MAU22C00 Lecture 18

John Stalker

Trinity College Dublin

Announcements

- I've posted more notes, adding a chapter on graph theory.
- I've posted Assignment 5. People requested posting assignments farther in advance. I'll try to do that for the remaining assignments.
- I'm not available at the time of Tuesday's lecture next week so I'll post a pre-recorded video, as I did last time.

Countable sets

Recall that A is countable if and only if there is an injective function from A to N.

At least according to my conventions. Roughly half the world substitutes "bijective" for "injective".

With either convention N itself is countable.

We usually show a set is countable using the following properties, not the definition!

- subsets of countable sets are countable
- the union or Cartesian product of two countable sets is countable
- the set of lists of items chosen from a countable set is countable

The rationals are countable

I'll define the rational numbers more formally later but if a, b, c are natural numbers and $c > 0$ then $(a - b)/c$ is rational.

Every rational number is of this form.

In fact there will be infinitely many such a, b and c for any rational number, e.g.

$$\frac{0-1}{2} = \frac{1-3}{4} = \frac{3-7}{8} = \frac{7-15}{16} = \cdots.$$

There's a particular standard choice, with $a \cdot b = 0$ and $\gcd(a, b, c) = 1$.

Define a function from Q to N^3 which associates to each rational to this standard triple (a, b, c). This is an injective function.

This is obvious. It's the statement that if $p = (a - b)/c$ and $q = (a - b)/c$ then $p = q$.

N^3 is countable, i.e. there is an injective function from it to N. Compose with the function above for an injective function from Q to N. So Q is countable.

The algebraic numbers are countable

A (complex) number is called algebraic if it is a root of a non-zero polynomial with rational coefficients.

The set of non-zero polynomials with rational coefficients is countable.

This is obvious; polynomials are really just lists of coefficients.

For each algebraic number there's a simplest non-zero polynomial of which it's a root, which is monic and of least degree.

Complication: this polynomial generally has multiple roots.

There are only finitely many roots though, and we can order them, so we can specify an algebraic number by giving its polynomial and its position in the ordered set of roots.

The coefficients, followed by this number, form a list of rationals.

The set of lists of rationals is countable, so the set of algebraic numbers is countable.

The reals are uncountable

Suppose the reals were countable.

Every real number has a decimal expansion.

Complication: Some have more than one, e.g. $1.0 = 0.99999999\ldots$.

If a real number has only the digits 0 and 1 in its decimal expansion then it has a unique decimal expansion.

Let A be the set of real numbers x with $0 \leq x < 1$ with only 0's and 1's in their decimal expansion.

If R is countable then so is A, i.e. there is an injection from A to N.

There is an injective function from PN to A which takes E to the member of A with 1's in the digits with position in E and 0's in the positions in $N \setminus E$, i.e. $\sum_{j \in E} \frac{1}{10^{j+1}}$.

Composing these gives an injective function from PN to N, but there is none, so R is uncountable.

Transcendental numbers

Numbers which are not algebraic are called transcendental. We can now easily show there are transcendental numbers.

The real numbers are a subset of the complex numbers, and are uncountable, so the complex numbers are uncountable.

The algebraic numbers are a subset of the complex numbers and are countable, so must be a proper subset.

Therefore there is a complex number which is not algebraic, i.e. is transcendental.

A more sophisticated version of this argument shows that there are infinitely many, in fact uncountably many, transcendental numbers.

Showing that some particular number is transcendental is much harder. e and π are known to be transcendental, but the proofs are much harder than the "counting" argument above.

Axioms of simple set theory:

These are what I called the axioms of simple set theory:

- *Extensionality*: Sets are equal if they have the same members
- *Elementary Sets* (aka Pairing): Given zero, one or two things there is a set of which they are members
- *Selection* (aka Restricted Comprehension): Given a set and a condition (Boolean expression) there's a subset consisting of the members which satisfy that condition
- *Union*: The union of a set of sets exists.
- *Power Set*: The power set of a set exists.

These axioms, together with first order logic is sufficient for the theory of finite sets and Peano arithmetic.

They're also enough to get some "paradoxes", like the fact that there is no set of sets, and (absolute) complements of sets don't exist.

More axioms

For infinite sets we want to add

- *Infinity*: Some infinite set exists, sufficient to construct the set of natural numbers.
- *Replacement*: Given a Boolean expression with two free variables which looks like the statement that one is a function of the other with a given set as its domain, there is another set which is its domain.

With these additional axioms we can do nearly all of computer science and some mathematics. We don't even need Replacement very much.

To get a few bits of computer science and most of classical mathematics we need one more axiom:

- *Dependent Choice*: A simple state machine, where there's always at least one option for the next state, can run forever.

We don't actually need a new axiom for this unless the number of states is uncountable and the state machine is non-deterministic.

Dependent Choice

Here's the formal version:

- *Dependent Choice*: For every set A, member $w \in A$ and left total relation T on A there is a function F from N to A such that if $(n, x) \in A$ and $(n+1, y) \in A$ then $(x, y) \in T$.

A is the set of states, w the start state, T the transition relation and F a computational path for the state machine.

Left totality means there's at least one allowed transition from each state.

You can use Dependent Choice to justify recursive definitions, e.g. of the Fibonacci sequence, but it's not really needed for that since there's no non-determinism there.

There's another, equivalent version:

- *Dependent Choice (alternate formulation)*: If every chain in a partially ordered set is finite, then it contains a maximal element.

Other axioms of choice

- Countable Choice: If A is a countable set of disjoint non-empty sets then there is a set which shares exactly one element with each of them.

This follows from Dependent Choice–this isn't obvious–but can't be proved using only the other axioms–this is also not obvious–and you can't prove Dependent Choice from this and the other axioms–yet again, not obvious.

So Countable Choice is a strictly weaker assumption than Dependent Choice. The following axiom is strictly stronger:

- *Choice*: If A is a set of disjoint non-empty sets then there is a set which shares exactly one member with each of them.

Most mathematicians assume the Axiom of Choice, or some equivalent axiom, like the following.

- *Zorn's Lemma*: If every chain in a partially ordered set is bounded, then it contains a maximal element.

Foundation

It's traditional to assume the following axiom as well:

Foundation (aka Regularity): Every non-empty set has a member which is disjoint from it, i.e. shares no members with it. Formally

$$[\forall A.[[\exists B.B \in A] \supset [\exists C \in A : [A \bigcap C] = \emptyset]]].$$

All the preceding axioms were at least plausible. This one is merely convenient.

It's not even all that convenient. Like Replacement it's essentially never used outside set theory.

It prevents sets from being members of themselves. Is that a good thing? Maybe.

Extensionality, again

The version of Extensionality I've been using is Zermelo's: If A and B are sets and every member of A is a member of B and vice versa then $A = B$.

Are the words "If A and B are sets" redundant? Are there things which are not sets, but can be members of sets?

Zermelo wanted to allow this, even though we don't strictly need it for mathematics.

Books on set theory start with examples like that, e.g. the set of people in this module.

Standard practice for the last century or so is to disallow it.

- *Extensionality (stronger version)*: Suppose every member of A is a member of B and vice versa. Then $A = B$.

This makes the theory of ordinals slightly easier, at the expense of dropping any pretense that the theory of sets has non-mathematical applications.

That might be defensible if people were at least honest about it.

Zermelo-Fraenkel

The usual version of set theory is called Zermelo-Fraenkel, after Zermelo, who had a fairly reasonable axiomatic system, and Fraenkel, who wrecked it.

- Elementary sets
- Selection
- Union
- Power sets
- Infinity
- Replacement
- Foundation
- Choice?

The version without Choice is called ZF while the version with it is called ZFC.

Banach-Tarski

This version of set theory has some unfortunate consequences.

There are sets A_1, A_2, A_3, A_4, A_5, B_1, B_2, B_3, C_1, C_2, C_3, C_4 and C_5 in three dimensional Euclidean space with the following properties.

- B_1, B_2 and B_3 are disjoint balls of radius 1.
- A_1 is congruent to C_1, A_2 is congruent to C_2, A_3 is congruent to C_3, A_4 is congruent to C_4, and A_5 is congruent to C_5.
- A_1, A_2, A_3, A_4 and A_5 are disjoint and their union is $B_1 \bigcup B_2$.
- C_1, C_2, C_3, C_4 and C_5 are disjoint and their union is B_3.

In other words, we can take a ball, split it into five pieces, move those pieces via a rigid motion, i.e. a combination of translations, reflections and rotations, and reassemble them to form two balls of the same radius as the original one.

The principal culprit here is the (unrestricted) Axiom of Choice. This doesn't happen with weaker versions like Dependent Choice.