The nature of sets in computer science

Murdoch J. Gabbay, www.gabbay.org.uk

King's College London
Monday 29 September 2008

Thanks to Maribel Fernández

What is this talk about?

In this talk I'll give an overview of the mathematical foundations of computer science.

I'm Murdoch James Gabbay. Everybody calls me Jamie.

I do research in theoretical computer science. Maribel Fernández was my boss for a while.

I expect that you will find this talk ridiculously simple and obvious . . . then perhaps you'll blink, and suddenly it'll be ridiculously incomprehensible. That is typical of this kind of mathematics; do not be afraid to interrupt me with questions.

What is this talk about?

Welcome to my seminar in Advanced Research Topics.

I can’t predict who’ll be in my audience, so let me know if you know this stuff. If I get to the end of my slides, this means you’re expert and I’ll switch to the blackboard.

What is a set?

A set is a collection of objects.

$\{$Plato, Socrates, Aristotle$\}$ is a subset of the set of hellenic philosophers.

$\{$Jamie, Maribel, Michael, Dov$\}$ is a subset of the set of people who have worked at King's.

$\{$King's College$\}$ is a subset of the set of world-class academic institutions.

$\{\}$ (the empty set $\emptyset$) is a subset of . . . any other set.

We use sets all the time, informally.

Sets as a mathematical foundation

All the sets above were sets of concrete objects, or at least, they are sets of entities which we might associate with something we can see, touch, hear, taste, or smell. For example, it is debatable whether one should identify Jamie with Jamie's body, but at least the body gives us a useful illusion that Jamie is a single, definite thing that we can put in a set.

What about numbers? Groups and fields? λ-terms? Abstract syntax?

How do we model them?

Do they exist? Does mathematics exist?

What a simplest world in which we can practice mathematics?

Ordinals

A well-ordered collection is a carrier collection with an order on it $<$ which is transitive, total, and well-founded.

Transitive: $x < y$ and $y < z$ imply $x < z$.

Total: either $x < y$ or $y < x$.

Well-founded: $x_1 > x_2 > x_3 > x_4 > \ldots$ is impossible.
(No infinite descending chains.)

An ordinal is an isomorphism class of well-ordered collections. That is, we take the carrier up to isomorphism.

(Ordinals were introduced by Cantor.)

Pictures of ordinals

Examples of ordinals (in ascending order) are:

- The ordinal 1, pictured as '$\bullet$'.
- The ordinal 2, pictured as '$\bullet < \bullet$'.
- The ordinal ω, pictured as '$\bullet < \bullet < \bullet < \ldots$' (the natural numbers, ordered in their natural order, are in this equivalence class).
- The ordinal $\omega + 1$, pictured as '$(\bullet < \bullet < \bullet < \ldots) < \bullet$' (a countable list of elements 'going on forever', plus one more element greater than all others).
- 'The first uncountable ordinal' (the least upper bound of all the countable ordinals). As is standard, we write this ordinal ω_1.

The cumulative hierarchy $\mathcal{U}$

Let's build a mathematical universe. We believe in ordinals: let α and β range over ordinals.

- We believe in the empty set: $\emptyset \in \mathcal{U}_1$.
- We believe in sets: if $U \subseteq \mathcal{U}_\alpha$ and $\alpha < \beta$ then $U \in \mathcal{U}_\beta$.

If $x \in \mathcal{U}$ write $\mathsf{rank}(x)$ for the least ordinal α such that $x \in \mathcal{U}_\alpha$. Such a least ordinal exists, since by assumption there is no infinite descending chain of ordinals.

The cumulative hierarchy $\mathcal{U}$

Let's just prove that by contradiction. Suppose $x \in \mathcal{U}$ and suppose there is no unique least ordinal α such that $x \in \mathcal{U}_\alpha$.

$x \in \mathcal{U}_\alpha$ for some α.

Choose any $\alpha' < \alpha$ such that $x \in \mathcal{U}_{\alpha'}$.

Iterate this, so we obtain an infinite descending chain. Contradiction.

Von Neumann numerals

- We identify 0 with $\emptyset$.
- We identify $i+1$ with $i \cup \{i\}$.

So

$$1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\},$$

and in general

$$n = \{n' \mid n' < n\}.$$

$\mathsf{rank}(n) = n + 1$. That is, $n \in \mathcal{U}_{n+1}$.

Write $\mathbb{N}$ for $\{0, 1, 2, 3, \ldots\}$.

$n \in \mathcal{U}_{n+1}$ for all n, so $\mathbb{N} \subseteq \mathcal{U}_\omega$. So $\mathsf{rank}(\mathbb{N}) = \omega + 1$.

An example

$$0 = \emptyset \in \mathcal{U}_1$$

$$0 \in \mathcal{U}_2 \qquad 1 = \{0\} \in \mathcal{U}_2$$

$$1 \in \mathcal{U}_3 \qquad 2 = \{1, 0\} = \{\{\{\}\}, \{\}\} \in \mathcal{U}_3 \qquad \{\{\{\}\}\} \in \mathcal{U}_3$$

$$\vdots$$

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\} \in \mathcal{U}_{\omega+1}$$

$$\mathbb{N} \cup \{\mathbb{N}\} \in \mathcal{U}_{\omega+2}$$

Set of rational numbers $\mathbb{Q} \in \mathcal{U}_{\omega+3}$

$$\vdots$$

Set of real numbers $\mathbb{R} \in \mathcal{U}_{\omega_1+1}$

Kuratowski pairs

Kuratowski pairs: $(x, y) = \{\{x\}, \{x, y\}\}$.

$\mathsf{rank}((x, y)) = \mathsf{max}(\mathsf{rank}(x), \mathsf{rank}(y)) + 2$.

We can identify the 'first' element x of a Kuratowski pair z by looking for the element $\{x\} \in z$. We can then identify the 'second' element y by looking at the other element $y' \in z$.

- If $y' = \{y\}$ then $x = y$.
- Otherwise, $y' = \{x, y\}$.

If X and Y are sets, write $X \times Y$ for $\{(x, y) \mid x \in X,\ y \in Y\}$.

Disjoint sum

Write $X + Y$ for $\{(0, x) \mid x \in X\} \cup \{(1, y) \mid y \in Y\}$.

Write $(0, x)$ as $\mathsf{inl}(x)$ and $(1, y)$ as $\mathsf{inr}(y)$.

Numbers

We can identify a rational number p as

$$\{(n, m) \mid n, m \in \mathbb{N},\ p = n/m\}.$$

Write $\mathbb{Q}$ for the set of rational numbers. We can identify a real number r as a Dedekind cut

$$(\{p \in \mathbb{Q} \mid p < r\},\ \{q \in \mathbb{Q} \mid r < q\}).$$

Write $\mathbb{R}$ for the set of rational numbers.

It should now be evident how to model complex numbers, vector spaces, groups, rings, fields, and loads more.

Functions

Do functions exist? Certainly.

If X and Y are sets, write $X \to Y$ for the set of functional relations between X and Y.

Let's write that out in first-order logic. $f \in X \to Y$ when

- $f \subseteq X \times Y$ (f is a graph).
- $\forall x, y, y'.((x, y) \in f \wedge (x, y') \in f) \Rightarrow y = y'$.
  (f is functional.)
- $\forall x \in X.\exists y.(x, y) \in f$.
  (f is total.)

We write $f(x)$ for the unique y such that $(x, y) \in f$.

Foundations of mathematics

If you're with me so far, then you've had a concise introduction to the foundations of mathematics.

Assuming that

- $\emptyset$ exists, and that
- if you can form a subset, then you can form a set which is that subset,

is assuming enough to build a rich mathematical universe.

Adding names

Jamie, Maribel, and other names, do not have sets structure. They are just names.

So we enrich our cumulative hierarchy with names. Suppose $\mathbb{A} = \{a, b, c, d, \ldots\}$ is a countably infinite collection of atoms.

Define a new sets hierarchy by:

A cumulative hierarchy with names

1. $\mathcal{U}_0 = \mathbb{A}$.
2. $\alpha < \beta$, $\beta < \omega$, $U \subseteq \mathcal{U}_\alpha$, and U is finite, imply $U \in \mathcal{U}_\beta$.
3. $\alpha < \beta$, $\omega \leq \beta$, and $U \subseteq \mathcal{U}_\alpha$, imply $U \in \mathcal{U}_\beta$.

Call an element that is not an atom a set.

If X is a set then $X = \{x \mid x \in X\}$. This is not the case of atoms. For example $a \neq \{x \mid x \in a\} = \emptyset$.

A cumulative hierarchy with names

We can draw the following diagram:

$$a \in \mathcal{U}_0 \qquad b \in \mathcal{U}_0$$

$$\emptyset \in \mathcal{U}_1 \qquad \{a\} \in \mathcal{U}_1 \qquad \{a, b\} \in \mathcal{U}_1$$

$$\{\emptyset\} \in \mathcal{U}_2 \qquad \{\{a\}, \{a, b\}\} \in \mathcal{U}_2$$

$$\vdots$$

$$\mathbb{A} \in \mathcal{U}_{\omega+1}$$

$$\mathbb{A} \cup \{\mathbb{A}\} \in \mathcal{U}_{\omega+1}$$

$$\vdots$$

$$\text{Set of real numbers} \in \mathcal{U}_{\omega_1+1}$$

A cumulative hierarchy with names

A word on our treatment of $\mathbb{A}$.

We could unify the second and third clauses of the inductive definition above to

$\alpha < \beta$ and $U \subseteq \mathcal{U}_\alpha$ imply $U \in \mathcal{U}_\beta$ (for any α and β).

However, then $\mathbb{A} \in \mathcal{U}_1$.

Since we take $\mathbb{A}$ to be countably infinite, this means that $\mathbb{A}$, an infinite set, appears in what is usually taken to be the finite initial segment of the cumulative hierarchy.

This is not wrong but we exert ourselves and preserve the standard intuition that '$\mathcal{U}_\omega$ is the collection of finite sets'.

Permutations

Given a and b write $(b\ a)$ for the function which 'swaps' a and b:

$$(b\ a)(a) = b \qquad (b\ a)(b) = a \qquad (b\ a)(c) = c$$

Extend this function to the sets universe as

$$(b\ a)X = \{(b\ a)x \mid x \in X\}.$$

Intuitively, $(b\ a)x$ is x, in which a and b are swapped.

The Gabbay-Pitts notion of the support of a set

Write $\mathsf{supp}(x)$ for the set of $a \in \mathbb{A}$ such that

$$\{b \mid b \neq a \wedge (b\,a)x \neq x\} \quad \text{is infinite.}$$

Say a is in the support of x. For example $a \in \mathsf{supp}(a)$ since

$$\{b \mid b \neq a \wedge (b\,a)a \neq a\} = \{b \mid b \neq a\}$$

is infinite. $a \notin \mathsf{supp}(\mathbb{A})$ since

$$\{b \mid b \neq a \wedge (b\,a)\mathbb{A} \neq \mathbb{A}\} = \emptyset$$

is finite.

Examples

Q1. Is $a \in \mathsf{supp}(\{a\})$?

Q2. Is $a \in \mathsf{supp}(\mathbb{A} \setminus \{a\})$?

Examples

A1. Yes. $a \in \mathsf{supp}(\{a\})$.

A2. Yes. $a \in \mathsf{supp}(\mathbb{A} \setminus \{a\})$.

Note that $a \notin a$ yet $a \in \mathsf{supp}(a)$.

Note that $a \in \mathbb{A}$ yet $a \notin \mathsf{supp}(\mathbb{A})$.

Note that $a \notin \mathbb{A} \setminus \{a\}$ yet $a \in \mathsf{supp}(\mathbb{A} \setminus \{a\})$.

$a \in \mathsf{supp}(x)$ measures whether a is 'conspicuous' in x, either by its presence or its absence.

Atoms-abstraction

Say that x has finite support when $\mathsf{supp}(x)$ is finite.

Q3. Does $\mathbb{A}$ have finite support?

Q4. Does a have finite support?

Q5. Does $\mathsf{comb} = \{a, c, e, g, \ldots\}$ (the set of 'every other atom') have finite support?

A model of α-abstraction

Suppose that x has finite support. Suppose $b \neq a$. Define

$$[a]x = \{(a, x)\} \cup \{(b, (b\ a)x \mid b \neq a \wedge b \notin \mathsf{supp}(x)\}.$$

$[a]x = [b]y$ if and only if for some/any c such that $c \notin \mathsf{supp}(x)$ it is the case that $(c\ a)x = (c\ b)y$.

$[a]x = [b]y$ if and only if $b \notin \mathsf{supp}(x)$ and $(b\ a)x = y$.

Why is a model of α-equivalence interesting?

We now have a convenient sets model syntax up to α-conversion.

$t ::= a \mid tt \mid \lambda a.t$ can be modelled using pairsets, disjoint sum, . . . and atoms-abstraction.

A function that generates a new name, like gensym in LISP or malloc in C, can be modelled using atoms-abstraction.