CS3110 Spring 2016 Lecture 11: Introduction to the Constructive Reals

Topics

- Observations about the integer square root theorem and program.
- Motivations for learning the constructive reals:
  - deep subtle computational ideas,
  - relevance to modern cyber-physical systems (CPS),
  - motivations for richer type theory supported by proof assistants.
- Basic concepts of constructive real analysis.

Observations about the integer square root

Logical specification:

Informal:	given a natural number n, say that natural number r is its integer square root iff $\underline{r^2 \leq n < (r+1)^2}$.
Symbolic:	$\forall n\!:\!\mathbb{N}.\ \exists r\!:\!\mathbb{N}.(r^2 \leq n < (r+1)^2)$

How to know we can find r given n?

- Write a (recursive) OCaml program to find it. Explain why *the program meets the specification.*

- Prove the logical specification, the proof will show *existence*, $\exists r:\mathbb{N}.(r^2 \leq n < (r+1)^2)$, but will it show how to compute r?
- Prove the logical specification "constructively."

We can prove $\forall n:\mathbb{N}.\exists r:\mathbb{N}.(r^2 \leq n < (r+1)^2)$ by *induction on n.* Recall the format of induction.

Base Case:

$n = 0$
$\exists r:\mathbb{N}.(r^2 \leq 0 < (r+1)^2)$
Take $r = 0$.

Induction Step:

Assume the result for n, prove it for $n+1$.

Assume $\exists r_n:\mathbb{N}.(r_n^2 \leq n < (r_n+1)^2)$ (Induction Hypothesis)

Show $\exists r:\mathbb{N}.(r^2 \leq n+1 < (r+1)^2)$

Analyze the assumed root r_n.

If $(r_n+1)^2 \leq n+1$ then choosing $r = (r_n+1)$ will work since $(n+1) < ((r_n+1)+1)^2$ by *arithmetic*.

If $n+1 < (r_n+1)^2$ then choose $r = r_n$.

QED

Notice that the logical reasoning "works forward" from the induction hypothesis, and the computation works as a recursive call, from $n+1$ to n, going "backwards" as in a recursive function definition.

As the Lecture 9 notes show, we can write the recursive core of this argument as the following recursive functional program:

let rec sqrt i

  $=$ **if** $i = 0$ **then** 0

    else let $r =$sqrt$(i - 1)$

        in

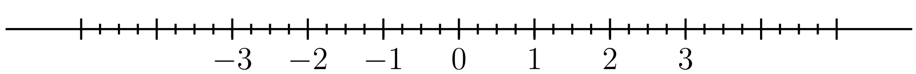
          if $(r + 1)^2 \leq i$ **then** $r + 1$

          else r

We will see other examples of the fact that inductive proofs have the structure of recursive programs. If the proofs are done using constructive logic then they are in fact also programs. This follows the "*Proofs as Programs*" methodology developed at Cornell in the 1980's.

Motivations for learning the constructive real numbers

The Greeks made the rational numbers, $\mathbb{Q}$, the central idea of their mathematics and philosophy. The Pythagoreans believed that all the ideas of mathematics, physics, art, and architecture could be expressed in terms of rational numbers. They believed that these "filled the *number line*."



The rationals are *dense* in the number line.

One of the momentous discoveries in the history of mathematics was that there are "holes" in the number line filled by irrational numbers, such as $\sqrt{2}$. The Greeks discovered and proved that $\sqrt{2}$ is not rational.

Exercise: find a very simple proof of this.

They soon found that the square root of every prime is irrational. By the time of Euclid's *Elements* (300 BCE) the irrationals were accepted (called *incommensurables*). This was the "state of the number line" for the next two and a half millennia.

In 1850 a new kind of number was discovered, the *transcendental* numbers. These are numbers that are *non algebraic* – they are not the solution of any polynomial equation with integer coefficients.

Is there a notion of the type (or set) of all real numbers – *all numbers of the number line?*

Basic concepts of constructive real analysis

One of the modern mathematicians to have a major impact on our understanding of the *continuum* and the real numbers is the topologist L.E.J. Brouwer famous for his fixed point theorem and for an approach to mathematics called *intuitionism.* He was not only a brilliant mathematician, he was good at "provoking" other top mathematicians, especially David Hilbert. He introduced several fundamental ideas into mathematics including a "computational" approach to real numbers. The American analyst, E. Bishop significantly advanced Brouwer's agenda in his book *Foundations of Constructive Analysis*, 1967.

Bishop shows that we can define all real numbers in terms of two fundamental ideas – the *rationals* and *computable functions* from $\mathbb{N}$ to the rationals $\mathbb{Q}$. We can implement his ideas in OCaml. You will be doing this in PS3. It is an elegant and important problem set that is also relatively straight forward in OCaml.

We start with these key concepts from Bishop & Bridges Chapter 2 of *Constructive Analysis*, available from the course web page (by permission of Spring-Verlag).

Def. 2.1	Regular sequence of rationals, equality of reals.
Def. 2.4	Canonical bounds and arithmetic operations (plus, times, max, minus, injection of $\mathbb{Q}$, α^*).
Prop. 2.5	$x + y$, $x * y$, $max\{x, y\}$, $-x$, α^* are reals.
Prop. 2.6	Algebraic properties of the reals

Intuition behind Bishop's definition of a real number

Why does the idea that a real number is a sequence of rational numbers, unbounded perhaps, make sense? We will examine it for $\sqrt{2}$, a real number known to be irrational.

We have Google access to at least a million digits of $\sqrt{2}$. The first 50 are these: 1.4142135623730950488016887242096980785696718753 7694.

We have a fast way of computing these in OCaml thanks to Mark Bickford.

This definition seems to be simply a *computational decimal expansion.* Why not use that as a definition? Indeed Turing proposed it and then retracted – proposal 1936, retracted 1937. See Bishop problem 9 page 62.

Real number presentation: $x_1 \pm 1,\ x_2 \pm 1/2,\ x_3 \pm 1/3$, ...

$$
\begin{array}{cc}
[_0\ 1\ ]_2 & \pm 1 \\
[_{0.9}\ 1.4\ ]_{1.9} & \pm 1/2 \\
[_{1.08}\ 1.41\ ]_{1.71} & \pm 1/3 \\
[\ 1.414\ ] & \pm 1/4 \\
[\ \ ] & \pm 1/5 \\
\vdots &
\end{array}
$$

The intervals overlap