EDAA40

Discrete Structures in Computer Science

Numbers

Jörn W. Janneck, Dept. of Computer Science, Lund University

Let's look at some of the most basic objects of maths: numbers.

The point is to use some of the tools we have
talked about in this course.

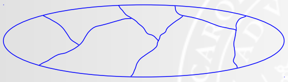
recap: equivalence relations

A binary relation $\approx \subseteq A \times A$ is an *equivalence relation* iff it is

1. reflexive
2. symmetric
3. transitive

recap: partitions

Given a set A, a *partition of A* is a set of pairwise disjoint sets $\{B_i : i \in I\}$, such that $A = \bigcup_{i \in I} B_i$



recap: equivalence class, quotient set

Given a set A and an equivalence relation $\approx$ on A, for any $a \in A$ we define the *equivalence class of a* $[a]_\approx$ as $[a]_\approx = \{b \in A : a \approx b\}$

Alternative syntax:

$[a]$ } when the relation is understood

SLAM { $|a|$, $|a|_\approx$

Given a set A and an equivalence relation on A, the *quotient (set)* $A/\approx$ is defined as $A/\approx\ = \{|a|_\approx : a \in A\}$

$\mathbb{N}$: the natural numbers

Remember the von Neumann construction of the natural numbers: $0 = \emptyset$, $n^+ = n \cup \{n\}$

$0 = \emptyset$

$1 = 0^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$

$2 = 1^+ = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$

$3 = 2^+ = ... = \{0, 1, 2\}$

...

We can establish an order on them:

$a \leq b \text{ iff } a = 0 \text{ or } (a = c^+ \text{ and } b = d^+ \text{ and } c \leq d)$

$\mathbb{N}$: the natural numbers

Addition and multiplication:

$$add(a,b) = \begin{cases} a & \text{for } b = 0 \\ add(a^+, c) & \text{for } b = c^+ \end{cases}$$

$$mul(a,b) = \begin{cases} 0 & \text{for } b = 0 \\ add(a, mul(a,c)) & \text{for } b = c^+ \end{cases}$$

We shall henceforth write

$a+b$	instead of	$add(a,b)$
$a \cdot b$ or ab	instead of	$mul(a,b)$

$\mathbb{N}$: the natural numbers

How do we actually know that **the set of all natural numbers** exists?

Because ZF say so.

There is actually an axiom which simply postulates that the set of natural numbers exists, the **Axiom of Infinity**:

$$\exists X : (\emptyset \in X \wedge \forall y : (y \in X \Rightarrow \{y, \{y\}\} \in X))$$

$\mathbb{Z}$: the integers

So how do we get integers, if all we got are

- the natural numbers and
- addition and comparison on them?

We represent each integer as a pair (a,b) of natural numbers, with the intuition that (a,b) represents the "difference" a-b. (Note that we have not defined subtraction yet!)

For example, -1 would be (3, 4). But it would also be (7,8).
How can we build a set that represents each integer by exactly one element?

First, when do two pairs (a,b) and (c,d) represent the same integer? When a-b = c-d.
But we do not have subtraction (yet), so we say

$$(a,b) \equiv (c,d) \text{ iff } a+d = c+b$$

$\mathbb{Z}$: the integers

So now we got pairs of natural numbers: $\mathbb{N} \times \mathbb{N}$

... and an equivalence relation on them: $(a, b) \equiv (c, d)$ iff $a + d = c + b$

Weren't we supposed to get integers? Here they are:

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \equiv$$

The integers are just the equivalence classes of the pairs of natural numbers under that equivalence relation.

$$[(3,4)] = [(7,8)] = [(0,1)] = -1$$
$$[(5,2)] = [(11,8)] = [(3,0)] = 3$$
$$[(4,4)] = [(11,11)] = [(0,0)] = 0$$

$\mathbb{Z}$: the integers

What about operations on $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \equiv$?

$(a, b) \equiv (c, d)$ iff $a + d = c + b$

$$[(a,b)] + [(c,d)] = [(a+c, b+d)]$$
$$[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$$
$$[(a,b)] \leq [(c,d)] \text{ iff } a+d \leq c+b$$

What about subtraction? We will define it by addition of the negative. So first:

$$[(a,b)]' = [(b,a)]$$

With this we can define:

$$[(a,b)] - [(c,d)] = [(a,b)] + [(c,d)]' = [(a,b)] + [(d,c)] = [(a+d, b+c)]$$

$\mathbb{Q}$: the rational numbers

Now we have integers, and we want to construct the rational numbers, i.e. fractions. Let's try the pairs-with-equivalence-relation trick again.

Rational numbers are typically represented as fractions $\frac{p}{q}$ with $q \neq 0$.

As with the differences we used to represent integers, different fractions represent the same rational number, e.g. $\frac{5}{7} = \frac{10}{14} = \frac{45}{63} = \frac{-5}{-7}$

When are two fractions equal? $\frac{p}{q} = \frac{r}{s}$ iff $ps = rq$

So if we represent rational numbers as pairs of integers (p, q), then this is our equivalence relation on those pairs:

$$(p, q) \equiv (r, s) \text{ iff } ps = rq$$

$\mathbb{Q}$: the rational numbers

Now we can construct the rational numbers simply like this:

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \equiv \qquad (p,q) \equiv (r,s) \text{ iff } ps = rq$$

Let us look at operations:

$$[(p,q)] + [(r,s)] = \quad [(ps + rq, qs)]$$
$$[(p,q)] \cdot [(r,s)] = \quad [(pr, qs)]$$
$$[(p,q)]' = \quad [(p', q)]$$
$$[(p,q)] \leq [(r,s)] \text{ iff } \quad (ps \leq rq \text{ if } qs > 0) \text{ or } (ps \geq rq \text{ if } qs < 0)$$

Division, like subtraction before, we define by multiplication by the inverse:

$$[(p,q)]^{-1} = \ [(q,p)] \text{ if } p \neq 0$$
$$[(p,q)] \div [(r,s)] = \ [(p,q)] \cdot [(r,s)]^{-1} = [(p,q)] \cdot [(s,r)] = [(ps, qr)] \text{ if } r \neq 0$$

$\mathbb{R}$: the real numbers

So now we have fractions. But what about the other stuff, like $\sqrt{2}$?
Things that aren't fractions.

$\mathbb{R}$: the real numbers

So now we have fractions. But what about the other stuff, like $\sqrt{2}$?
Things that aren't fractions.

What? Wait --- why isn't that a fraction?

Okay, suppose it was.

$$\sqrt{2} = \frac{p}{q} \text{ for } p \perp q$$
$$2 = \frac{p^2}{q^2}$$
$$2q^2 = p^2$$

This means p must be even, so let's say $p = 2r$

$$2q^2 = 4r^2$$
$$q^2 = 2r^2$$

So q is even, too. So p and q aren't coprime. Kapow. Moving on...

$\mathbb{R}$: the real numbers

So now we have fractions. But what about the other stuff, like $\sqrt{2}$?
Things that aren't fractions.

The rational numbers are dense, yet there are "holes" in them.
Very, very tiny holes. But VERY many of them.

So we define the real numbers to be just those holes.
Gaps between two sets of rational numbers that juuuust touch each other.
These are called *Dedekind cuts*, and they can be defined like this:

$$\mathbb{R} = \{(A,B) : A, B \subset \mathbb{Q}, A \cup B = \mathbb{Q}, \text{for all } x \in A \text{ there is } x' \in A \text{ with } x < x',\ \text{and for all } y \in B : x < y\}$$

So (A,B) is a partition of the rational numbers, such that A contains all the smaller numbers, and B all the larger ones. A also has no biggest number (it is open), while B may or may not have a smallest.

$\mathbb{R}$: the real numbers

$$\mathbb{R} = \{(A,B) : A, B \subset \mathbb{Q}, A \cup B = \mathbb{Q}, \text{for all } x \in A \text{ there is } x' \in A \text{ with } x < x',\ \text{and for all } y \in B : x < y\}$$

Since B is uniquely determined by A ($B = \mathbb{Q} \setminus A$) we can simplify this definition a little:

$$\mathbb{R} = \{A \subset \mathbb{Q} : A \neq \emptyset, \text{for all } x \in A \text{ there is } x' \in A \text{ with } x < x',\ \text{and for all } y \in \mathbb{Q} \setminus A : x < y\}$$

So the real numbers are the set of open lower (proper sub-) sections of the rational numbers.

$\mathbb{R}$: the real numbers

$$\mathbb{R} = \{A \subset \mathbb{Q} : A \neq \emptyset, \text{for all } x \in A \text{ there is } x' \in A \text{ with } x < x',\ \text{and for all } y \in \mathbb{Q} \setminus A : x < y\}$$

A real number is a partition of the rational numbers, such that A contains all the smaller numbers, and Q\A all the larger ones. A also has no biggest number (it is open), while Q\A may or may not have a smallest.

If it does, that's the one:

$$\left\{q \in \mathbb{Q} : q < \frac{1}{2}\right\} = \frac{1}{2}$$

If Q\A has a smallest element, the Dedekind cut does not actually represent a hole, but it represents just that rational number.

But now we also have numbers that aren't rational numbers:

$$\{q \in \mathbb{Q} : q \cdot q < 2 \text{ or } q < 0\} = \sqrt{2}$$

In this case, Q\A has no smallest element (as we have seen).
This cut, therefore, represents an **irrational number**.

$\mathbb{R}$: the real numbers

$$\mathbb{R} = \{A \subset \mathbb{Q} : A \neq \emptyset, \text{for all } x \in A \text{ there is } x' \in A \text{ with } x < x', \text{ and for all } y \in \mathbb{Q} \setminus A : x < y\}$$

So let's look at ops:

$$\begin{aligned} A + B &= \{a + b : a \in A, b \in B\} \\ -A = A' &= \{\cancel{-b : b \in \mathbb{Q}} \setminus A\} \\ &\quad \{-b : b \in \mathbb{Q} \setminus A,\ \text{exists } b' \in \mathbb{Q} \setminus A \text{ with } b' < b\} \end{aligned}$$

We will omit the rest, but they work similarly. Care needs to be taken to make sure the set has no upper bound, which often requires distinguishing several cases (e.g. when multiplying by a negative number).

number weirdness

The rational numbers are dense: between any two rationals there is always another rational number
Therefore, there are infinitely many rational numbers between any two rational numbers.

The same is true for the real numbers.

The real numbers are the "holes" between the rationals. Yet, there are MASSIVELY more real numbers than rational numbers.

Moreover, the rational numbers are **dense within the real numbers**
Between any two real numbers, there is a rational number.
In fact, there are infinitely many rational numbers between any two real numbers.