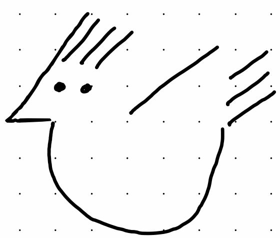
Reals

in

Agda



Robert Atkey ◆ University of Strathclyde ◆ 2021-06-10

Objective: Construction of (a setoid of) real numbers in Agda

Motivation:

- Modelling Artificial Neural Nets
- Modelling Probabilistic Systems
- Differentiable Programming Languages
- Modelling Cyber-Physical systems.
- It's fun

Plan:

[Russell O'Connor, 2007]

1. Metric spaces

   $X = (|X|$ ← a set of points

   $d : |X| \times |X| \to \mathbb{R}^{\geq 0})$ ← a distance function

2. Define <u>completion</u> of a metric space $\mathcal{C}(X)$

3. Define the metric space of rationals $\mathbb{Q}$.

4. $\mathbb{R} = \mathcal{C}(\mathbb{Q})$

Completion

Q: What is the difference between rationals and reals?

A1: Real numbers include limits of converging sequences:

$x_1, x_2, x_3, \ldots$ Cauchy sequence

s.t. $\forall \varepsilon > 0.\ \exists N.\ \forall m, n > N.\ |x_m - x_n| < \varepsilon$

x is a limit point if...

$\forall \varepsilon > 0.\ \exists N.\ \forall m > N.\ |x_m - x| < \varepsilon$

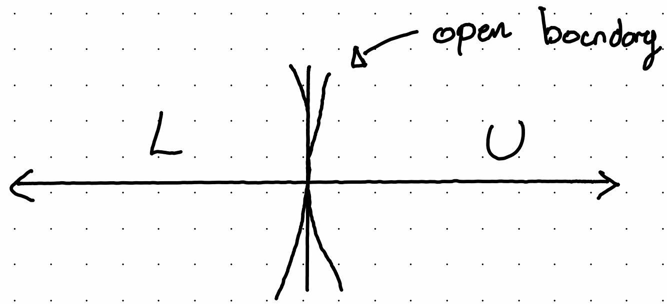
Makes sense in any metric space

A2: Every non-empty bounded $X \subseteq \mathbb{R}$ has a suprema (least upper bound)

$\{ x \mid x^2 < 2 \}$

Construction I: Dedekind Cuts

- A real number is (represented as) a pair of sets $L, U \subseteq \mathbb{Q}$



s.t.

- L, U are inhabited
- $\forall q < r.\ r \in L \Rightarrow q \in L$ (L is lower).
- $\forall q.\ q \in L \Rightarrow \exists r.\ q > r \wedge r \in L$ (L is open)
- U is upper and open
- $L \cap U = \emptyset$ (disjoint)
- $\forall q < r.\ q \in L \vee r \in U$ (no gap "located")

Easy to construct suprema.

Construction II: Cauchy Sequences

- Represent reals by Cauchy sequences
  $x_1, x_2, \ldots \quad \underline{\forall \varepsilon > 0}\,.\,\underline{\exists N}\,.\,\forall m,n > N\,.\,|x_m - x_n| < \varepsilon$
- Rationals are constant sequences

- Variants: (constructively assuming a modulus of continuity)
  - Regular sequences:
    $x_1, x_2, \ldots \quad$ s.t. $\forall m,n\,.\,|x_m - x_n| \leq \frac{1}{m} + \frac{1}{n}$
    $\left(\text{or } \frac{1}{2^m} + \frac{1}{2^n}\right)$
  - Regular Functions:
    $x : \underline{\mathbb{Q}^+} \to \mathbb{Q} \quad$ s.t. $\forall \varepsilon_1, \varepsilon_2\,.\,\underbrace{|x(\varepsilon_1) - x(\varepsilon_2)|} \leq \varepsilon_1 + \varepsilon_2$

- Easy to construct limits of sequences

Metric Spaces

sometimes includes $+\infty$

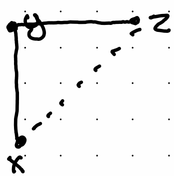
$X = (|X|,$ set of points

$d : |X| \times |X| \longrightarrow \mathbb{R}^{\geq 0})$ distance function

s.t. $d(x,y) = 0 \iff x = y$

$d(x,y) = d(y,x)$ symmetry

$d(x,z) \leq d(x,y) + d(y,z)$ triangle



What do we require of $\mathbb{R}^{\geq 0}$?

What do we require of $\mathbb{R}^{\geq 0}$?

- Representation of positive rationals with 0
- Ordering
- Addition

triangle inequality

- (Infinite) suprema — for cartesian products + fn spaces
- Truncated subtraction — for the completion monad.

The 'Upper Reals'

- Represent distances as <u>upper</u> Dedekind cuts.

  $\Longrightarrow$ a real number 'x' is represented by the set of all $q \in \mathbb{Q}^+$ greater or equal to it $\leadsto$ so these are upper sets

- Choice: open or closed?

$U : \mathbb{Q}^+ \to \Omega$

$U : \mathbb{Q}^+ \to Set$

1. Open : $\forall q . q \in U \Rightarrow \exists r < q . r \in U$
2. Closed : $\forall q . (\forall r . q + r \in U) \Rightarrow q \in U$

In a predicative setting, closed is more useful

- Any set can be made closed, but we require impredicativity to find the smallest open set containing a given set.

Upper Reals

```
record ℝᵘ : Set₁ where
  no-eta-equality
  fields
    contains : ℚ⁺ → Set
    upper    : ∀ {q₁ q₂} → q₁ ≤ q₂ → contains q₁ → contains q₂
    closed   : ∀ {q} → (∀ r → contains (q + r)) → contains q
```

```
record _≤_ (x y : ℝᵘ) : Set where
  field
    *≤* : ∀ {q} → y .contains q → x .contains q
```

$\Longrightarrow$ No constructive content in the sense that we cannot get rationals approximations from an upper real

<u>Aside</u> "Upper Semicontinuous Reals"

- Constructively, one-sided reals are not equivalent to two-sided reals (cannot just take the negation)

- So what are these 'Upper Reals'?

  In a sheaf topos over a topological space X,
  upper reals (externally) $\Leftrightarrow$ upper semicontinuous fns
  $U \to \mathbb{R}^{-\infty,\infty}$ (externally)

  $\forall t \in \mathbb{R}^{-\infty,\infty}.\ \{x \mid f(x) < t\}$ is open in U

[Reichman 1982]

Arithmetic on Upper Reals

- For any $U \subseteq \mathbb{Q}^+$, an upper set let
$$\mathrm{Clo}(U) = \lambda q. \forall r. (q+r) \in U$$

- Define
$$0 = \lambda q. \top$$
$$\infty = \lambda q. \bot$$
$$\underline{r} = \lambda q. r \le q$$
$$U_1 + U_2 = \mathrm{Clo}\left(\lambda q. \Sigma q_1 \Sigma q_2. \; q_1 + q_2 \le q \times U_1 q_1 \times U_2 q_2\right)$$
$$U_1 \times U_2 = \mathrm{Clo}\left(\lambda q. \Sigma q_1 \Sigma q_2. \; q_1 q_2 \le q \times U_1 q_1 \times U_2 q_2\right)$$

- This is <u>nearly</u> a semiring except that $0 \times \infty = \infty$

Truncating subtraction

$$U_1 \ominus U_2 = \lambda q. \forall q'. U_1 q' \to U_2(q+q')$$

(not clear how to define this with open sets predicatively)

⌜Aside: the definition of $+$ and $\ominus$ are very similar to the Day tensor product and its closure in presheaves over monoidal categories.

With the reverse ordering, this makes $\mathbb{R}^{\cup}$ symmetric monoidal closed, which we are choosing to see as posetal, but maybe there is interest in distinguishing morphisms⌟.

Suprema

$$\mathrm{sup} : (I : \mathrm{Set}) \to (I \to \mathbb{R}^{u}) \to \mathbb{R}^{u}$$
$$\mathrm{sup}\ I\ S = \lambda q.\ \forall i.\ S\ i\ q$$

$\Rightarrow$ an Archimedean principle:

$$\forall y.\ \ y \leq \mathrm{sup}\ \mathbb{Q}^{+}\ (\lambda \varepsilon.\ y \ominus \varepsilon)$$

"nothing infinitesimally below y"

Infima

$$\mathrm{inf} : (I : \mathrm{Set}) \to (I \to \mathbb{R}^{u}) \to \mathbb{R}^{o}$$
$$\mathrm{inf}\ I\ S = \mathrm{Clo}(\lambda q.\ \underline{\underline{\Sigma i}}.\ S\ i\ q)$$

$\Rightarrow$ Approximation from above:

$$\forall y.\ \ y \simeq \mathrm{inf}\ (\Sigma q : \mathbb{Q}^{+}.\ y \leq q)\ (\lambda q.\ q)$$

- So now we have upper reals.

- Why not carry on and define two-sided Dedekind reals?

    1. In a predicative theory like Agda, they live in Set_1, not Set.

    2. Construction is limited to rationals (or similar) completing arbitrary metric spaces will be useful.

Metric Spaces (again)

$X = (|X|$: Set

$d : |X| \times |X| \longrightarrow \mathbb{R}^{\infty})$ allows ∞ distances

s.t. $d(x,x) = 0$ (!)

- $d(x,y) = d(y,x)$
- $d(x,z) \leq d(x,y) + d(y,z)$

$x \approx y = d(x,y) \leq 0$

Category of Metric Spaces (Met)

Objects : $(\underset{\cdot}{|X|}, \underset{\cdot}{d_X})$

Morphisms : non-expansive maps.

$$|f| : |X| \longrightarrow |Y|$$

s.t. $\forall x_1, x_2.\ d_Y(fx_1, fx_2) \leq d_X(x_1, x_2)$

"short maps"

Why not : • Lipschitz continuous ? ⟵ recover this.

{ • Uniformly continuous ?

- Continuous ? } don't get a nice category

Products in Met

$$X \times Y = (|X| \times |Y|, \quad d((x_1,y_1),(x_2,y_2)) = \max(d_X(x_1,x_2), d_Y(y_1,y_2)))$$

(cartesian product)

$$T = (\{*\}, d(*,*) = 0)$$

- $$X \otimes Y = (|X| \times |Y|, \quad d((x_1,y_1),(x_2,y_2)) = d_X(x_1,x_2) + d_Y(y_1,y_2))$$

- $$X \multimap Y = (|X| \to_{ne} |Y|, \quad d(f_1,f_2) = \sup |X| \; (\lambda x.\, d_Y(f_1\, x)(f_2\, x)))$$

Scaling

$$[q] : \mathrm{Met} \to \mathrm{Met} \qquad q \in \mathbb{Q}^+$$

$$[q]X = (|X|,\ d_{[q]X}(x_1, x_2) = q \cdot d(x_1, x_2)).$$

$[q]X \to_{ne} Y$ $\quad d(fx_1, fx_2) \leq q \cdot d(x_1, x_2)$

Lipschitz cont with constant q.

a graded-! modality :

- wk : $q_1 \leq q_2 \to [q_1]X \to_{ne} [q_2]X$
- derelict : $[1]X \to_{ne} X$

  dig : $[q_1 q_2]X \to_{ne} [q_1][q_2]X$

  dup : $[q_1 + q_2]X \to_{ne} [q_1]X \otimes [q_2]X$

  disc : $[0]X \to_{ne} 1$ terminal object.

Rationals

$$\mathbb{Q}^{spc} = (\underbrace{\mathbb{Q}}, d_{\mathbb{Q}^{spc}}(q_1, q_2) = |q_1 - q_2|)$$

Arithmetic

$$\begin{cases} \underline{0} : T \to_{ne} \mathbb{Q}^{spc} \\ \underline{+} : \mathbb{Q}^{spc} \otimes \mathbb{Q}^{spc} \to_{ne} \mathbb{Q}^{spc} \end{cases}$$

$$\text{negate} : \mathbb{Q}^{spc} \to_{ne} \mathbb{Q}^{spc}$$

"graded" Abelian group:

$$\begin{tikzcd}
{[2]\mathbb{Q}^{spc}} \arrow[r, "dup"] \arrow[dd] & \mathbb{Q}^{spc} \otimes \mathbb{Q}^{spc} \arrow[d, "id \otimes negate"] \\
 & \mathbb{Q}^{spc} \otimes \mathbb{Q}^{spc} \arrow[d, "\underline{+}"] \\
T \arrow[r, "\underline{0}"] & \mathbb{Q}^{spc}
\end{tikzcd}$$

Scaling and Multiplication

$$\mathrm{scale} : (q : \mathbb{Q}^{+}) \to [q]\,\mathbb{Q}^{spc} \to_{ne} \mathbb{Q}^{spc}$$

$$\times : \forall a\, b.\ [a]\left(\mathbb{Q}^{spc}[-b, b]\right) \otimes [b]\left(\mathbb{Q}^{spc}[-a, a]\right) \to_{ne} \mathbb{Q}^{spc}$$

$$\mathrm{recip} : \forall a.\ \left[\tfrac{1}{a^2}\right] \mathbb{Q}^{spc}[a, \infty) \to_{ne} \mathbb{Q}^{spc}$$

Completion

Let X be a metric space

a Regular Function is

$$x : \mathbb{Q}^+ \to X$$

s.t. $\forall \varepsilon_1, \varepsilon_2.\ d_X(x(\varepsilon_1), x(\varepsilon_2)) \leq \varepsilon_1 + \varepsilon_2$

Intuition: $x(\varepsilon)$ is an approximation of 'x' to within ε.

$\mathcal{C}(X) = ($ Regular Functions $\mathbb{Q}^+ \to X$

$$d_{\mathcal{C}(X)}(x, y) =$$

$$\sup\ (\mathbb{Q}^+ \times \mathbb{Q}^+)\ (\lambda(\varepsilon_1, \varepsilon_2).\ d_X(x(\varepsilon_1), y(\varepsilon_2)) \ominus (\varepsilon_1 + \varepsilon_2))$$

Properties of Completion.

1. A functor $\mathcal{C} : \mathrm{Met} \longrightarrow \mathrm{Met}$ ✓

2. A monad : $\eta : X \longrightarrow_{ne} \mathcal{C}(X)$
   $\mu : \mathcal{C}(\mathcal{C}(X)) \longrightarrow_{ne} \mathcal{C}(X)$ ✓

3. Idempotent, so $\mathcal{C}(\mathcal{C}(X)) \cong \mathcal{C}(X)$ ✓

4. Monoidal : $\mathcal{C}X \otimes \mathcal{C}Y \xrightarrow{\cong}_{ne} \mathcal{C}(X \otimes Y)$ ✓

5. Distributes over scaling: $[q](\mathcal{C}X) \longrightarrow_{ne} \mathcal{C}([q]X)$ ✓

Reals as a Metric Space

$$\underline{\mathbb{R}^{spc}} = \underline{\mathcal{C}(\mathbb{Q}^{spc})}$$

Arithmetic:

$$\underline{0} = \Big(\underbrace{T \xrightarrow{\underline{0}} \mathbb{Q}^{spc}} \underbrace{\xrightarrow{\eta} \mathcal{C}(\mathbb{Q}^{spc}) = \mathbb{R}^{spc}} \Big)$$

$$\underline{+} = \Big(\mathbb{R}^{spc} \otimes \mathbb{R}^{spc} = \mathcal{C}(\mathbb{Q}^{spc}) \otimes \mathcal{C}(\mathbb{Q}^{spc}) \to \mathcal{C}(\mathbb{Q}^{spc} \otimes \mathbb{Q}^{spc}) \xrightarrow{\mathcal{C}(\underline{+})} \mathcal{C}(\mathbb{Q}^{spc}) = \mathbb{R}^{spc} \Big)$$

similarly for negation. Monoidality means that abelian group property carries over.

Multiplication and Reciprocal

$$\underline{\times} : \forall a\ b.$$
$$[a](\mathbb{R}^{spc}[-b, b]) \otimes [b](\mathbb{R}^{spc}[-a, a])$$
$$\longrightarrow_{ne}$$
$$\mathbb{R}^{spc}$$

$$\text{recip} : \forall a.\ [\tfrac{1}{a^2}](\mathbb{R}^{spc}[a, \infty)) \longrightarrow_{ne} \mathbb{R}^{spc}$$

Forgetting Metric structure

$$\underline{\underline{\mathbb{R}}} = |\mathbb{R}^{spc}|$$

$$+ : \mathbb{R} \to \mathbb{R} \to \mathbb{R}$$

$$x + y = \underbrace{|\pm|}(x, y)$$

Forget the non-expansive m.s.

$$x \cdot y : \mathbb{R} \to \mathbb{R} \to \mathbb{R}$$

$$\underbrace{x \cdot y = ?}$$

Defining total multiplication

$$\text{multiply} : \forall a\ b.\ [a]\,\mathbb{R}^{spc}[-b, b] \otimes [b]\,\mathbb{R}^{spc}[-a, a] \to_{ne} \mathbb{R}^{spc}$$

To multiply 'x' and 'y':

- Need to bound 'x' and 'y':

  $$\text{bound} : \mathbb{R} \to \Sigma q.\ \mathbb{R}[-q, q]$$

  - find a bound on the input via $x(\frac{1}{2}) \pm \frac{1}{2}$
  - clamp values of $x(\varepsilon)$ to be within that bound
  - result is equal to original as a real number.

- Then multiply the bounded numbers.

Looking forward

1. Defining the elementary functions on $\mathbb{R}$:

   - exp
   - sin
   - ln
   - arctan

   O'Connor defines these via alternating decreasing series

   - Requires a lot of reasoning about rationals
   - Agda's automation is very weak here.

2. Quantitative Algebraic Theories
(Mardare, Panangaden, Plotkin; 2016)

- Equational theories with <u>approximate</u> equalities:

  $x =_\varepsilon y$ "x and y are equal up to ε"

- Algebras for these theories live in Met.
- Examples:
  - Probability distributions with Kantorovich metric
  - Sets with Hausdorff metric.
- Completion extends them to complete metric spaces
- Relatively easy to encode using inductive families.

3. Integration

(O'Connor and Spitters, 2010)

- Define step functions as a monad $\mathfrak{S}$
- sum : $\mathfrak{S}(\mathbb{R}^{spc}) \longrightarrow_{ne} \mathbb{R}^{spc}$
- (I think) $\mathfrak{S}$ arises from a quantitative eq. theory.
- unifcon : $T \longrightarrow_{ne} \mathcal{C}(\mathfrak{S}(\mathbb{Q}^{spc})) \longrightarrow_{ne} \mathfrak{S}(\mathcal{C}(\mathbb{Q}^{spc}))$

Conclusion

https://github.com/bobatkey/agda-metric-reals

- Two formalisations of "the" reals in Agda:
  - Upper reals, for distances · $\mathbb{Q}^+ \to \mathrm{Set}$
  - Reals as regular functions ·
- Completion as a monad ·
- Hopefully applications to cyber-physical and probabilistic modelling in Agda.

Thanks!