CS3110 Spring 2017 Lecture 11: Constructive Real Numbers

Robert Constable

Reminder: Prelim in class next Tuesday. It will not cover the real numbers beyond this lecture.

Note: One definition of the void type in OCaml is this: ``type void = {none:`a.`a}``.

	Date for	Due Date
Prelim	Tue. March 14, in class	
PS3	Out on Thur. March 2	March 16
PS4	Out on March 16	March 30
PS5	Out on April 10	April 24
PS6	Out on April 24	May 8 (day of last lecture)

1 Value of the constructive real numbers

Some approximation of the real numbers is used in science, engineering, and general computing. By far the most widely used and commonly taught approximation are the *IEEE floating point numbers.* The latest IEEE standard is essentially universal on all modern computers, and there is a great deal of firm knowledge about these numbers taught in numerical analysis courses and other science and engineering courses. On the other hand, the mathematics of the floating point numbers is not as conceptually clear as the basic mathematical definition of the constructive real numbers, and it is more difficult to precisely relate their properties to those of the formal mathematical notion.

It is much more rare to teach the underlying mathematical notion of the real numbers and how it is possible to compute with them. This is the goal of the next two lectures. In many ways this account is conceptually much simpler than the IEEE floating point account, and we can prove many of the standard results from calculus and analysis using the constructive reals. The use of these constructive reals in the Coq and Nuprl proof assistants has led to useful implementations and applications of the basic results in real analysis – a core area of mathematics.

One reason we can teach these ideas in an undergraduate computer science course is that in 1967 the American mathematician Errett Bishop wrote a very clear textbook, *Foundations of Constructive Analysis* [1]. In many ways this was a landmark event. It drew the United States into the effort to develop constructive mathematics in the tradition of Brouwer. It also came at a time that I had embarked on teaching the results of computing theory constructively (in a way that the graduate students would not even notice was different). I was doing this as a challenge to understand the emerging theory of computing constructively. I was aware of intuitionism from my PhD advisor S.C.Kleene who had studied with Brouwer and was working to relate intuitionism to mainstream mathematics [5, 6, 4].

Bishop's remarkable book was a blueprint for how to teach mathematical concepts constructively without raising philosophical issues. The point was to obtain sharper results which had computational meaning and notice any points where this could not be done. It was a revelation that most computer science concepts could be taught constructively and that this would make them richer and even more computational in a straight forward way.

After Bishop died, Douglas Bridges revised his book by adding important new results since 1967, such as a better treatment of integration. The revised book is simply called *Constructive Analysis* [2]. By this time we had formalize in Nuprl several results from Bishop's book, and Springer-Verlag allowed us to post a copy of Chapter 2 on our web page. Mark Bickford has linked this chapter to his formalization of the results in Nuprl. This gives you access to the combined results of Bishop, Bridges, and Bickford that build on Brouwer.[1]

We have recently learned, based on interest in Cornell research into these topics, that the constructive real numbers form the basis for *ground truth* in applied real analysis. Other mathematicians and computer scientists have turned to the research groups who have implemented the constructive real

[1] What does this say about last names that start with the letter B?

numbers to evaluate how closely the floating point results match the true results. This is one of the capabilities that the PL, formal methods, and verification researchers can provide to science and engineering. We want students and readers to understand this paradigm, even though we cannot afford to spend many lectures on this topic.[2]

1.1 From the rational numbers to the reals

The numbers studied in early Greek mathematics were the rational numbers. The idea of ratios was important in Greek philosophy and ontology. It was a shock when Pythagoras discovered irrational numbers, and it became a challenge of mathematics from that point onward to understand what we now know as the *real numbers.*

The key discovery of Pythagoras was that in a square with sides s and hypotenuse h, the square of the hypotenuse is equal to the sum of the squares of the sides, i.e. $h^2 \ = \ s^2 + s^2$. Already from this Pythagoras saw the existence of a number that is not rational. Let the sides of the square be of unit length, then we have $h^2 \ = \ 1 + 1$. But h cannot be a ratio a/b because then $(a/b)^2 \ = \ 2$, hence $a^2 \ = \ 2b^2$. Thus 2 divides a^2 an even number of times and 2 divides $2b^2$ an odd number of times. Hence there is no solution to $a^2 \ = \ 2b^2$ in the integers. We can also directly prove that the square root of 2, $\sqrt{2}$, is not a rational number. Once it was known that there is such an entity as an irrational number, many deep mathematical questions arose. The study of this topic eventually led to the formulation of the mathematical notion of the *real numbers*; it took until the late 1800's for this concept to become clear and well understood. Here are some of the historical highlights.

By 1835 William Hamilton offered a precise definition of the irrational numbers as limits of a sequence of rational numbers. He published this in his book *Algebra as the Science of Pure Time.* Oddly enough, it was not until 1860 that the notion of a rational number as a pair of integers was proposed and explored. It was not until Peano in 1889 that a rigorous account of the natural numbers and integers was achieved. In 1874 Cantor wrote his first article on set theory, and that provided a framework for a precise definition

[2] We use PL to stand for the very wide area of *Programming Languages.* It is a subject area that has been part of computer science from the very beginning and has been a key interface between computer science and other disciplines.

of the natural numbers and the rational numbers.

In 1899 Hilbert proposed a set of axioms for the real numbers, in a four page article. The modern set theoretic account of natural numbers, rational numbers, and real numbers was established by Cantor in his set theory, but he also discovered Cantor's paradox about sets. A great deal of effort was need to establish set theory on firm ground which was accomplished in the formalization of Zermelo Fraenkel set theory with the axiom of choice, ZFC. We do not have time to investigate set theory and this approach to the real numbers. Furthermore, that approach does not lead to a computationally meaningful notion of real numbers. That accomplishment is due to L.E.J. Brouwer whom we have mentioned before. This is a very rigorous notion that has been implemented in proof assistants as we noted above. It is formulated in type theory rather than set theory because set theory does not have a computational basis. This choice of type theory creates an opportunity for us. A very accessible historical account of the development of the notion of the real numbers is give in Morris Kline's book *Mathematical Thought from Ancient to Modern Times* [7]. Another good historical account that includes the role of Brouwer and other constructive mathematicians can be found in the book *Foundations of Set Theory* [3].

Many new computational questions arose such as how to perform the arithmetic operations on these new numbers. This led to the discovery that the algebra of the reals is also a field. There followed a great enrichment of algebra. Discovering the real numbers also led to the need to understand what it means to "compute with" them more generally, i.e. what is a function from reals to reals? We write the type of these functions as $\mathbb{R} \to \mathbb{R}$.

Once it was discovered that we could perform all of the arithmetic operations of a field on these new "numbers," another topic in algebra arose and a whole new branch of mathematics was created called *real analysis* or just *analysis* for short. Many of the questions investigated were computational, and others were algebraic. The ties to geometry were established by Rene Descartes. In addition a whole category of investigation opened related to geometric ideas, it is called *topology.* One of its founders was L.E.J. Brouwer, and he worked to understand the fundamental character of the real numbers which he associated with the geometric idea of a line or more intuitively for most people, with the *continuum of time* which is essential to the human experience.

Historical background to Bishop

Greek geometry was “constructive” using straight edge and compass. But the Greeks “feared” the idea of *infinity* or unbounded constructions. They loved rational numbers and harmonics.

The idea of a *function* did not become clear until the 1800’s “y varies with x according to some law.”

- Cauchy – 1821 “Course in analysis.”
- Weierstrauss – by 1859 (high school teacher)

1880 split

↙ ↘

Dedekind	Kronecker
Cantor	Poincaré
Weierstrauss	Weil
Hilbert	Weyl

Brouwer 1907, 1912 (Intuitionism and Formalism)
Heyting 1956, Intuitionism
Turing 1936, On computable numbers with an application to the Entscheidungs problem

Note, Turing made a mistake in defining the reals computationally, a common one. He published a correction in 1937. He originally said that a real number is computable iff we can compute its (unending) decimal by a (Turing) machine. See Bishop p.62 problem 9.

Note further, Brouwer allowed a more general notion of computability which could involve “free choice sequences.” Nuprl follows Brouwer, Coq follows Bishop. There is a large library of real analysis built using both proof assistants.

Further motivation to study constructive reals

One reason to study constructive reals is that the proof assistants are making them practical for results in *cyber-physical systems* (CPS). Another reason is that the computer science development and implementation are part of the intellectual history of constructive mathematics. Bishop's book is a landmark that computer science has "brought to life" and deepened.

The role of computer science in intellectual history is clear in *theory* (e.g. the notion of computational complexity – two Cornell Turing Awards) and in *artificial intelligence*, the understanding and extension of intelligence. *It is also there in PL as computer science enriches the type systems and capabilities of programming languages to support high level programming of cyber-physical systems, computational geometry, homotopy type theory (HTT), and other areas of mathematics.*

Differences between constructive analysis over the reals, $\mathbb{R}$, and ordinary calculus over the "classical" reals

1. In calculus books, the operations on the reals are not defined by algorithms. Indeed we imagine that we can say things in calculus that don't make sense computationally. For example, in calculus we assume that given two reals, say r_1 and r_2 we know:

   - Is $r_1 = r_2$? – In fact we can't decide this in general.
   - Is $r_1 = 0$? – We can't decide this in general.
   - Is $r_1 < r_2$? – We can't decide this in general.

   Bishop needed results such as Proposition 2.16 and Corollary 2.17, page 26, to deal with these concepts constructively.

2. We will see that all functions on the reals are continuous. It is not possible to create "step functions."

is countably infinite. A similar proof using (1.2) shows that $\mathbb{Z} \times \mathbb{Z}$ is countably infinite

A set which is in one-one correspondence with $\mathbb{Z}_n$ is said to *have n elements*, and to be *finite*. Every finite set is countable.

It is not true that every countable set is either countably infinite or subfinite. For example, let A consist of all positive integers n such that both n and $n+2$ are prime; then A is countable, but we do not know if it is either countably infinite or subfinite. This does not rule out the possibility that at some time in the future A will have become countably infinite or subfinite; it is possible that tomorrow someone will show that A is subfinite. This set A has the property that if it is subfinite, then it is finite. Not all sets have this property.

2. The Real Number System

The following definition is basic to everything that follows.

(2.1) **Definition.** A sequence (x_n) of rational numbers is *regular* if

(2.1.1) $$|x_m - x_n| \leqq m^{-1} + n^{-1} \qquad (m, n \in \mathbb{Z}^+).$$

A *real number* is a regular sequence of rational numbers. Two real numbers $x \equiv (x_n)$ and $y \equiv (y_n)$ are *equal* if

(2.1.2) $$|x_n - y_n| \leqq 2n^{-1} \qquad (n \in \mathbb{Z}^+).$$

The set of real numbers is denoted by $\mathbb{R}$.

(2.2) **Proposition.** *Equality of real numbers is an equivalence relation.*

Proof: Parts (i) and (ii) of (1.1) are obvious. Part (iii) is a consequence of the following lemma.

(2.3) **Lemma.** *The real numbers $x \equiv (x_n)$ and $y \equiv (y_n)$ are equal if and only if for each positive integer j there exists a positive integer N_j such that*

(2.3.1) $$|x_n - y_n| \leqq j^{-1} \qquad (n \geqq N_j).$$

Proof: If $x = y$, then (2.3.1) holds with $N_j \equiv 2j$.

Assume conversely that for each j in $\mathbb{Z}^+$ there exists N_j satisfying (2.3.1). Consider a positive integer n. If m and j are any positive integers with $m \geqq \max\{j, N_j\}$, then

$$\begin{aligned}|x_n - y_n| &\leqq |x_n - x_m| + |x_m - y_m| + |y_m - y_n| \\ &\leqq (n^{-1} + m^{-1}) + j^{-1} + (n^{-1} + m^{-1}) < 2n^{-1} + 3j^{-1}.\end{aligned}$$

Since this holds for all j in $\mathbb{Z}^+$, (2.1.2) is valid. □

Notice that the proof of Lemma (2.3) singles out a specific N_j satisfying (2.3.1). This situation is typical: every proof of a theorem which asserts the existence of an object must embody, at least implicitly, a finite routine for the construction of the object.

The rational number x_n is called the n^{th} *rational approximation* to the real number $x \equiv (x_n)$. Note that the operation from $\mathbb{R}$ to $\mathbb{Q}$ which takes the real number x into its n^{th} rational approximation is not a function.

For later use we wish to associate with each real number $x \equiv (x_n)$ an integer K_x such that

$$|x_n| < K_x \qquad (n \in \mathbb{Z}^+).$$

This is done by letting K_x be the least integer which is greater than $|x_1| + 2$. We call K_x the *canonical bound* for x.

The development of the arithmetic of the real numbers offers no surprises: we operate with real numbers by operating with their rational approximations.

(2.4) **Definition.** Let $x \equiv (x_n)$ and $y \equiv (y_n)$ be real numbers with respective canonical bounds K_x and K_y. Write

$$k \equiv \max\{K_x, K_y\}.$$

Let α be any rational number. We define

(a) $x + y \equiv (x_{2n} + y_{2n})_{n=1}^{\infty}$

(b) $xy \equiv (x_{2kn} y_{2kn})_{n=1}^{\infty}$

(c) $\max\{x, y\} \equiv (\max\{x_n, y_n\})_{n=1}^{\infty}$

(d) $-x \equiv (-x_n)_{n=1}^{\infty}$

(e) $\alpha^* \equiv (\alpha, \alpha, \alpha, \ldots)$.

(2.5) **Proposition.** *The sequences* $x+y$, xy, $\max\{x, y\}$, $-x$, *and* α^* *of Definition* (2.4) *are real numbers.*

References

[1] E. Bishop. *Foundations of Constructive Analysis.* McGraw Hill, NY, 1967.

[2] E. Bishop and D. Bridges. *Constructive Analysis.* Springer, New York, 1985.

[3] A. A. Fraenkel, Y. Bar-Hillel, and A. Levy. *Foundations of Set Theory*, volume 67 of *Studies in Logic and the Foundations of Mathematics.* North-Holland, Amsterdam, 2nd edition, 1984.

[4] S. C. Kleene and R. E. Vesley. *Foundations of Intuitionistic Mathematics.* North-Holland, 1965.

[5] S.C. Kleene. On the interpretation of intuitionistic number theory. *J. of Symbolic Logic*, 10:109–124, 1945.

[6] S.C. Kleene. Mathematical logic: Constructive and non-constructive operations. *Proceedings of the International Congress of Mathematics*, pages 137–153, 1960.

[7] Morris Kline. *Mathematical thought from ancient to modern times.* Oxford University Press, 1990.