CS3110 Fall 2013 Lecture 11: The Computable Real Numbers, $\mathbb{R}$ (10/3)

Robert Constable

1 Lecture Plan

- More about the rationals
  - dependent types
  - enumerating $\mathbb{Q}$ ($\mathbb{Q}$ is **countable**)
- Function inverses
  - bijections
  - one-one correspondence (equipollent types)
- Cautionary note
  - $\mathbb{Z}, \mathbb{Z}^+, \mathbb{Q}, \mathbb{R}$ are **mathematical types** whereas `int` is a **partial type** in OCaml
- Real numbers (arbitrary precision floats)
  - central concept in mathematics
  - crisis of understanding in 1800s
- Computable reals a la Bishop and Markov
  - Courant calculus book
  - Real analysis book
  - The "number line" and geometry

- Equality and arithmetic on $\mathbb{R}$
  - equality definition
  - canonical bounds
  - addition, multiplication

2 More about the rationals, $\mathbb{Q}$

We saw that the mathematical type $\mathbb{Z} \times \mathbb{Z} - \{0\}$ captures our intuitive idea about the rationals very well, BUT OCaml can't define this type. The best we can do is use a Boolean function `rational : int * int → bool` to help us.

There are programming languages under development which can define $\mathbb{Q}$, e.g. Agda, Coq, Nuprl, F*,.... They use **dependent types** such as $\{z : int * int \mid snd(z) \neq 0\}$.

Notice also that we can define an ordering on $int * int$ that allows us to "list" $int * int$ and thus enumerate $\mathbb{Q}$. For example, order (m, n) by

1. $|m| + |n|$, e.g. by absolute value
2. then order by value m
3. then by value n

Then eliminate

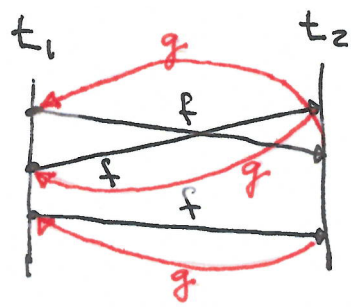
4. $n = 0$ cases, then
5. keep only $n > 0$, then
6. divide m, n by gcd of m and n.

$$(0,1), (-1,1), (0,2), (1,1), (1,2), (2,1), (3,1), \ldots$$

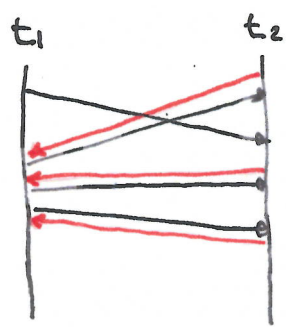
To talk precisely about enumeration, we use these definitions, given types t_1, t_2 and functions

$$f : t_1 \to t_2 \qquad\qquad g : t_2 \to t_1$$

1. If $\forall x : t_1.\big(\, g\,(f\ x) = x\,\big)$ then g **is the left inverse of** f
2. and f **is the right inverse of** g



3. A function f which has g as both a right and left inverse is said to have an inverse, and a function with an inverse is called a **bijection** or a 1-1 correspondence.



4. When there is a bijection between t_1 and t_2, we say that the types are **equipollent** or in **one-one correspondence**.

Definition: Any type equipollent with $\mathbb{Z}$ is **countable**.

Fact: $\mathbb{Q}$ is countable, $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are equipollent.

In type theory, these functions are all computable and total, e.g. terminate on all inputs.

3 Cautionary Note

The mathematical type $\mathbb{Z}$ is not the same as OCaml's `int` type because `int` is a **partial type**. OCaml does not have any total types. But in some discussions we might overlook this distinction. Only one of the modern type theories used in computer science has partial types, that is Constructive Type Theory (CTT).

As we examine the real numbers, $\mathbb{R}$, we will use mathematical types, and we note that these can be directly connected to OCaml partial types.

4 Real Numbers (Arbitrary Precision Floats)

Floating point numbers are central to scientific computing and computational geometry, two large applied areas of computer science – or better said, two areas of computer science with very wide application in engineering, physics, computational biology, etc.

Real numbers are of central concern in mathematics, e.g. in real and complex analysis, geometry, and algebra. The lack of a precise understanding of these numbers led to a so called *crisis in mathematics* in the 1800s.

Before the "crisis" the truth of mathematical results rested on the belief

that the world was mathematically designed and the results of real analysis were justified by nature as was "clear and obvious from their natural applicability."

All this started to go wrong when mathematicians "discovered" contradictory results about functions on the reals.

Cauchy believed that all continuous functions were differentiable – until 1854 results of Riemann.

In his *Course on Analysis*, Cauchy claimed that $F(x) = \sum_{i=1}^{\infty} u_i(x)$ is continuous if the series converges and the u_i are continuous. (see Klein *Math Thought* ... p. 964). Abel fixed the error in 1826.

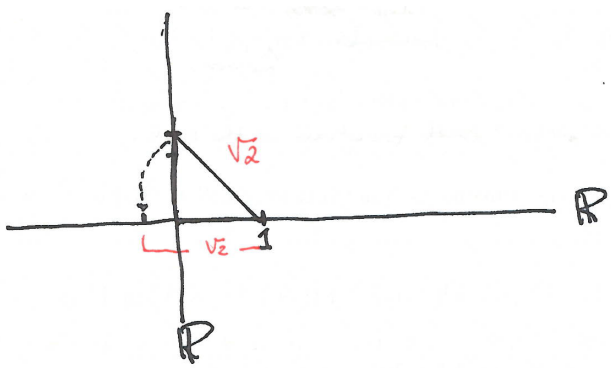
5 Defining the Real Numbers $\mathbb{R}$

We take our computational definition from Errett Bishop *Foundations of Constructive Analysis*, 1967.

Many books on analysis simply give the axioms, say 9 axioms for a field, 4 for order and one completeness axiom (every non empty set of real numbers which has an upper bound has a least upper bound). We could put these "specifications" into an OCaml module as a start, but it would not tell us how to build them and compute with them.

Other famous books on analysis, say by Courant, simply say: "the totality of all real numbers is represented by the **totality of all finite and infinite decimals**."

Courant stresses that these finite and infinite decimals are the real numbers and we can see this by establishing a correspondence with the points on the **number line** from geometry.



5.1 Bishop's definition of $\mathbb{R}$

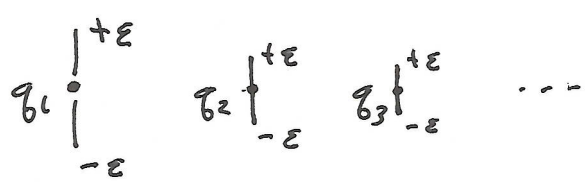
Definition: A sequence $\{x_n\}$ of rational numbers is **regular** iff $|\, x_m - x_n \,| \leq 1/m + 1/n$.

A **real number** is a regular sequence of rational numbers.

Two real numbers are **equal** $\quad \{x_n\} = \{y_n\} \quad$ iff $\quad |\, x_n - y_n \,| \leq 2/n$.

This notion of equality suggests we can think about the real as the kind of sequence of approximations one might make in a laboratory notebook:

> I measured $q_1 \pm \varepsilon_1,\ q_2 \pm \varepsilon_2, \ldots$ where q_i are finite decimal approximations made "within epsilon" and we keep increasing the accuracy, the number of digits, and decreasing the tolerance, the $2/n$ as n increases.



> The rationals q_i are the ith approximation of the real $r = \{q_i\}$. (Note, not all approximations need be nested like this, just the lab notebook kind.)

6 Arithmetic Operations on $\mathbb{R}$

To carry out the arithmetic operations, it is useful to have a **canonical bound** k to a real $\{x_n\}$. We want $|\, x_n \,| < k$ for all n.

Take $k_{\{x_n\}}$ = least positive integer greater than $|\, x_1 \,| + 2$.

(**Note**, this is NOT given by a function $\mathbb{R} \to \mathbb{N}$, there are no such functions in the sense that if $\{x_n\} = \{y_n\}$ in $\mathbb{R}$, then $k_{\{x_n\}} = k_{\{y_n\}}$.)

Definition:

- $\{x_n\} + \{y_n\} = \{x_{2\cdot n} + y_{2\cdot n}\}$
- $max\{\, \{x_n\}, \{y_n\} \,\} = \{\, max\{x_n, y_n\}\}$
- $-\{x_n\} = \{-x_n\}$
- $q^* = \{q_i\}$ each $q_i = q$
- $\{x_n\} * \{y_n\} = \{x_{2kn} * y_{2kn}\}$ where $k = max\{k_{\{x_n\}}, k_{\{y_n\}}\}$, and k is the canonical bound.

7 Properties of $\mathbb{R}$

Fact 1. Equality is an equivalence relation.

Bishop proves this from the following basic fact.

Lemma 1. $x = \{x_n\} = \{y_n\} = y$ iff for each positive integer k, we can find a positive integer N_k such that

$$|\, x_n - y_n \,| \leq 1/k \text{ for any } n \geq N_k$$

Proof

If $x = y$ then take $N_j = 2 \cdot j$
Conversely if for each $k \in \mathbb{Z}^+$ there is N_k,
then let $m \geq max\{k, N_k\}$, then

$$\begin{aligned} |\, x_n - y_n \,| &\leq |\, x_n - x_m \,| + |\, x_m - y_m \,| + |\, y_m - y_n \,| \\ &\leq (1/n + 1/m) + 1/k + (1/n + 1/m) \\ &< 2/n + 3/k \end{aligned}$$

Qed