 and 1, no matter how short the interval is, no sequence of digits can represent the results.

In binary numbers with proportional relaxation, the intervals represented by 0 and 1 are overlapped with each other. The following lemma states the relationship between the size of an interval and the number of digits that can be decided for the interval. The relationship is guaranteed by the overlap in the semantics of digits 0 and 1.

**Lemma 1.** For any rational interval \( I = [x, y] \subseteq [0, 1] \), we can find a finite sequence \( A \) such that

\[
\begin{align*}
I & \subseteq \lfloor A \rfloor \\
\frac{1}{3} |\lfloor A \rfloor| & < |I| \\
|A| & = \max\{0, \left\lceil \log_3 \frac{3}{|I|} \right\rceil + 1\}
\end{align*}
\]
Intuitively, Lemma 1 guarantees the computability of addition. Because when more digits are known from the inputs, the sum interval will have smaller size, which ensures that more digits are produced in the result. This is stated as the following theorem.

**Theorem 3.1** (Computability of Addition). Let $A$ and $B$ be finite prefixes of two real numbers, and $|A|, |B| \geq n + 4$. We can find a finite sequence $C$ such that

- $[A] + [B] \subseteq [C]$,
- $|C| \geq n$

We now give a recursive definition of addition. The computation is conducted from left to right on the inputs. The carry is also generated from the most significant digit to the right. We define $\oplus$ such that $[A \oplus B] \simeq \left(\frac{2}{3}\right)^2([A] + [B])$, where $A, B \in (\exists n \in \mathbb{N}, \mathbb{B}^n)$. The actual summation of the inputs is derived by left shifting the results.

**Definition 3.2** (Addition of Binary Numbers with Proportional Relaxation.). For any finite prefixes $a_1a_2A$ and $b_1b_2B \in (\exists n \in \mathbb{N}, \mathbb{B}^{n+2})$, we have

\[
\begin{align*}
\ & a_1a_2A \oplus b_1b_2B = \\
\ & \quad \text{let } s = \frac{1}{3}\left\lfloor\left(\frac{2}{3}\right)^2(a_1 + b_1) + \left(\frac{2}{3}\right)^3(a_2 + b_2)\right\rfloor \\
\ & \quad \text{in addc } (A, B, s) \\
\ & \text{addc } (aA, bB, r) = \\
\ & \quad \text{let } s = \frac{2}{3}r + \left(\frac{2}{3}\right)^3(a + b) \\
\ & \quad \text{in round } (s) \downarrow \text{ addc } (A, B, s - \frac{1}{2} \text{ round } (s)) \\
\ & \text{addc } (A, \epsilon, r) = \epsilon \\
\ & \text{addc } (\epsilon, B, r) = \epsilon \\
\ & \text{round } (s) = \begin{cases} 
0 & 0 \leq s < \frac{1}{2} \\
1 & \frac{1}{2} \leq s \leq 1 
\end{cases}
\end{align*}
\]

where $d :: A$ means the concatenation of digit $d$ and sequence $A$, $\epsilon$ means the empty sequence.

**Theorem 3.2** (Correctness of Addition). For any $A, B \in (\exists n \in \mathbb{N}, \mathbb{B}^n)$, if $\min(|A|, |B|) = n + 2$, $n \geq 0$ and $A \oplus B$ is defined, then:

- $|A \oplus B| = n$
- $\left(\frac{2}{3}\right)^2([A] + [B]) \subseteq [A \oplus B]$

**Theorem 3.3** (Computability of Multiplication). Let $A, B \in (\exists n \in \mathbb{N}, \mathbb{B}^n)$, and $|A| = |B| = n + 4$. Then we can find a finite sequence $C$ such that

- $[A] \times [B] \subseteq [C]
- |C| \geq n$

**Definition 3.3** (Multiplication of Binary Numbers with Proportional Relaxation.). For any finite prefixes $a_1a_2a_3A$ and $b_1b_2b_3B$, we have

\[
\begin{align*}
\ & a_1a_2a_3A \times b_1b_2b_3B = \\
\ & \quad \text{let } x = \frac{1}{2}[a_1 + \left(\frac{2}{3}\right)^2a_2] \quad \text{and} \\
\ & \quad y = \frac{1}{2}[b_1 + \left(\frac{2}{3}\right)^2b_2] \quad \text{and} \\
\ & \quad s = x \times y \\
\ & \quad \text{in } \text{mult } (A, B, x, y, 4, s) \\
\ & \text{mult } (aA, bB, x, y, n, r) = \\
\ & \quad \text{let } s = \frac{2}{3}r + \left(\frac{2}{3}\right)^3(b \times x + a \times y + \left(\frac{2}{3}\right)^n ak) \\
\ & \quad \text{in } \text{round } (s) \downarrow \text{ mult } (A, B, x + (\frac{2}{3})^n a, y + (\frac{2}{3})^n b, n + 1, s - \frac{1}{2} \text{ round } (s)) \\
\ & \text{mult } (A, \epsilon, c) = \epsilon \\
\ & \text{mult } (\epsilon, B, c) = \epsilon \\
\ & \text{round } (s) = \begin{cases} 
0 & 0 \leq s < \frac{1}{2} \\
1 & \frac{1}{2} \leq s \leq 1 
\end{cases}
\end{align*}
\]

**Theorem 3.4** (Correctness of Multiplication). For any $A, B \in (\exists n \in \mathbb{N}, \mathbb{B}^n)$, if $\min(|A|, |B|) = n + 4$, $n \geq 0$ and $A \times B$ is defined, then:

- $|A \times B| = n$
- $[A] \times [B] \subseteq [A \times B]$

Besides basic operations such as addition and multiplication, comparisons of two real numbers also has great importance in exact real arithmetic. For example, when conducting division, the first thing to do is to test whether the divisor is equal to 0. Comparison for real numbers is inherently semi-decidable, regardless of the way it is defined. We give a definition for comparison of binary numbers with proportional relaxation. A direct implementation of this definition would either return a correct answer, or return an uncertainty of the comparison with an indication on how close the inputs are.

**Definition 3.4** (Comparison). For any finite prefixes $A$ and $B$, we have

\[
\begin{align*}
\ & A > B \iff \text{gt } (A, B, 0) \text{ where} \\
\ & \text{gt } (aA, bB, r) = \begin{cases} 
\text{true} & \text{if } s > 1 \\
\text{false} & \text{if } s < -1 \\
\text{gt } (A, B, r) & \text{otherwise} 
\end{cases} \\
\ & \text{gt } (A, \epsilon, r) = \text{unknown} \\
\ & \text{gt } (\epsilon, B, r) = \text{unknown}
\end{align*}
\]

**Theorem 3.5.**

\[
\begin{align*}
\ & A > B \text{ is true} \Rightarrow |A| > |B| \\
\ & A > B \text{ is false} \Rightarrow |B| > |A| \\
\ & A > B \text{ is unknown} \Rightarrow |A| - |B| \leq \left(\frac{2}{3}\right)^{\min(|A|, |B|)}
\end{align*}
\]

Other comparison operations like $<, \geq, \leq$ can be defined similarly.
4. Binary Numbers with Negative Digits

The design of binary numbers with proportional relaxation is inspired by the need of being able to express all intervals, which is achieved by providing redundancy on the semantics of different digits. Another way to introduce redundancy is to use an extra digit besides zero and one (Leslie 1817, Cauchy 1840). The semantics of digit 1 is −1. Digit 0 means zero. Digit 1 and 1 means 2−n and −2−n respectively, when being placed as the nth digit after the binary point. For a finite sequence of digits A, the infinite sequence 0.A would range from 0.A(1)∞ to 0.A(1)∞. So the sequence 0.1 means −1, 0, and the sequence 0.1 means −1, 1, and the sequence 0.1 means 0, 1 (Figure 3).

![Figure 3. Binary Numbers with Negative Digits](image)

We next define ⊕ such that [A ⊕ B] ∼ [A] + [B] 2, where A, B ∈ (∃n ∈ N, B^n). The actual summation of the inputs is derived by left shifting the results.

**Definition 4.3** (Addition of Binary Numbers with Negative Digits). For any real numbers with prefixes aA and bB, A, B ∈ (∃n ∈ N, B^n), we have

\[
aA ⊕ bB = \text{addc} (A, B, \frac{1}{2}(a + b))
\]

**Theorem 4.2.** For any finite prefix A and B, if min(|A|, |B|) = n + 1, n ≥ 1 and A ⊕ B is defined, then:

- |A ⊕ B| = n
- \[\frac{|A| + |B|}{2} \subseteq [A ⊕ B]\]

We next define multiplication of binary numbers with negative digits in the following two definitions.

**Definition 4.4** (Multiplication of a real number by a digit).

\[
1 \cdot dA = d(1 \cdot A)
\]

\[
0 \cdot dA = 0(0 \cdot A)
\]

\[
1 \cdot dA = (0 \cdot d)(1 \cdot A)
\]

**Definition 4.5** (Multiplication of two real numbers). Multiplication of two finite prefixes can be recursively defined as follows [22]:

\[
a_1a_2A × b_1b_2B = ((a_1 \cdot b_1 :: (b_2 \cdot A + a_2 \cdot B)) ⊕ (a_1 \cdot b_1 :: a_2 \cdot b_1 :: a_2 \cdot b_2 :: A × B))
\]

**Theorem 4.2.** For finite prefixes A and B, n ≥ 2 and A × B is defined, then:

- |A × B| = n
- \([A] × [B] \subseteq [A × B]\)

We have similar definition of comparison for binary numbers with negative digits as for binary numbers with proportional relaxation.

**Definition 4.6** (Comparison). For any real numbers with finite prefix A and B, we have

\[
A > B \iff \text{gt} (A, B, 0) \text{ where } \text{gt} (aA, bB, r) = \begin{cases} 
\text{true} & \text{if } s > 1 \\
\text{false} & \text{if } s < -1 \text{ gt} (A, C, r) = \text{unknown} \\
\text{gt} (A, B, s) & \text{otherwise}
\end{cases}
\]

\[
\text{gt} (ε, B, s) = \text{unknown}
\]
The definition above satisfies:

**Theorem 4.3.**

\[ A > B \text{ is true } \Rightarrow [A] > [B] \]
\[ A > B \text{ is false } \Rightarrow [B] > [A] \]
\[ A > B \text{ is unknown } \Rightarrow |[A] - [B]| \leq (2 \cdot \frac{1}{2})^{\min(|A|,|B|)} \]

### 4.1 Related Work

Most existing computer systems approximate exact real numbers by floating point numbers [13]. The standard most commonly used is IEEE-754, which includes 32-bit single precision and 64-bit double precision representations [2]. Unfortunately, floating point arithmetic is inherently inaccurate. Only a very limited subset of real numbers may be represented exactly, and rounding errors occur in almost every floating point operation. Error analysis have been studied to overcome the problem, for example based on automatic differentiation [16], or using stochastic numbers to represent real numbers by tuples of randomly rounded floating-point numbers [24]. Some comparison between different methods based on a formal semantics for floating point numbers with errors can be found in [18].

A few academic tools exist with guaranteed fidelity in some very specific cases, such as systems with validated numerical solvers for Ordinary Differential Equations (ODE) in initial value problems [21, 9, 6, 3]. They are able to bound the distance between the computed and exact solution to ODEs. For example, Nedialkov et al [21] use interval-valued functions to approximate a solution to an initial value problem of ODEs by finding fixed points of some functions. Issues with interval arithmetic such as wrapping effects are addressed in detail.

Affine arithmetic improves the precision of interval arithmetic [10]. Compared to usual intervals, affine arithmetic makes it possible to reduce the over-approximation introduced by interval arithmetic by recording some relations between values. Recently, an abstract domain based on affine arithmetic has been proposed in [15]. Modal arithmetic is obtained by coupling an existential or universal quantifier to the usual intervals [12]. Modal intervals have been recently extended to generalized intervals which are intervals whose bounds are not constrained to be ordered [14]. Generalized intervals whose upper bound are less than the lower one are quantified existentially.

Different design and representations of exact real numbers using lazy representation has also been researched for a long time. Boehm, Cartwright, et al. [5] have implemented exact real arithmetic by representing real numbers as potentially infinite sequences of digits and evaluating on demand. They have compared this lazy implementation with a functional implementation and given some empirical comparison of the two techniques. Boehm and Cartwright provide more insights on the comparisons of different approaches to performing exact real arithmetic on a computer in [4].

Potts, Edalat and Escardó proposed a lazy representation of exact real numbers called Linear Fractional Transformations in [23]. They incorporated a representation of the non-negative extended real numbers based on the composition of linear fractional transformations with non-negative coefficients into the Programming Language for Computable Functions (PCF) with products. They have presented two models for the extended language and show that they are computationally adequate with respect to the operational semantics. Later on, Edalat and Sunderhauf [11] use basic ingredients of an effective theory of continuous domains to spell out notions of computability of the reals and for functions on the real line.

While all of these works representing exact real numbers using lazy representation demonstrated impressive results, we believe that a better understanding of the design space of representations of exact real arithmetic may both yield a way to unify these approaches and accelerate advancement in this area.

## 5 Conclusions and Future Work

We began this paper by making a case for the importance and the timeliness of research on exact real computation, and followed this by an expository review of some of the basic issues that arise in exact real computation. To highlight some of the peculiarities of exact real computation, we discuss the difficulty in defining addition using the standard binary digit representation of fractions. We explain how this can be traced to the strictly hierarchical manner in which this representation forces intervals to be structured. This was followed by showing two different ways of solving this problem, namely, relaxing the meaning of digits and adding negative digits. For both these representations, we show how addition, multiplication, and comparison can be defined.

While space does not allow us in this paper, we believe that the issue of comparison deserves further discussion and analysis. Whereas here we have focused on pointing out these issues, our ultimate goal is to formalize these issues in a manner that allows us to classify and investigate the wide range of possible representations in a systematic and empirically justified manner. Because of their prominent role in scientific computing, in future work we hope to also identify the issues that arise in the introduction of the notions of division, exponentiation, continuous functions, integration, and differentiation.

Interval arithmetic suffers from the wrapping effect which makes the intervals grow artificially because of unavoidable over-approximations. For example, let us consider the function \( f \) which computes a rotation of angle \( \theta \):
\[
f(x, y) = \begin{pmatrix} x \cos \theta - y \sin \theta \\ x \sin \theta + y \cos \theta \end{pmatrix}
\]

Intuitively, a pair \((x, y)\) of intervals defines a box in the plane. The image \(f(x, y)\) of this box by a function \(f : \mathbb{R}^2 \rightarrow \mathbb{R}^2\) is not necessarily a box. However, in interval arithmetic, \(f(x, y)\) must be approximated by a new pair of intervals which must strictly encompass the exact image. The dotted box on the right-hand-side of the figure below shows the most precise interval image of \(f(x, y)\) with \(\theta = \pi/4\).

Future work will explore ways of capturing and exploiting such dependence between different values.

References

Appendix

Proofs for Base-2 Real Numbers

Proposition 2.1. For any \( A \in \mathbb{B}^n \):

- \( [A] \subseteq [0, 1] \)
- \( |[[A]]| = (\frac{1}{2})^{|A|} \)

Proof. By induction on the length of \( A \).

If \( |A| = 0 \), \( [A] = [0, 1] \). Also, \( |[A]| = 1 = (\frac{1}{2})^0 \)

Suppose \( [A] \subseteq [0, 1] \) and \( |[[A]]| = (\frac{1}{2})^{|A|} \) holds when \( |A| = n - 1 \) and let \( [A] = [x, y] \). Then we have \( \lfloor A0 \rfloor = [x, x + \frac{1}{2}(y - x)] \subseteq [0, 1] \) and \( \lfloor A1 \rfloor = [x + \frac{1}{2}(y - x), y] \subseteq [0, 1] \). This also gives \( \lfloor [A0] \rfloor = \lfloor \frac{1}{2}(y - x) \rfloor = \frac{1}{2} \lfloor [A] \rfloor = (\frac{1}{2})\lfloor A \rfloor \).

Lemma 2. \( [dA] = \frac{d}{2} + \frac{|[A]|}{2} \)

Proof. By induction:

If \( A = \epsilon \), \( [dA] = [\frac{d}{2} + \frac{|[A]|}{2}] \).

Let \( [A] = [x, y] \), if \( [dA] = \frac{d}{2} + \frac{|[A]|}{2} = [\frac{d}{2} + \frac{d}{2} + \frac{|[A]|}{2}] = \frac{d}{2} + \frac{|[A]|}{2} \).

Thus, \( [dA] = \frac{d}{2} + \frac{|[A]|}{2} \) always holds.

Lemma 3. \( [\text{add_one}(A)] \geq \frac{1}{4} + \frac{|[A]|}{2} \)

Proof. By induction on the length of \( A \).

If \( A = \epsilon \), \( [\text{add_one}(A)] = [1] \).

If \( [A] = [x, y] \), if \( [dA] = \frac{d}{2} + \frac{|[A]|}{2} \).

Then, \( \lfloor A0 \rfloor = \lfloor [A0] \rfloor = \frac{d}{2} + \frac{|[A]|}{2} \).

Thus, \( [\text{add_one}(A)] = \frac{1}{4} + \frac{|[A]|}{2} \).

Theorem 2.1 (Correctness of Addition)

If \( A \oplus B \) is defined, then \( [A1 + B] \subseteq [A \oplus B] \)

Proof. By induction. If \( A = \epsilon \).

\[
\lfloor A \oplus B \rfloor = \lfloor \epsilon \oplus B \rfloor = [\epsilon] = [0, 1] \\
\lfloor A \oplus B \rfloor = \lfloor [A] + [B] \rfloor \subseteq [0, 1]
\]

\[
\lfloor A \oplus B \rfloor = [\frac{aA + bB}{2}]
\]

Similar for case \( B = \epsilon \).

Now, if \( [A1 + B] \subseteq [A \oplus B] \). Then for \( aA \oplus bB \).

- \( b = a \).

\[
\lfloor aA + bB \rfloor = \lfloor a(A \oplus B) \rfloor = a + \frac{|A|}{2} + \frac{|B|}{2} \subseteq a + [A \oplus B]
\]

- \( b = 1 - a \).

\[
\lfloor aA + bB \rfloor = \lfloor [\text{add_one}(A) \oplus B] \rfloor \quad \frac{1}{4} + \frac{|A| + B}{2} \\
\lfloor aA + bB \rfloor = \lfloor [\frac{A + B}{2}] \rfloor \quad = \frac{1}{2} + [A \oplus B]
\]

\[
\lfloor aA + (1-a)B \rfloor \subseteq [A \oplus (1-a)B].
\]

Theorem proved.

Lemma 4. If \( |A \oplus B| = l \geq 1 \), then \( |aA \oplus bB| = l + 1 \).

Proof. If \( b = a \), then \( |aA \oplus bB| = |(a(A \oplus B))| = 1 + |A \oplus B| = l + 1 \).

If \( b = 1 - a \), then \( |aA \oplus bB| = |\text{add_one}(A \oplus B)| \).

Theorem 2.2 Let \( A = A_1dA_2 \) and \( B = B_1dB_2 \), \( |A_1| = |B_1| = l \). Then \( |A \oplus B| \geq l + 1 \).

Proof. \( |dA_2 \oplus dB_2| = |d(A_2 \oplus B_2)| \geq 1 \).

Applying Lemma 4 for \( l \) times, we get \( |A_1dA_2 \oplus B_1dB_2| \geq l + 1 \).

Proofs for Proportional Relaxation

Lemma 1. For any rational interval \( I = [x, y] \subseteq [0, 1] \), we can find a finite sequence \( A \) such that

- \( I \subseteq [A] \)
- \( \frac{1}{3} |[A]| < |I| \)
- \( |A| = \max\{0, \lfloor \log_2 \frac{3}{4} |I| \rfloor + 1\} \)

Proof. We inductively construct the sequence of digits \( \{A\} \) as follows: \( A_0 = \epsilon \).

If \( |I| \geq \frac{1}{4} = \frac{1}{4} |[A_0]| \), \( A_0 = A_1 \) is such a sequence we are looking for.

Otherwise, \( \frac{1}{4} |[A_0]| \geq |I| \).

Let \( A_{i+1} = \begin{cases} A_0 & \text{if } I \subseteq [A_0] \\ A_1 & \text{else} \end{cases} \)

For the first case, \( I \subseteq [A_1, A_1] \). For the second case, let \( A_2 = [a, b], [A_0] = [a, \frac{1}{2}(b - a)] \).

From \( I \subseteq [A_1] \) and \( I \not\subseteq [A_0] \), we have \( y \in (\frac{1}{2}(b - a), b] \). Since \( \frac{1}{4} |[A_1]| \geq |I| \),
Lemma 5.

Theorem 3.1 (Computability of Addition).

Let $A$ and $B$ be finite prefixes of two real numbers, and $|A|, |B| \geq n+4$. Then we can find a finite sequence $C$ such that

- $[A] + [B] \subseteq [C]$
- $|C| \geq n$

Proof. Let us assume $[A] + [B] \subseteq [0, 1]$, otherwise we can achieve this by shifting the addends and shift back the results.

$[[A]] \leq \left(\frac{2}{3}\right)^{n+4}$ and $[[B]] \leq \left(\frac{2}{3}\right)^{n+4}$ thus

$[[A] + [B]] \leq 2 \cdot \left(\frac{2}{3}\right)^{n+4} = \frac{64}{273} \left(\frac{2}{3}\right)^{n-1}$

From lemma 1 we know we can find a real number $C$ such that

- $[A] + [B] \subseteq [C]$
- $|C| \geq \left|\log_{\frac{2}{3}} \frac{64}{273} \left(\frac{2}{3}\right)^{n-1}\right| + 1 \geq n$

Theorem proved.

Lemma 5. $|dA| = \frac{d}{3} + \frac{2}{3}|A|$

Proof by induction similar to Lemma 2

Lemma 6. In definition 3.2, we have $r \in [0, \frac{1}{2}]$, and $s \in [0, 1]$

Proof. We prove it by induction.

For base case, $a_i, b_i \in \{0, 1\}$, $r = s = \frac{1}{3}(\frac{2}{3})^2(a_1 + b_1) + (\frac{2}{3})^3(a_2 + b_2)$. We have $r = \frac{40}{81} \in [0, \frac{1}{2}]$.

In the iterative function application of $addc$, we have

$s = \frac{3}{2}r + \frac{1}{3}(\frac{2}{3})^3(a + b) \in \left[\frac{3}{2} \cdot \frac{1}{2}, \frac{16}{81}\right] \subset [0, 1]$

Thus, by definition of round $s$, we have

$r = s - \text{round}(s) \in \left[0, \frac{1}{2}\right]$

Therefore $s \in [0, 1]$ and $r \in [0, \frac{1}{2}]$ always hold.

Lemma 7. $[[addc(A, B, r)] \geq \left(\frac{2}{3}\right)^4([A] + [B]) + r$

Proof. Proof by induction.

For base case,

By induction hypothesis,

Thus $addc(A, B, r) \subseteq addc(A, B, r')$

On the other hand,

This gives

Theorem 3.2 (Correctness of Addition).

For any $A, B \in (\exists n \in \mathbb{N})$, if $\min(|A|, |B|) = n+2$, $n \geq 0$ and $A \oplus B$ is defined, then:

- $|A \oplus B| = n$
- $\left(\frac{2}{3}\right)^2([A] + [B]) \subseteq [A \oplus B]$

Proof. 1. If $n = 0$ then $\min(|A|, |B|) = 2$, without loss of generality, let $A \equiv a_1 a_2, B \equiv b_1 b_2 Y$ and $s = \frac{1}{3}(\frac{2}{3})^2(a_1 + b_1) + (\frac{2}{3})^3(a_2 + b_2)$

$|A \oplus B| = 0$

$\left(\frac{2}{3}\right)^2([A] + [B]) = [s, s + 2(\frac{2}{3})^4]$)

It is easy to show $s \in [0, \frac{1}{2}]$, thus

$\left(\frac{2}{3}\right)^2([A] + [B]) \subseteq [0, 1] = [\epsilon] = [A \oplus B]$

2. If $n > 0$, let $A \equiv a_1 a_2 X, B \equiv b_1 b_2 Y$, $\min(|A|, |B|) = n+2$. It is easy to show by induction that

$addc(A, B, r) = \min(|A|, |B|)$

which follows which we get

$x = addc(X, Y, r) = \min(|x|, |y|) = n$

Let $s = \frac{1}{3}(\frac{2}{3})^2(a_1 + b_1) + (\frac{2}{3})^3(a_2 + b_2)$

$[A \oplus B] = addc(X, Y, s) \geq \left(\frac{2}{3}\right)^4([X] + [Y]) + s$

Meanwhile, by lemma 5,

$\left(\frac{2}{3}\right)^2([A] + [B]) = s + \left(\frac{2}{3}\right)^3([X] + [Y])$

Thus shows that $\left(\frac{2}{3}\right)^2([A] + [B]) \subseteq [A \oplus B]$
**Theorem 3.3** (Computability of Multiplication)

Let $A, B \in (\exists n \in \mathbb{N}). B^n$, and $|A| = |B| = n + 4$. Then we can find a finite sequence $C$ such that

- $[A] \times [B] \subseteq [C]$
- $|C| \geq n$

**Proof.** From Proposition 3.1 we know that

- $[A] \subseteq [0, 1], [B] \subseteq [0, 1]$
- $|[A]| = (\frac{2}{3})^{n+4}, |[B]| = (\frac{2}{3})^{n+4}$.

Let us assume $[A] = [x, x + z], [B] = [y, y + z]$, where $z = (\frac{2}{3})^{n+4}$ and $0 \leq x, y \leq 1 - z = 1 - (\frac{2}{3})^{n+4}$.

We have $[A] \times [B] = [xy, xy + (x + y)z + z^2] \subseteq [0, 1]$.

$$|[A] \times [B]| = (x + y)z + z^2$$

$$\leq 2(1 - (\frac{2}{3})^{n+4}) + (\frac{2}{3})^{2(n+4)}$$

$$= (2 - (\frac{2}{3})^{n+4})(\frac{2}{3})^{n+4} < 2(\frac{2}{3})^{n+4}$$

From Lemma 1 we know we can find $C$ such that

- $[A] \times [B] \subseteq [C]$ and $|C| = \lceil \log_2 3 |[A] \times [B]| \rceil > n$

□

**Proofs for Binary Numbers with Negative Digits**

**Lemma 8.** $[dA] = \frac{d}{2} + \frac{1}{2} |A|$

By induction similar to Lemma 2

**Lemma 9.** In definition 3.2, we have $r \in [-1, 1]$ and $s \in [-3, 3]$.

By induction similar to Lemma 6

**Lemma 10.** $[addc(A, B, r)] \supseteq [A] + [B] + 2r$

By induction similar to Lemma 7.

**Theorem 4.1** For real numbers with infinite prefix $A$ and $B$, if $\min(|A|, |B|) = n + 1$, $n \geq 1$ and $A \oplus B$ is defined, then:

- $|A \oplus B| = n$
- $\frac{|A| + |B|}{2} \subseteq [A \oplus B]$

The proof is similar to the proof of Theorem 3.2.