MAU22C00 Lecture 14

John Stalker

Trinity College Dublin

Announcements

- I can't make Thursday's lecture next week. I'll post a prerecorded video.
- I've posted the first part of the set theory lecture notes. I decided to revise the section following that part and will post more notes after I finish doing that, perhaps over the weekend.
- I leave it up to the markers how much detail is required on the assignments. Keep in mind that they took the module in a different year, if at all, so you can't assume they know everything I said in lecture or in the notes. You probably want to give more detail than you would on a timed exam.
- The assignments count 40%, so you can work together but you shouldn't simply copy, either from each other or from other sources.

Set theory

Elementary arithmetic is arithmetic without sets, just numbers.

We were sort of able to smuggle sets in, via Boolean expressions.

Now we consider set theory with just sets, no numbers.

Sets of what? We'll defer that question for now.

We're sort of able to smuggle numbers in, in a variety of ways.

Set theory starts out normal enough, but will get weird.

As usual, I'll start with a grammar for a language, then describe the intended interpretation, then give a formal system.

Most proofs will be semiformal, a few will be informal, but none will be formal.

A phrase structure grammar

```
statement : bool_exp ;
bool_exp | [ ¬ bool_exp ] | [ bool_exp b_operator bool_exp ]
         | [ quantifier variable . bool_exp ]
         | [ quantifier variable ∈ set_exp : bool_exp ]
         | [ variable relation variable ] ;
b_operator : ∧ | ∨ | ⊃ ;
quantifier : ∀ | ∃ ;
relation : ∈ | = | ⊆ ;
set_exp : ∅ | variable | [ ∩ set_exp ] | [ ∪ set_exp ]
        | [ set_exp ∩ set_exp ] | [ set_exp ∪ set_exp ]
        | [ set_exp ∖ set_exp ] | [ set_exp × set_exp ]
        | [ P set_exp ] | { list } | ( list )
        | { variable ∈ set_exp : bool_exp } ;
list : /* empty */ | sequence ;
sequence : set_exp | set_exp , sequence ;
variable : letter | variable ! ;
letter : v | w | x | y | z | A | B | C | D | E | F
       | G | H | I | J | K | L | R | S | T | U | V ;
```

Comments

[and] are still used for grouping but (and) and $\{$ and $\}$ are reserved for special meanings. (and) are used to indicate lists and $\{$ and $\}$ are used to describe sets. (x,y,z) is the list (ordered triple) whose elements are x, y and z, in that order. $\{x,y,z\}$ is the set whose members are x, y and z.

$\{$ and $\}$ are also used describe subsets selected using a condition (Boolean expression), like $\{x \in A : [\neg[x \in B]]\}$, the set of members of A which are not members of B, also denoted $A \setminus B$.

Besides the relative complement operator $\setminus$ we have the set operators $\bigcap$ (intersection), $\bigcup$ (union) and $\times$ (product). There are two variants of $\bigcap$ and $\bigcup$, a unary variant and a binary variant. $[\bigcup A]$ is the set whose members are the members of the members of A. $[B \bigcup C]$ is shorthand for $[\bigcup\{B,C\}]$.

$\emptyset$ is the empty set. $[PA]$ is power set of A, i.e. the set of its subsets.

Comments, continued

We have two relations, $\in$ and $\subseteq$.

$[A \in B]$ means A is a member of B.

$[A \subseteq B]$ means A is a subset of B, i.e. every member of A is a member of B.

These are not the same thing!

$[A \subseteq B]$ can be thought of as shorthand for $[\forall x.[[x \in A] \supset [x \in B]]]$.

Or we could express $[A \in B]$ as $[\{A\} \subseteq B]$. Note that A and $\{A\}$ are not the same thing.

We also have an alternate form of quantifier expressions. $[\forall x \in A : [...]]$ is shorthand for $[\forall x.[[x \in A] \supset [...]]]$ and similarly for $\exists$.

So $[\forall x.[[x \in A] \supset [x \in B]]]$ could also have been written as $[\forall x \in A : [x \in B]]$.

I'll explain $\circ$ later. I'll also, eventually, introduce a few more symbols.

Expressing more complicated ideas

By combining ideas for which we do have notations we can express more complicated ideas for which we don't.

We don't have numbers, for example, so there's no direct way to say "A has two members".

We can express "A has at least two members" by

$$[\exists x \in A : [\exists y \in A : [\neg[x = y]]]].$$

We can express "A has at most two members" by

$$[\forall x \in A : [\forall y \in A : [\forall z \in A : [[[x = y] \vee [x = z]] \vee [y = z]]]]].$$

Stick them together with an $\wedge$ in between and you get "A has two members".

Expressing even more complicated ideas

For a more complicated example, how do we express the idea that the members of A are disjoint sets, i.e. that no member of one member of A is a member of another member of A?

One option is

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

Another is

$$[\forall B \in A : [\forall x \in B : [\{C \in A : [x \in C]\} = \{B\}]]].$$

We can express even more complicated ideas, e.g. "A is finite", but we'll get to that later.

Axioms

The following is a subset of our eventual set of axioms, sufficient for most of mathematics and computer science:

- *Extensionality*: Suppose A and B are sets and every member of A is a member of B and vice versa then $A = B$.
- *Elementary sets*: $\emptyset$ is a set. For all x we have $[\neg[x \in \emptyset]]$. For all x we have a set $\{x\}$, of which x is a member and there are no other members. Similarly, for all x and y we have a set $\{x, y\}$ such that x and y are members and there are no other members.
- *Separation*: For every variable x, set A and Boolean expression θ the set $\{x \in A : \theta\}$, whose members are those members of A for which θ is true, exists.
- *Power set*: For any set A the power set $[PA]$ exists. $[B \in [PA]]$ if and only if every member of B is a member of A, i.e. if and only if B is a subset of A.
- *Union*: For every set A the set $[\bigcup A]$ exists. This is the set of all members of members of A.

Comments on the axioms

There are no (new) rules of inference, just new axioms. We keep the rules of inference from first order logic though.

You can find the formal counterparts of these axioms in the notes.

Separation is not actually an axiom, it's a *axiom schema*, i.e. a pattern from which an infinite number of axioms can be generated.

Extensionality means sets are determined by their members, not be any particular description, e.g. "the set of all even prime numbers" and "$\{2\}$" are the same set. There can also be indescribable sets.

You can't conjure things into existence just by introducing a notation for them. That's we we need axioms to assure us of the existence of pairs, unions, power sets, etc. even though we already have a notation for them.

We don't need axioms for everything we have notation for though. We can construct $\{x, y, z\}$ or $[A \bigcap B]$ from other axioms, as $[\bigcup\{\{x, y\}, \{y, z\}\}]$ and $\{x \in A : [x \in B]\}$, respectively.

There is no set of all sets!

The axioms above imply that there is no set of all sets.

Suppose there were a set A such that every set is a member of A. By the Axiom of Separation then we can form the set

$$B = \{C \in A : [\neg[C \in C]]\}.$$

In other words C is the set of all sets which are not members of themselves. Is B a member of B?

If not then B is a set which is not a member of itself, but then by the definition of B it is a member of B.

Similarly, if B is a member of B then it doesn't satisfy the definition of B and so isn't a member of B.

So the assumption that there is a set of all sets leads to a contradiction.

"The universal set" appears on the Junior Cert curriculum but it does not actually exist!

Complements and relative complements

Relative complements exist. If A and B are sets then there is a set whose members are all elements of B which are not elements of B. This follows immediately from the Axiom of Separation. It's denoted $A \setminus B$.

Complements do not exist! If there were a set A which had as a member everything which is not an element of a set B the we could, by the Axiom of Union and Axiom of Selection, construct a set of all sets from it. But we know there is no set of all sets.

Do not use the notation A^c or similar. It does not refer to anything.

If all sets considered in a particular context are subsets of a given set then some people will use the word complement as shorthand for relative complement, specifically complement relative to that set. It's still a relative complement though.

Sets and Boolean operations

There is a partial correspondence between set operators and Boolean operators.

Pretend, for a moment, that there were a universal set.

We could take any implication from zeroeth order logic, replace Boolean variables by set variables, $\wedge$ by $\bigcap$, $\vee$ by $\bigcup$, $\neg$ by ^{c} and replace "has as a consequence" by "is a subset of".

For example p has as a consequence $[p \vee q]$ so from $[x \in A]$ we can derive $[x \in A] \vee [x \in B]$. But $[x \in A] \vee [x \in B]$ is equivalent to $[x \in [A \bigcup B]]$, by the definition of the union. So if $[x \in A]$ then $[x \in [A \bigcup B]]$. Then A is a subset of $[A \bigcup B]$, i.e. $A \subseteq [A \bigcup B]$, by the definition of a subset.

This works for statements involving only $\wedge$ and $\vee$, because $[[x \in [A \bigcap B]]$ if and only if $[[x \in A] \wedge [x \in B]]]$ and $[[x \in [A \bigcup B]]$ if and only if $[[x \in A] \vee [x \in B]]]$ but it doesn't work for ones involving $\neg$ because there is no complement operation for sets.

We do have relative complements though, and $[[x \in [A \setminus B]]$ if and only if $[\neg[[x \in A] \supset [x \in B]]]]$, so we can convert *some* of zeroeth order logic involving $\neg$ and $\supset$ into set theory.

Sets and Boolean operations, continued

It works better in the other direction. If α and β are set valued expressions constructed using $\bigcap$, $\bigcup$ and $\setminus$ then $[\alpha \subseteq \beta]$ is a set theory identity if and only if the Boolean expression corresponding to β is a logical consequence of the one corresponding to α.

Zeroeth order logic is *decidable* so this is something we can check.

If the same works for $[\beta \subseteq \alpha]$ then you get $[\alpha = \beta]$.

Lots of identities

All of the following can be proved by the method just described.

$$[[A \bigcap B] \subseteq A] \qquad [[A \setminus [A \setminus B]] = [A \bigcap B]]$$
$$[[A \bigcap B] \subseteq B] \qquad [[[A \bigcap B] \bigcap C] = [A \bigcap [B \bigcap C]]]$$
$$[A \subseteq [A \bigcup B]] \qquad [[[A \bigcup B] \bigcup C] = [A \bigcup [B \bigcup C]]]$$
$$[B \subseteq [A \bigcup B]] \qquad [[[A \setminus B] \setminus C] = [A \setminus [B \bigcup C]]]$$
$$[[A \setminus B] \subseteq A] \qquad [[[A \setminus B] \bigcap C] = [A \bigcap [C \setminus B]]]$$
$$[[A \bigcap A] = A] \qquad [[A \setminus [B \setminus C]] = [[A \bigcap C] \bigcup [B \setminus C]$$
$$[[A \bigcup A] = A] \qquad [[[A \bigcap [B \bigcup C]] = [[A \bigcup C] \bigcap [B \bigcup C]]]$$
$$[[A \bigcap B] = [B \bigcap A]] \qquad [[[A \bigcup [B \bigcap C]] = [[A \bigcap C] \bigcup [B \bigcap C]]]$$
$$[[A \bigcup B] = [B \bigcup A]] \qquad [[C \setminus [A \bigcap B]] = [[C \setminus B] \bigcup [C \setminus A]]]$$
$$[[A \bigcap [A \bigcup B]] = A] \qquad [[C \setminus [A \bigcup B]] = [[C \setminus B] \bigcap [C \setminus A]]]$$
$$[[A \bigcup [A \bigcap B]] = A]$$

I don't see the point in memorising lists like this. If you see one often you'll remember it. If you don't you probably don't need to, and can check it in any case.