M3P65 Mathematical Logic

Lectured by Prof David Evans
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

Lecture 1
Thursday
04/10/18

0 Introduction

The module is concerned with some of the foundational issues of mathematics, namely propositional logic, predicate logic, and set theory. These topics have applications to other areas of mathematics. Formal logic has applications via model theory and ZFC provides an essential toolkit for handling infinite objects.

In propositional logic, we look at the way simple propositions can be built into more complicated ones using connectives and make precise how the truth or falsity of the component statements influences the truth or falsity of the compound statement. This is done using truth tables and can be useful for testing the validity of various forms of reasoning. It provides a way of analysing deductions of the form 'If the following statements are true, ..., then so is ...'. A completely symbolic process of deduction and describe the formal deduction system for propositional calculus. The propositional formulas are regarded as strings of symbols and we give rules for deducing a new formula from a given collection of formulas. We want these deduction rules to have the property that anything that could be deduced using truth tables (so by considering truth or falsity of the various statements), can be deduced in this formal way, and vice versa. This is the soundness and completeness of our formal system.

In predicate logic, we analyse mathematics using quantifiers. We introduce the notion of a first-order structure, which is general enough to include many of the algebraic objects you come across in mathematics, such as groups, rings, and vector spaces. We then have to be precise about the formulas which make statements about these structures, and give a precise definition of what it means for a particular formula to be true in a structure. This is quite intricate, and the clever part is in getting the definitions right, but it corresponds to ordinary mathematical usage. Once this is done, we set up a formal deduction system for predicate logic. This parallels what we did for propositional logic, but is much harder. Nevertheless, the end result is the same. The formulas which are produced by our formal deduction system are precisely the formulas which are true in all first-order structures. This is Gödel's completeness theorem.

Set theory provides the basic foundations and the language in which most of modern mathematics can be expressed, as well as the means for discussing the various notions of sizes of infinity. For example, although the set of natural numbers, the set of integers and the set of real numbers are all infinite, there is a very natural sense in which the first two have the same size, whereas the third is strictly bigger. This is expressed properly in the notion of cardinality. To avoid paradoxes and inconsistencies, we have to be careful about what collections of objects we allow to be called sets. This is done by the Zermelo-Fraenkel axioms, which essentially tell us how we are allowed to create new sets out of old ones. Of course, having laid down these quite rigid rules, we have to show that they are sufficiently flexible to allow us to talk about everyday objects of mathematics. There are also situations in mathematics where an extra axiom is needed, the axiom of choice. For example without this axiom, we cannot show that every vector space has a basis. But it also has some slightly counterintuitive consequences, and we shall also look at some of these.

The lecture notes should be fairly self-contained, but the following books might also be of use. You might find that the notation which they use differs form that used in the lectures. You will be able to find various lecture notes on the internet. Some will be good, others not so good.

1. P Johnstone, Notes on logic and set theory, 1987
2. P J Cameron, Sets, logic and categories, 1999
3. A G Hamilton, Logic for mathematicians, 1988
4. R Cori and D Lascar, Mathematical logic: a course with exercises parts I and II, 2001
5. K Hrbaček and T Jech, Introduction to set theory 3rd edition, 1999

1 is very concise, but covers a surprising amount. 2 is friendlier, but skips some of the harder material. 4 is quite comprehensive and also available in the original French. 3 is useful for the logic part and 5 is a very nice introduction to set theory.

1 Propositional logic

Let p be 'Mr Jones is happy' and q be 'Mrs Jones is unhappy'. Then 'If Mr Jones is happy, then Mrs Jones is unhappy and if Mrs Jones is unhappy then Mr Jones is unhappy, so Mr Jones is unhappy' is

$$(((p \to q) \wedge (q \to (\neg p))) \to (\neg p)).$$

1.1 Propositional formulas

The following are **truth table rules**.

Definition 1.1.1. A **proposition** is a statement that is either **True** (T) or **False** (F), which can be represented symbolically as **propositional variables**

$$p, \quad q, \quad \dots \qquad p_1, \quad p_2, \quad \dots.$$

We combine basic propositions into others using **connectives**, which are one of

- **negation 'not'** $(\neg p)$, which has value F if p has value T and has value T if p has value F,
- **conjunction 'and'** $(p \wedge q)$, which has value T iff p and q both have value T,
- **disjunction 'or'** $(p \vee q)$, which has value T iff at least one of p and q has value T,
- **implication 'implies'** $(p \to q)$, which has value F iff p has value T and q has value F, and
- **biconditional 'iff'** $(p \leftrightarrow q)$, which has value T iff p and q has the same value.

This can be represented in the following **truth table**.

p	q	$(p \wedge q)$	$(p \vee q)$	$(p \to q)$	$(p \leftrightarrow q)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Definition 1.1.2. A **propositional formula** is obtained in the following way.

1. Any propositional variable is a formula.
2. If ϕ and ψ are formulas, then so are

$$(\neg \phi), \qquad (\phi \wedge \psi), \qquad (\phi \vee \psi), \qquad (\phi \to \psi), \qquad (\phi \leftrightarrow \psi).$$

3. Any formula arises in this way.

Example. Some formulas are

$$p_1, \qquad p_2, \qquad (\neg p_1), \qquad (p_1 \to (\neg p_2)), \qquad ((p_1 \to (\neg p_2)) \to p_2).$$

Some not formulas are

$$p_1 \wedge p_2 \quad (\text{missing brackets}), \qquad)(\neg p_1 \quad (\text{not well-formed}).$$

Because of the brackets, every formula is either a propositional variable or is built from shorter formulas in a unique way. Arguments are often proved by induction on length of the formula, or the number of connectives in the formula.

Definition 1.1.3.

1. Let $n \in \mathbb{N}$. A **truth function** of n variables is a function $f : \{T, F\}^n \to \{T, F\}$, where $\{T, F\}^n = \{(x_1, \dots, x_n) \mid x_i \in \{T, F\}\}$.
2. Suppose ϕ is a formula whose variables are amongst $p_1, \dots, p_n$. We obtain a truth function $F_\phi : \{T, F\}^n \to \{T, F\}$ whose value at $(x_1, \dots, x_n)$ is the truth value of ϕ when p_i has value x_i for $i = 1, \dots, n$, computed using the rules in 1.1.1. F_ϕ is the **truth function of** ϕ.

Example. $\phi : ((p \to (\neg q)) \to p)$ has the following truth table.

p	q	$(\neg q)$	$(p \to (\neg q))$	ϕ
T	T	F	F	T
T	F	T	T	T
F	T	F	T	F
F	F	T	T	F

So for example $F_\phi(T, F) = T$. This can also be written in a **condensed form** as follows.

$((p$	$\to$	$(\neg$	$q))$	$\to$	$p)$
T	F	F	T	T	T
T	T	T	F	T	T
F	T	F	T	F	F
F	T	T	F	F	F

Lecture 2 Friday 05/10/18

Example. The truth function of $(((p \to q) \wedge (q \to (\neg p))) \to (\neg p))$ is always T.

Definition 1.1.4.

1. A propositional formula is a **tautology** if its truth function F_ϕ always has value T.
2. Say that formulas ϕ, ψ are **logically equivalent** (LE) if they have the same truth function, that is $F_\phi = F_\psi$.

Remark 1.1.5.

1. ϕ, ψ are LE iff $(\phi \leftrightarrow \psi)$ is a tautology.
2. Suppose ϕ is a formula with variables $p_1, \dots, p_n$ and $\phi_1, \dots, \phi_n$ are formulas with variables $q_1, \dots q_r$. For each $i \leq n$ substitute ϕ_i in place of p_i in ϕ. Then the result is a formula θ, and if ϕ is a tautology, then so is θ.

Example. Check $(((\neg p_2) \to (\neg p_1)) \to (p_1 \to p_2))$ is a tautology. So by 1.1.5(2), if ϕ_1 and ϕ_2 are any formulas, then $(((\neg \phi_2) \to (\neg \phi_1)) \to (\phi_1 \to \phi_2))$ is a tautology.

Proof of 1.1.5.

1. Easy.
2. Prove $F_\phi(p_1, \dots, p_r) = F_\phi(F_{\phi_1}(q_1, \dots, q_r), \dots, F_{\phi_n}(q_1, \dots, q_r))$ by induction on the number of connectives in ϕ.

□

Example. The following are LE formulas.

1. $(p_1 \wedge (p_2 \wedge p_3))$ is LE to $((p_1 \wedge p_2) \wedge p_3)$.
2. $(p_1 \vee (p_2 \vee p_3))$ is LE to $((p_1 \vee p_2) \vee p_3)$.
3. $(p_1 \vee (p_2 \wedge p_3))$ is LE to $((p_1 \vee p_2) \wedge (p_1 \vee p_3))$.
4. $(p_1 \wedge (p_2 \vee p_3))$ is LE to $((p_1 \wedge p_2) \vee (p_1 \wedge p_3))$.

5. $(\neg(\neg p_1))$ is LE to p_1.
6. $(\neg(p_1 \wedge p_2))$ is LE to $((\neg p_1) \vee (\neg p_2))$.
7. $(\neg(p_1 \vee p_2))$ is LE to $((\neg p_1) \wedge (\neg p_2))$.

By the first two examples, we usually omit brackets as $(p_1 \wedge p_2 \wedge p_3)$ and $(p_1 \vee p_2 \vee p_3)$ without ambiguity.

Note. By 1.1.5 we obtain, for formulas ϕ, ψ, χ, $(\phi \wedge (\psi \wedge \chi))$ is LE to $((\phi \wedge \psi) \wedge \chi)$, etc.

Lemma 1.1.6. There are 2^{2^n} truth functions of n variables.

Proof. A truth function is a function $F : \{T, F\}^n \to \{T, F\}$. $|\{T, F\}^n| = 2^n$ and for each $\overline{x} \in \{T, F\}^n$, $F(\overline{x}) \in \{T, F\}$. Hence the result. $\square$

Definition 1.1.7. A set of connectives is **adequate** if for every $n \geq 1$, every truth function of n variables is the truth function of some formula which involves only connectives from the set, and variables $p_1, \ldots, p_n$.

Theorem 1.1.8. The set $\{\neg, \wedge, \vee\}$ is adequate.

Proof. Let $G : \{T, F\}^n \to \{T, F\}$.

1. $G(\overline{v}) = F$ for all $\overline{v} \in \{T, F\}^n$. Take ϕ to be $(p_1 \wedge (\neg p_1))$. Then $F_\phi = G$.
2. List the $\overline{v} \in \{T, F\}^n$ with $G(\overline{v}) = T$ as $\overline{v_1}, \ldots, \overline{v_r}$. Write $\overline{v_i} = (v_{i1}, \ldots, v_{in})$, where each v_{ij} is T or F. Define
$$q_{ij} = \begin{cases} p_j & v_{ij} = T \\ (\neg p_j) & v_{ij} = F \end{cases}.$$
So q_{ij} has value T iff p_j has value v_{ij}. Let ψ_i be $(q_{i1} \wedge \cdots \wedge q_{in})$. Then $F_{\psi_i}(\overline{v}) = T$ iff each q_{ij} has value T, iff $\overline{v} = \overline{v_i}$. Let θ be $(\psi_1 \vee \cdots \vee \psi_r)$. Then $F_\theta(\overline{v}) = T$ iff $F_{\psi_i}(\overline{v}) = T$ for some i, iff $\overline{v} = \overline{v_i}$ for some $i \leq r$. Thus $F_\theta(\overline{v}) = T$ iff $G(\overline{v}) = T$, that is $F_\theta = G$.

As ϕ and θ were constructed using only $\neg, \wedge, \vee$, 1.1.8 follows. $\square$

A formula θ as in case 2 is said to be in **disjunctive normal form** (DNF).

Corollary 1.1.9. Suppose χ is a formula whose truth function is not always F. Then χ is LE to a formula in DNF.

Proof. Take $G = F_\chi$ and apply case 2 of 1.1.8. $\square$

Example. Let χ be $((p_1 \to p_2) \to (\neg p_2))$. Then $F_\chi(\overline{v}) = T$ iff $\overline{v} = (T, F), (F, F)$. Thus its DNF is
$$((p_1 \wedge (\neg p_2)) \vee ((\neg p_1) \wedge (\neg p_2))).$$

Corollary 1.1.10. The following sets of connectives are adequate.

1. $\{\neg, \vee\}$.
2. $\{\neg, \wedge\}$.
3. $\{\neg, \to\}$.

Proof.

1. By 1.1.8 it is sufficient to show that we can express $\wedge$ using $\neg, \vee$, which holds since $(p_1 \wedge p_2)$ is LE to $(\neg((\neg p_1) \vee (\neg p_2)))$.
2. By 1.1.8 it is sufficient to show that we can express $\vee$ using $\neg, \wedge$, which holds since $(p_1 \vee p_2)$ is LE to $(\neg((\neg p_1) \wedge (\neg p_2)))$.

3. By 1.1.8 it is sufficient to show that we can express $\vee$ using $\neg, \rightarrow$, which holds since $(p_1 \vee p_2)$ is LE to $((\neg p) \rightarrow q)$.

$\square$

Lecture 3 Monday 08/10/18

Example. The following are not adequate.

1. $\{\wedge, \vee\}$. If ϕ is built using $\wedge, \vee$, then $F_\phi(T, \ldots, T) = T$. Proof by induction on number of connectives.
2. $\{\neg, \leftrightarrow\}$. (TODO Exercise: proof)

Example. The NOR connective $\downarrow$ has the following truth table.

p	q	$(p \downarrow q)$
T	T	F
T	F	F
F	T	F
F	F	T

.

$(p \downarrow q)$ is LE to $((\neg p) \wedge (\neg q))$. $\{\downarrow\}$ is adequate. $(p \downarrow p)$ is LE to $(\neg p)$ and $((p \downarrow p) \downarrow (q \downarrow q))$ is LE to $(p \wedge q)$. So as $\{\neg, \vee\}$ is adequate, so is $\{\downarrow\}$.

1.2 A formal system for propositional logic

Idea is to try to generate all tautologies from basic assumptions, or axioms, using appropriate deduction rules. A very general definition is the following.

Definition 1.2.1.

1. A **formal deduction system** Σ has the following ingredients.
   (a) a non-zero **alphabet** A of symbols,
   (b) a non-empty subset $\mathcal{F}$ of the set of all finite sequences, or **strings**, of elements of A, the **formulas** of Σ,
   (c) a subset $\mathcal{A} \subseteq \mathcal{F}$ called the **axioms** of Σ, and
   (d) a collection of **deduction rules**.
2. A **proof** in Σ is a finite sequence of formulas in $\mathcal{F}$ $\phi_1, \ldots, \phi_n$ such that each ϕ_i is either an axiom in $\mathcal{A}$ or is obtained from $\phi_1, \ldots, \phi_{i-1}$ using one of the deduction rules. The last, or any, formula in a proof is a **theorem** of Σ.

Write $\vdash_\Sigma \phi$ for 'ϕ is a theorem of Σ'.

Remark 1.2.2.

1. If $\phi \in \mathcal{A}$, then $\vdash_\Sigma \phi$.
2. We should have an algorithm to test whether a string is a formula and whether it is an axiom. Then a computer can systematically generate all possible proofs in Σ, and check whether something is a proof. Say Σ is **recursive** in this case.

The main example is the following.

Definition 1.2.3. The formal system L for propositional logic has the following.

1. Alphabet. Alphabets are
   (a) variables $p_1, p_2, \ldots$,
   (b) connectives $\neg, \rightarrow$, and

   (c) punctuation (,).

2. Formulas. **L-formulas** are defined in 1.1.2 for $\neg, \to$ by
   (a) any variable p_i is a formula,
   (b) if ϕ, ψ are formulas so are $(\neg\phi), (\phi \to \psi)$, and
   (c) any formula arises in this way.

3. Axioms. Suppose ϕ, ψ, χ are L-formulas, then the axioms of L are
   (A1) $(\phi \to (\psi \to \phi))$,
   (A2) $((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi)))$, and
   (A3) $(((\neg\psi) \to (\neg\phi)) \to (\phi \to \psi))$.

4. Deduction rules. **Modus Ponens** (MP), from formulas $\phi, (\phi \to \psi)$, deduce ψ.

Example. Suppose ϕ is an L-formula. Then $\vdash_L (\phi \to \phi)$. Here is a proof in L.

1	$(\phi \to ((\phi \to \phi) \to \phi))$	(A1)
2	$((\phi \to ((\phi \to \phi) \to \phi)) \to ((\phi \to (\phi \to \phi)) \to (\phi \to \phi)))$	(A2)
3	$((\phi \to (\phi \to \phi)) \to (\phi \to \phi))$	$(1, 2, \mathrm{MP})$
4	$(\phi \to (\phi \to \phi))$	(A1)
5	$(\phi \to \phi)$	$(3, 4, \mathrm{MP})$

Lecture 4 Thursday 11/10/18

Definition 1.2.4. Suppose Γ is a set of L-formulas. A **deduction from** Γ is a finite sequence of L-formulas $\phi_1, \ldots, \phi_n$ such that each ϕ_i is either an axiom, a formula in Γ, or is obtained from previous formulas $\phi_1, \ldots, \phi_{i-1}$ using the deduction rule MP. Write $\Gamma \vdash_L \phi$ if there is a deduction from Γ ending in ϕ. Say ϕ is a **consequence** of Γ. So $\emptyset \vdash_L \phi$ is the same as $\vdash_L \phi$.

Theorem 1.2.5 (Deduction theorem)**.** Suppose Γ is a set of L-formulas and ϕ, ψ are L-formulas. Suppose $\Gamma \cup \{\phi\} \vdash_L \psi$. Then $\Gamma \vdash_L (\phi \to \psi)$.

Corollary 1.2.6 (Hypothetical syllogism)**.** Suppose ϕ, ψ, χ are L-formulas and $\vdash_L (\phi \to \psi)$ and $\vdash_L (\psi \to \chi)$. Then $\vdash_L (\phi \to \chi)$.

Proof. Use deduction theorem with $\Gamma = \emptyset$. Show $\{\phi\} \vdash_L \chi$. Here is a deduction of χ from ϕ.

1	$(\phi \to \psi)$	(theorem of L)
2	$(\psi \to \chi)$	(theorem of L)
3	ϕ	(assumption)
4	ψ	$(1, 3, \mathrm{MP})$
5	χ	$(2, 4, \mathrm{MP})$

Thus $\{\phi\} \vdash_L \chi$. By deduction theorem, $\emptyset \vdash_L (\phi \to \chi)$, that is $\vdash_L (\phi \to \chi)$. □

Proposition 1.2.7. Suppose ϕ, ψ are L-formulas. Then

1. $\vdash_L ((\neg\psi) \to (\psi \to \phi))$,
2. $\{(\neg\psi), \psi\} \vdash_L \phi$, and
3. $\vdash_L (((\neg\phi) \to \phi) \to \phi)$.

Proof.

1. Problem sheet 1.

2. By 1 and MP twice.

3. Suppose χ is any formula. Then $\{(\neg\phi), ((\neg\phi) \to \phi)\} \vdash_L \chi$ by 2 and MP. Let α be any axiom and let χ be $(\neg\alpha)$. Apply deduction theorem to get $\{((\neg\phi) \to \phi)\} \vdash_L ((\neg\phi) \to (\neg\alpha))$. Using A3 and MP we get $\{((\neg\phi) \to \phi)\} \vdash_L (\alpha \to \phi)$. As α is an axiom we get from MP $\{((\neg\phi) \to \phi)\} \vdash_L \phi$. Now use deduction theorem to obtain $\vdash_L (((\neg\phi) \to \phi) \to \phi)$.

□

Proof of 1.2.5. Suppose $\Gamma \cup \{\phi\} \vdash_L \psi$ using a deduction of length n. Show by induction on n that $\Gamma \vdash_L (\phi \to \psi)$.

1. Base step is $n = 1$. In this case ψ is either an axiom or in Γ or is ϕ. In the first two cases $\Gamma \vdash_L \psi$ is a one line deduction. Using the A1 axiom $(\psi \to (\phi \to \psi))$ and MP we obtain $\Gamma \vdash_L (\phi \to \psi)$. If ϕ is ψ we have $\Gamma \vdash_L (\phi \to \phi)$ by 1.2.3. This finishes the base case.

2. Inductive step. In our deduction of ψ from $\Gamma \cup \{\phi\}$ either ψ is an axiom, or in Γ, or is ϕ, or ψ is obtained from earlier steps using MP. In the first three cases we argue as in the base case to get $\Gamma \vdash_L (\phi \to \psi)$. In the last case there are formulas χ, $(\chi \to \psi)$ earlier in the deduction. We use the inductive hypothesis to get $\Gamma \vdash_L (\phi \to \chi)$ and $\Gamma \vdash_L (\phi \to (\chi \to \psi))$. We have the A2 axiom $((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi)))$. This A2 axiom and MP twice we obtain $\Gamma \vdash_L (\phi \to \chi)$ as required, completing the inductive step.

□

Lecture 5
Friday
12/10/18

1.3 Soundness and completeness of L

Theorem 1.3.1 (Soundness theorem of L)**.** Suppose ϕ is a theorem of L. Then ϕ is a tautology.

Definition 1.3.2. A **propositional valuation** v is an assignment of truth values to the propositional variables $p_1, p_2, \ldots$. So $v(p_i) \in \{T, F\}$ for $i \in \mathbb{N}$.

Note. Using the truth table rules, this assigns a truth value $v(\phi) \in \{T, F\}$ to every L-formula ϕ satisfying $v((\neg\phi)) \neq v(\phi)$, etc. See problem sheet 2, question 3(b).

By induction on the length of a proof of ϕ it is enough to show

1. every axiom is a tautology, and

2. MP preserves tautologies, that is if $\psi, (\psi \to \chi)$ are tautologies, so is χ.

Proof of 1.3.1.

1. Use truth tables, or argue as follows. For A2, suppose for a contradiction there is a valuation v with $v(((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi)))) = F$. Then
$$v((\phi \to (\psi \to \chi))) = T, \tag{1}$$
and
$$v(((\phi \to \psi) \to (\phi \to \chi))) = F. \tag{2}$$
By (2), $v((\phi \to \psi)) = T$ and $v((\phi \to \chi)) = F$. So by the latter, $v(\phi) = T$ and $v(\chi) = F$. By the former, $v(\psi) = T$. This contradicts (1). (TODO Exercise: for A1 and A3)

2. If v is a valuation and $v(\psi) = T$ and $v((\psi \to \chi)) = T$ then $v(\chi) = T$.

□

Theorem 1.3.3 (Generalisation of Soundness theorem of L)**.** Suppose Γ is a set of formulas and ϕ a formula with $\Gamma \vdash_L \phi$. Suppose v is a valuation with $v(\psi) = T$ for all $\psi \in \Gamma$. Then $v(\phi) = T$.

Proof. Same proof. (TODO Exercise) □

Theorem 1.3.4 (Completeness theorem of L)**.** Suppose ϕ is a tautology, that is $v(\phi) = T$ for every valuation v. Then $\vdash_L \phi$.

The following are steps in the proof.

1. If $v(\phi) = T$ for all valuations v, want to show $\vdash_L \phi$.
2. Try to prove a generalisation. Suppose that for every v with $v(\Gamma) = T$, that is $v(\psi) = T$ for all $\psi \in \Gamma$, we have $v(\phi) = T$. Then $\Gamma \vdash_L \phi$.
3. Equivalently, if $\Gamma \nvdash_L \phi$, show there is a valuation v with $v(\Gamma) = T$ and $v(\phi) = F$.

Definition 1.3.5. A set Γ of L-formulas is **consistent** if there is no L-formula ϕ such that $\Gamma \vdash_L \phi$ and $\Gamma \vdash_L (\neg\phi)$.

Proposition 1.3.6. Suppose Γ is a consistent set of L-formulas and $\Gamma \nvdash_L \phi$. Then $\Gamma \cup \{(\neg\phi)\}$ is consistent.

Proof. Suppose not. So there is some formula ψ with

$$\Gamma \cup \{(\neg\phi)\} \vdash_L \psi, \tag{3}$$

and

$$\Gamma \cup \{(\neg\phi)\} \vdash_L (\neg\psi). \tag{4}$$

Apply deduction theorem to (4), $\Gamma \vdash_L ((\neg\phi) \to (\neg\psi))$. By A3 and MP we obtain $\Gamma \vdash_L (\psi \to \phi)$. By this, (3), and MP, $\Gamma \cup \{(\neg\phi)\} \vdash_L \phi$. By deduction theorem, $\Gamma \vdash_L ((\neg\phi) \to \phi)$. By 1.2.7(3), $\vdash_L (((\neg\phi) \to \phi) \to \phi)$. So by these and MP, $\Gamma \vdash_L \phi$. This contradicts $\Gamma \nvdash_L \phi$. □

Proposition 1.3.7 (Lindenbaum's lemma)**.** Suppose Γ is a consistent set of L-formulas. Then there is a consistent set of formulas $\Gamma^* \supseteq \Gamma$ such that for every ϕ either $\Gamma^* \vdash_L \phi$ or $\Gamma^* \vdash_L (\neg\phi)$.

Sometimes say Γ^* is **complete**.

Proof. The set of L-formulas is countable, so we can list the L-formulas as $\phi_0, \phi_1, \dots$. It is countable because the alphabet $\neg, \to,), (, p_1, p_2, \dots$ is countable, and the formulas are finite sequences from this alphabet. Define inductively sets of formulas $\Gamma_0 \subseteq \Gamma_1 \subseteq \dots$ where $\Gamma_0 = \Gamma$ and $\Gamma^* = \cup_{i \in \mathbb{N}} \Gamma_i$. Suppose Γ_n has been defined. If $\Gamma_n \vdash_L \phi_n$ then let $\Gamma_{n+1} = \Gamma_n$. If $\Gamma_n \nvdash_L \phi_n$ then let $\Gamma_{n+1} = \Gamma_n \cup \{(\neg\phi_n)\}$. An easy induction using 1.3.6 shows that each Γ_i is consistent. Claim that Γ^* is consistent. If $\Gamma^* \vdash_L \phi$ and $\Gamma^* \vdash_L (\neg\phi)$ then as deductions are finite sequence of formulas, $\Gamma_n \vdash_L \phi$ and $\Gamma_n \vdash_L (\neg\phi)$ for some $n \in \mathbb{N}$, a contradiction. Let ϕ be any formula. So $\phi = \phi_n$ for some n. If $\Gamma^* \nvdash_L \phi$ then $\Gamma_n \nvdash_L \phi$. So by construction $\Gamma_{n+1} \vdash_L (\neg\phi)$ as $(\neg\phi) = (\neg\phi_n) \in \Gamma_{n+1}$. Thus $\Gamma^* \vdash_L (\neg\phi)$. □

Lecture 6 Monday 15/10/18

Lemma 1.3.8. Let Γ^* be as above. Then there is a valuation v such that for every L-formula ϕ, $v(\phi) = T$ iff $\Gamma^* \vdash_L \phi$.

Corollary 1.3.9. Suppose Δ is a set of L-formulas which is consistent and $\Delta \nvdash_L \phi$. Then there is a valuation v with $v(\Delta) = T$ and $v(\phi) = F$.

Proof. Let $\Gamma = \Delta \cup \{(\neg\phi)\}$. By 1.3.6, Γ is consistent. By 1.3.7 there is $\Gamma^* \supseteq \Gamma$ which is still consistent and such that for every χ either $\Gamma^* \vdash_L \chi$ or $\Gamma^* \vdash_L (\neg\chi)$. By 1.3.8 there is a valuation v with $v(\Gamma^*) = T$. In particular $v(\Delta) = T$ and $v((\neg\phi)) = T$. So $v(\phi) = F$. □

Proof of 1.3.4. Suppose $\nvdash_L \phi$. Apply 1.3.9 with $\Delta = \emptyset$. This is consistent due to the Soundness theorem. There is a valuation v with $v(\phi) = F$. □

Proof of 1.3.8. Let Γ^* be a consistent set of L-formulas such that for every L-formula ϕ either $\Gamma^* \vdash_L \phi$ or $\Gamma^* \vdash_L (\neg\phi)$. Want a valuation v with $v(\phi) = T$ for all $\phi \in \Gamma^*$, that is $v(\phi) = T$ iff $\Gamma^* \vdash_L \phi$. Note that for each variable p_i either $\Gamma^* \vdash_L p_i$ or $\Gamma^* \vdash_L (\neg p_i)$. So let v be the valuation with $v(p_i) = T$ iff $\Gamma^* \vdash_L p_i$. Prove by induction on the length of ϕ that $v(\phi) = T$ iff $\Gamma^* \vdash_L \phi$. Base case for ϕ is just a propositional variable. This case is by definition of v. Inductive step is the following.

1. Assume that ϕ is $(\neg\psi)$.

   $\Longrightarrow$ $v(\phi) = T$ gives $v(\psi) = F$ since v is a valuation. By inductive hypothesis, $\Gamma^* \nvdash_L \psi$. Then Lindenbaum property gives $\Gamma^* \vdash_L (\neg\psi)$, that is $\Gamma^* \vdash_L \phi$.

   $\Longleftarrow$ Conversely suppose $\Gamma^* \vdash_L \phi$. By consistency $\Gamma^* \nvdash_L \psi$. By inductive hypothesis, $v(\psi) = F$. As v is a valuation we obtain $v((\neg\psi)) = T$, that is $v(\phi) = T$.

2. Assume that ϕ is $(\psi \to \chi)$.

   $\Longleftarrow$ Suppose $v(\phi) = F$. Show $\Gamma^* \nvdash_L \phi$. Then $v(\psi) = T$ and $v(\chi) = F$. By inductive hypothesis, $\Gamma^* \vdash_L \psi$ and $\Gamma^* \nvdash_L \chi$. If $\Gamma^* \vdash_L \phi$ then using $\Gamma^* \vdash_L \psi$ and MP we get $\Gamma^* \vdash_L \chi$, which is a contradiction. So $\Gamma^* \nvdash_L \phi$.

   $\Longrightarrow$ Suppose $\Gamma^* \nvdash_L \phi$, that is $\Gamma^* \nvdash_L (\psi \to \chi)$. Then $\Gamma^* \nvdash_L \chi$ as $\vdash_L (\chi \to (\psi \to \chi))$. Also $\Gamma^* \nvdash_L (\neg\psi)$ as $\vdash_L ((\neg\psi) \to (\psi \to \chi))$ by 1.2.7(1). By inductive hypothesis, $v(\chi) = F$ and $v((\neg\psi)) = F$ so $v(\psi) = T$. Thus $v(\phi) = F$, which does the inductive step.

□

Corollary 1.3.10. Suppose Δ is a set of L-formulas and ϕ is an L-formula. Then

1. Δ is consistent iff there is a valuation v with $v(\Delta) = T$, and
2. $\Delta \vdash_L \phi$ iff for every valuation v with $v(\Delta) = T$ we have $v(\phi) = T$.

Proof. TODO Exercise: deduce these from the preliminaries to Completeness theorem - warning that in 2 do not assume that Δ is consistent. □

Theorem 1.3.11 (Compactness theorem for L)**.** Suppose Δ is a set of L-formulas. The following are equivalent.

1. There is a valuation v with $v(\Delta) = T$.
2. For every finite subset $\Delta_0 \subseteq \Delta$ there is a valuation w with $w(\Delta_0) = T$.

Proof. By 1.3.10 1 holds iff Δ is consistent. Similarly 2 holds iff every finite subset of Δ is consistent. But if $\Delta \vdash_L \psi$ and $\Delta \vdash_L (\neg\psi)$ then as deductions are finite and therefore only involve finitely many formulas in Δ, for some finite $\Delta_0 \subseteq \Delta$, $\Delta_0 \vdash_L \psi$ and $\Delta_0 \vdash_L (\neg\psi)$. □

Let P be the set of sequences of $\{T, F\}$, that is the set of functions $f : \mathbb{N} \to \{T, F\}$. Topologise with basic open sets. For $a_1, \dots, a_n \in \{T, F\}$ consider $O(a_1, \dots, a_n)$, all sequences starting $a_1, \dots, a_n$. (TODO Exercise: use Compactness theorem to prove P is compact)

Lecture 7 Thursday 18/10/18

Lecture 7 is a problem class.

Lecture 8 Friday 19/10/18

2 Predicate logic

Predicate logic is first-order logic. Plan is the following.

1. Introduce the mathematical objects, first-order structures.
2. Introduce the formulas, first-order languages.
3. Describe a formal system.
4. Show that its theorems are precisely the formulas true in all structures. This is Gödel's completeness theorem.

1 and 2 are semantics while 3 and 4 are syntax.

2.1 Structures

Definition 2.1.1. Suppose A is a set and $n \geq 1$ and $n \in \mathbb{N}$. An n**-ary relation** on A is a subset $\overline{R} \subseteq A^n = \{(a_1, \dots, a_n) \mid a_i \in A\}$ of n-tuples. An n**-ary function** on A is a function $\overline{f} : A^n \to A$.

Example.

1. Ordering $\leq$ on $\mathbb{R}$ is a binary relation on $\mathbb{R}$.
2. $+$ on $\mathbb{C}$ is a binary function on $\mathbb{C}$.
3. Even integers as a subset of $\mathbb{Z}$ is a unary relation on $\mathbb{Z}$.

If $\overline{R} \subseteq A^n$ is an n-ary relation and $a_1, \dots, a_n \in A$, write $\overline{R}(a_1, \dots, a_n)$ to mean $(a_1, \dots, a_n) \in \overline{R}$.

Definition 2.1.2. A **first-order structure** $\mathcal{A}$ consists of

1. a non-empty set A, the **domain** of $\mathcal{A}$,
2. a set $\left\{\overline{R_i} \mid i \in I\right\}$ of relations on A for $\overline{R_i} \subseteq A^{n_i}$,
3. a set $\left\{\overline{f_j} \mid j \in J\right\}$ of functions on A for $\overline{f_j} : A^{m_j} \to A$, and
4. a set $\{\overline{c_k} \mid k \in K\}$ of **constants**, just elements of A.

The sets I, J, K are indexing sets and can be empty. Usually subsets of $\mathbb{N}$. The information $(n_i \mid i \in I)$, $(m_j \mid j \in J)$, and the set K is called the **signature** of $\mathcal{A}$. Might denote the structure by

$$\mathcal{A} = \left\langle A; \left(\overline{R_i} \mid i \in I\right), \left(\overline{f_j} \mid j \in J\right), \left(\overline{c_k} \mid k \in K\right)\right\rangle.$$

Example.

1. Orderings on $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ where

$$I = \{1\}, \qquad J = \emptyset, \qquad K = \emptyset, \qquad \overline{R_1}(a_1, a_2) \iff a_1 < a_2.$$

2. Groups.
   (a) $\overline{R}$, the binary relation for equality,
   (b) $\overline{m}$, the binary function for multiplication,
   (c) $\overline{i}$, the unary function for inversion, and
   (d) $\overline{e}$, the constant for identity element.
3. Rings.
   (a) $\overline{R}$, the binary relation for equality,
   (b) $\overline{m}$, the binary function for multiplication,
   (c) $\overline{a}$, the binary function for addition,
   (d) $\overline{n}$, the binary function for negation,
   (e) $\overline{0}$, the constant for zero, and
   (f) $\overline{1}$, the constant for one.
4. Graphs.
   (a) $\overline{R}$, the binary relation for equality, and
   (b) $\overline{E}$, the binary relation for adjacency.

2.2 First-order languages

Definition 2.2.1. A **first-order language** $\mathcal{L}$ has an alphabet of symbols of the following types.

1. Variables $x_0, x_1, \ldots$.
2. Punctuation (,), ,.
3. Connectives $\neg$, $\rightarrow$.
4. **Quantifier** $\forall$.
5. Relation symbols R_i for $i \in I$.
6. Function symbols f_j for $j \in J$.
7. Constant symbols c_k for $k \in K$.

Here I, J, K are indexing sets and could have $J, K = \emptyset$. Each R_i comes equipped with an **arity** n_i. Each f_j comes equipped with an arity m_j. The information $(n_i \mid i \in I)$, $(m_j \mid j \in J)$, K is called the signature of $\mathcal{L}$. A first-order structure $\mathcal{A}$ with the same signature as $\mathcal{L}$ is referred to as an $\mathcal{L}$-structure.

Definition 2.2.2. A **term** of $\mathcal{L}$ is defined as follows.

1. Any variable is a term.
2. Any constant symbol is a term.
3. If f is an m-ary function symbol of $\mathcal{L}$ and $t_1, \ldots, t_m$ are terms, then $f(t_1, \ldots, t_m)$ is also a term.
4. Any term arises in this way.

Example. Suppose $\mathcal{L}$ has a binary function symbol f and constant symbols c_1, c_2. Some terms are

$$c_1, \qquad c_2, \qquad x_1, \qquad f(c_1, x_1), \qquad f(f(c_1, x_2), c_2), \qquad f(x_1, f(f(c_1, x_2), c_2)).$$

Some not terms are

$$ffx_1 \quad (\text{not well-formed}).$$

Lecture 9 Monday 22/10/18

Definition 2.2.3.

1. An **atomic formula** of $\mathcal{L}$ is of the form $R(t_1, \ldots, t_n)$ where R is an n-ary relation symbol of $\mathcal{L}$ and $t_1, \ldots, t_n$ are terms.
2. The **formulas** of $\mathcal{L}$ are defined as follows.
   (a) Any atomic formula is a formula.
   (b) If ϕ, ψ are $\mathcal{L}$-formulas then $(\neg\phi)$, $(\phi \rightarrow \psi)$, $(\forall x)\,\phi$ are $\mathcal{L}$-formulas, where x is any variable.
   (c) Every $\mathcal{L}$-formula arises in this way.

Example. Suppose $\mathcal{L}$ has a binary function symbol f, a unary relation symbol P, a binary relation symbol R, and constant symbols c_1, c_2. Some terms are

$$x_1, \qquad c_1, \qquad f(x_1, c_1), \qquad f(f(x_1, c_1), x_2).$$

Some atomic formulas are

$$P(x_1), \qquad R(f(x_1, c_1), x_2).$$

Some formulas are

$$(\forall x_1)(R(f(x_1, c_1), x_2) \rightarrow P(x_1)).$$

Definition 2.2.4. Suppose ϕ, ψ are $\mathcal{L}$-formulas. $(\exists x)\,\phi$ means $(\neg\,(\forall x)\,(\neg\phi))$. $(\phi \vee \psi)$ means $((\neg\phi) \to \psi)$, etc as in propositional logic.

Definition 2.2.5. Suppose $\mathcal{L}$ is a first-order language with relation symbols R_i of arity n_i for $i \in I$, function symbols f_j of arity m_j for $j \in J$, and constant symbols c_k for $k \in K$. An **$\mathcal{L}$-structure** is a structure

$$\mathcal{A} = \left\langle A; \left(\overline{R_i} \mid i \in I\right), \left(\overline{f_j} \mid j \in J\right), \left(\overline{c_k} \mid k \in K\right)\right\rangle$$

of the same signature as $\mathcal{L}$.

There is a correspondence between the relation, function, and constant symbols of $\mathcal{L}$ and the actual relations, functions, and constants in $\mathcal{A}$, and the arities match up. This correspondence, or $\mathcal{A}$, is called an **interpretation** of $\mathcal{L}$.

Definition 2.2.6. With the same notation, suppose $\mathcal{A}$ is an $\mathcal{L}$-structure. A **valuation** in $\mathcal{A}$ is a function v from the set of terms of $\mathcal{L}$ to A satisfying

1. $v\,(c_k) = \overline{c_k}$, and
2. if $t_1, \dots, t_m$ are terms of $\mathcal{L}$ and f is an m-ary function symbol then

   $$v\,(f\,(t_1, \dots, t_m)) = \overline{f}\,(v\,(t_1), \dots, v\,(t_m)),$$

   where $\overline{f}$ is the interpretation of f in $\mathcal{A}$.

Lemma 2.2.7. Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and $a_0, a_1, \dots \in A$. Then there is a unique valuation v in $\mathcal{A}$ with $v\,(x_l) = a_l$ for all $l \in \mathbb{N}$, where the variables of $\mathcal{L}$ are $x_0, x_1, \dots$.

Proof. By induction on the length of terms. Show that if we let

1. $v\,(x_l) = a_l$ for all $l \in \mathbb{N}$,
2. $v\,(c_k) = \overline{c_k}$ for all $k \in K$, and
3. $v\,(f\,(t_1, \dots, t_m)) = \overline{f}\,(v\,(t_1), \dots, v\,(t_m))$,

then v is a well-defined valuation. $\square$

Example. Groups with signature of

1. binary relation symbol R for equality,
2. binary function symbol m for multiplication,
3. unary function symbol i for inversion, and
4. constant e for identity element.

Let G be a group and $g, h \in G$. Let v be a valuation with $v\,(x_0) = g$ and $v\,(x_1) = h$. Then

$$v\,(m\,(m\,(x_0, x_1), i\,(x_0))) = \overline{m}\,(v\,(m\,(x_0, x_1)), v\,(i\,(x_0))) = \overline{m}\,(v\,(x_0), v\,(x_1))\,\overline{i}\,(v\,(x_0)) = ghg^{-1}.$$

Definition 2.2.8. Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and x_l is any variable. Suppose v, w are valuations in $\mathcal{A}$. We say v, w are x_l-equivalent if $v\,(x_m) = w\,(x_m)$ whenever $m \neq l$.

Definition 2.2.9. Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and v is a valuation in $\mathcal{A}$. Define, for an $\mathcal{L}$-formula ϕ, what is meant by v **satisfies** ϕ in $\mathcal{A}$ by the following.

1. Suppose R is an n-ary relation symbol and $t_1, \dots, t_n$ are terms of $\mathcal{L}$. Then v satisfies the atomic formula $R\,(t_1, \dots, t_n)$ iff $\overline{R}\,(v\,(t_1), \dots, v\,(t_n))$ holds in $\mathcal{A}$.
2. Suppose ϕ, ψ are $\mathcal{L}$-formulas and we already know about valuations satisfying ϕ, ψ.

(a) v satisfies $(\neg\phi)$ in $\mathcal{A}$ iff v does not satisfy ϕ in $\mathcal{A}$.

(b) v satisfies $(\phi \to \psi)$ in $\mathcal{A}$ iff it is not the case that v satisfies ϕ in $\mathcal{A}$ and v does not satisfy ψ in $\mathcal{A}$.

(c) v satisfies $(\forall x_l)\,\phi$ in $\mathcal{A}$ iff whenever w is a valuation in $\mathcal{A}$ which is x_l-equivalent to v, then w satisfies ϕ in $\mathcal{A}$.

Lecture 10 Thursday 25/10/18

Remark 2.2.10. 2.2.9 does not work if we allow empty structure.

If v satisfies ϕ, write $v[\phi] = T$. If v does not satisfy ϕ, write $v[\phi] = F$. If every valuation in $\mathcal{A}$ satisfies ϕ, say that ϕ is **true** in $\mathcal{A}$ or $\mathcal{A}$ is a **model** of ϕ and write $\mathcal{A} \vDash \phi$. If $\mathcal{A} \vDash \phi$ for every $\mathcal{L}$-structure $\mathcal{A}$, we say that ϕ is **logically valid** and write $\vDash \phi$. These are the analogues of tautologies in the propositional logic. Difference is in propositional logic there is an algorithm to decide whether a given formula is a tautology. There is no such algorithm to decide whether a given $\mathcal{L}$-formula is logically valid or not, a consequence of Gödel's incompleteness theorem.

Example.

1. Suppose $\mathcal{L}$ has a binary relation symbol R. The $\mathcal{L}$-formula $(R(x_1, x_2) \to (R(x_2, x_3) \to R(x_1, x_3)))$ is true in $\mathcal{A} = \langle \mathbb{N}; < \rangle$, where R is interpreted as $<$. If not, there is a valuation v in $\mathcal{A}$ such that v satisfies $R(x_1, x_2)$ or v does not satisfy $(R(x_2, x_3) \to R(x_1, x_3))$. So $v[R(x_2, x_3)] = T$ and $v[R(x_1, x_3)] = F$. Let $v(x_i) = a_i \in \mathbb{N}$. So $a_1 < a_2$, $a_2 < a_3$, and $a_1 \not< a_3$. As $<$ is transitive on $\mathbb{N}$, this is a contradiction.

2. The same formula is not true in the structure $\mathcal{B}$ with domain $\mathbb{N}$ where we interpret $R(x_i, x_j)$ as $x_i \neq x_j$. Take a valuation in $\mathcal{B}$ with $v(x_1) = 1 = v(x_3)$ and $v(x_2) = 2$. v does not satisfy the formula in $\mathcal{B}$.

3. Recall that $(\exists x_1)\,\phi$ is an abbreviation for $(\neg(\forall x_1)(\neg\phi))$. Suppose $\mathcal{A}$ is an $\mathcal{L}$-structure and ϕ an $\mathcal{L}$-formula. Let v be a valuation in $\mathcal{A}$. Then v satisfies $(\exists x_1)\,\phi$ in $\mathcal{A}$ iff there is a valuation w which is x_1-equivalent to v such that w satisfies ϕ. Suppose v satisfies $(\neg(\forall x_1)(\neg\phi))$. Using 2.2.9 v does not satisfy $(\forall x_1)(\neg\phi)$. So there is valuation w x_1-equivalent to v such that w does not satisfy $(\neg\phi)$. Such a w satisfies ϕ. (TODO Exercise: converse)

Example. $(\forall x_1)(\exists x_2)\,R(x_1, x_2)$ is true in $\langle \mathbb{Z}; < \rangle$ and $\langle \mathbb{N}; < \rangle$ but not in $\langle \mathbb{N}; > \rangle$.

TODO Exercise: Suppose ϕ is any $\mathcal{L}$-formula. Then

1. $((\exists x_1)(\forall x_2)\,\phi \to (\forall x_2)(\exists x_1)\,\phi)$ is logically valid, and

2. $((\forall x_2)(\exists x_1)\,\phi \to (\exists x_1)(\forall x_2)\,\phi)$ is not necessarily logically valid.

Consider the propositional formula χ by $(p_1 \to (p_2 \to p_1))$. Suppose $\mathcal{L}$ is a first-order language and ϕ_1, ϕ_2 are $\mathcal{L}$-formulas. Substitute ϕ_1 in place of p_1 and ϕ_2 in place of p_2 in χ. We obtain an $\mathcal{L}$-formula θ by $(\phi_1 \to (\phi_2 \to \phi_1))$. Check that as χ is a tautology θ is logically valid. (TODO Exercise)

Definition 2.2.11. Suppose χ is an $\mathcal{L}$-formula involving propositional variables $p_1, \ldots, p_n$. Suppose $\mathcal{L}$ is a first-order language and $\phi_1, \ldots, \phi_n$ are $\mathcal{L}$-formulas. A **substitution instance** of χ is obtained by replacing each p_i in χ by ϕ_i for $i = 1, \ldots, n$. Call the result θ.

Theorem 2.2.12.

1. θ is an $\mathcal{L}$-formula, and

2. if χ is a tautology then θ is logically valid.

Lecture 11 Friday 26/10/18

Proof. Take an $\mathcal{L}$-structure $\mathcal{A}$ and a valuation v in $\mathcal{A}$. Use this to define a propositional valuation w with $w(p_i) = v[\phi_i]$ for $i \leq n$. Then prove by induction on the number of connectives in χ that $w(\chi) = v[\theta]$. In particular if χ is a tautology, then $v[\theta] = T$. In the inductive step, consider χ is $(\alpha \to \beta)$. So θ is $(\theta_1 \to \theta_2)$ where θ_1 is obtained from α and θ_2 is obtained from β. By inductive hypothesis $w(\alpha) = v[\theta_1]$ and $w(\beta) = v[\theta_2]$. So $w(\alpha \to \beta) = v[(\theta_1 \to \theta_2)]$, etc. (TODO Exercise) $\square$

Note. Not all logically valid formulas arise in this way.

Example. $((\exists x_2)(\forall x_1)\,\phi \to (\forall x_1)(\exists x_2)\,\phi)$.

2.3 Bound and free variables in formulas

Definition 2.3.1. Suppose ϕ, ψ are $\mathcal{L}$-formulas and $(\forall x_i)\,\phi$ occurs as a subformula of ψ, that is ψ is $\dots(\forall x_i)\,\phi\dots$. We say that ϕ is the **scope** of that quantifier $(\forall x_i)$ here in ψ. An occurrence of a variable x_j in ψ is **bound** if it is in the scope of a quantifier $(\forall x_j)$ in ψ, or it is the x_j here. Otherwise it is a free occurrence of x_j. Variables having a free occurrence in ψ are called **free** variables of ψ. A formula with no free variables is called a **closed** formula or a **sentence** of $\mathcal{L}$.

Example.

1. Let ψ_1 be $(R_1(x_1, x_2) \to (\forall x_3)\, R_2(x_1, x_3))$. Then x_1 and x_2 are free, and x_3 is bound with scope $R_2(x_1, x_3)$.
2. Let ψ_2 be $((\forall x_1)\, R_1(x_1, x_2) \to R_2(x_1, x_2))$. Then the first x_1 is bound with scope $R_1(x_1, x_2)$, and the second x_1 and x_2 are free. Compare with $(\forall x_1)\,(R_1(x_1, x_2) \to R_2(x_1, x_2))$. Then x_1 is bound with scope $(R_1(x_1, x_2) \to R_2(x_1, x_2))$, and x_2 is free.
3. Let ψ_3 be $((\exists x_1)\, R_1(x_1, x_2) \to (\forall x_2)\, R_2(x_2, x_3))$. Then x_1 and the second x_2 are bound with scope $R_1(x_1, x_2)$, and the first x_2 and x_3 are free.

Definition 2.3.2. If ψ is an $\mathcal{L}$-formula with free variables amongst $x_1, \dots, x_n$, we might write $\psi(x_1, \dots, x_n)$ instead of ψ. If $t_1, \dots, t_n$ are terms, by $\psi(t_1, \dots, t_n)$ we mean the $\mathcal{L}$-formula obtained by replacing each free occurrence of x_i in ψ by t_i.

Example. Let $\psi(x_1, x_2)$ be $((\forall x_1)\, R(x_1, x_2) \to (\forall x_3)\, R(x_1, x_2, x_3))$, t_1 be $f_1(x_1)$, and t_2 be $f_2(x_1, x_2)$. Then x_2 and the second x_1 are free. So $\psi(t_1, t_2)$ is

$$((\forall x_1)\, R_1(x_1, f_2(x_1, x_2)) \to (\forall x_3)\, R_2(f_1(x_1), f_2(x_1, x_2), x_3)).$$

Theorem 2.3.3. Suppose ϕ is a closed $\mathcal{L}$-formula and $\mathcal{A}$ is an $\mathcal{L}$-structure. Then either $\mathcal{A} \vDash \phi$ or $\mathcal{A} \vDash (\neg\phi)$. More generally, if ϕ has free variables amongst $x_1, \dots, x_n$ and v, w are valuations in $\mathcal{A}$ with $v(x_i) = w(x_i)$ for $i = 1, \dots, n$, then $v[\phi] = T$ iff $w[\phi] = T$. Allow $n = 0$ here for no free variables.

Proof. Note that the first statement follows from the generalisation. If ϕ has no free variables, then for any valuations v, w in $\mathcal{A}$, they agree on the free variables of ϕ so $v[\phi] = w[\phi]$. Prove the generalisation by induction on the number of connectives and quantifiers in ϕ.

1. Base case. ϕ is atomic, so ϕ is $R(t_1, \dots, t_m)$ for t_j terms. The t_j only involve variables amongst $x_1, \dots, x_n$. As v and w agree on these variables $v(t_j) = w(t_j)$. So
$$v[R(t_1, \dots, t_m)] = T \qquad \Longleftrightarrow \qquad \overline{R}(v(t_1), \dots, v(t_m)) \qquad \Longleftrightarrow \qquad w[R(t_1, \dots, t_m)] = T.$$
2. Inductive step. ϕ is $(\neg\psi)$, $(\psi \to \chi)$, or $(\forall x_i)\,\psi$. (TODO Exercise: first two cases) Suppose ϕ is $(\forall x_i)\,\psi$. Suppose $v[\phi] = F$. By 2.2.9 there is a valuation v' x_i-equivalent to v with $v'[\psi] = F$. The free variables of ψ are amongst $x_1, \dots, x_n, x_i$. Let w' be the valuation x_i-equivalent to w with $w'(x_i) = v'(x_i)$. Then v', w' agree on the free variables of ψ. By inductive hypothesis $v'[\psi] = w'[\psi]$ so $w'[\psi] = F$. As w' is x_i-equivalent to w we obtain $w[(\forall x_i)\,\psi] = F$.

□

Lecture 12 Monday 29/10/18

Remark 2.3.4. If $\mathcal{A}$ is an $\mathcal{L}$-structure and $\psi(x_1, \dots, x_n)$ an $\mathcal{L}$-formula, whose free variables are amongst $x_1, \dots, x_n$, and $a_1, \dots, a_n \in A$ for domain A then we write $\mathcal{A} \vDash \psi(a_1, \dots, a_n)$ to mean $v[\psi] = T$ for every valuation v in $\mathcal{A}$ with $v(x_i) = a_i$ for $i = 1, \dots, n$.

Note. By the proof of 2.3.3 this holds if $v[\psi] = T$ for some such valuation.

Example. An example where $\mathcal{A} \vDash (\forall x_1)\, \phi(x_1)$ but we have term t, and a valuation v in $\mathcal{A}$ with $v[\phi(t)] = F$. Let $\phi(x_1)$ be $((\forall x_2)\, R(x_2, x_2) \to S(x_1))$. Scope of x_2 is $R(x_1, x_2)$. Let t_1 be x_2, then $\phi(t_1)$ is $((\forall x_2)\, R(x_2, x_2) \to S(x_2))$. Suppose $\mathcal{A} = \langle \mathbb{N}; \leq, = 0\rangle$. Domain is $\mathbb{N} = \{0, 1, \dots\}$, $R(x_1, x_2)$ interpreted as $x_1 \leq x_2$, and $S(x_1)$ interpreted as $x_1 = 0$. So $\mathcal{A} \vDash (\forall x_1)\, \phi(x_1)$ but we choose a valuation $v(x_2) = 1$ then $v[\phi(t_1)] = F$ in $\mathcal{A}$.

Definition 2.3.5. Let ϕ be an $\mathcal{L}$-formula, x_i a variable, t an $\mathcal{L}$-term. We say t is free for x_i in ϕ if there is no variable x_j in t such that x_i has a free occurrence within the scope of a quantifier $(\forall x_j)$ in ϕ.

TODO Exercise: Let $t = f(x_3, x_2, x_5)$, ϕ_1 be $(((\forall x_2) R(x_1, x_4) \to K(x_1)) \to (\forall x_1) R(x_1, x_1))$, and ϕ_2 be $((\forall x_2)(R(x_2, x_4) \to (\forall x_1) K(x_1)) \to (\forall x_2) R(x_1, x_1))$. For which t is t free for x_1?

Theorem 2.3.6. Suppose $\phi(x_1)$ is an $\mathcal{L}$-formula, possibly with other free variables. Let t be a term free for x_1 in ϕ, then $\vDash ((\forall x_1) \phi(x_1) \to \phi(t))$. In particular, if $\mathcal{A}$ is an $\mathcal{L}$-structure with $\mathcal{A} \vDash (\forall x_1) \phi(x_1)$ then $A \vDash \phi(t)$.

Lemma 2.3.7. With this notation, suppose v is a valuation in $\mathcal{A}$. Let v' be the valuation in $\mathcal{A}$ which is x_1-equivalent to v, with $v'(x_1) = v(t)$. Then $v'[\phi(x_1)] = T$ iff $v[\phi(t)] = T$.

Proof. This is by induction on the number of connectives and quantifiers in ϕ.

1. Base case. ϕ is an atomic formula $R(u_1, \dots, u_m)$ where R is an m-ary relation symbol and $u_1, \dots, u_m$ are terms. Let u_i^* be the result of substituting t for x_1 in u_i. Then, by induction on the length of the terms, each u_i^* is a term and $v'(u_i) = v(u_i^*)$. Moreover, $\phi(t)$ is $R(u_1^*, \dots, u_m^*)$. Then
$$\begin{aligned} v'[\phi(x_1)] = T \quad &\iff \quad \mathcal{A} \vDash R(v'(u_1), \dots, v'(u_m)) \\ &\iff \quad \mathcal{A} \vDash R(v(u_1^*), \dots, v(u_m^*)) \\ &\iff \quad v[\phi(t)] = T. \end{aligned}$$

2. Inductive step. There are three cases,
   (a) ϕ is $(\neg\psi)$,
   (b) ϕ is $(\psi \to \chi)$, and
   (c) ϕ is $(\forall x_i)\psi$.

   We leave the first two cases as exercises and do the third. We can assume that $i \neq 1$. Otherwise x_1 is not free in ϕ and $\phi(t)$ is just ϕ. 2.3.7 then follows from 2.3.3. Note also that as t is free for x_1 in $(\forall x_i)\psi$, it follows that t is free for x_1 in ψ and x_i is not a variable in t. Suppose first that $v'[\phi(x_1)] = F$. We show that $v[\phi(t)] = F$. By 2.2.9, there is a valuation w' which is x_i-equivalent to v' with $w'[\psi(x_1)] = F$. Note that as $i \neq 1$,
$$w'(x_1) = v'(x_1) = v(t). \tag{5}$$
   Define a valuation w by
$$w(x_j) = \begin{cases} v(x_j) & j \neq 1, i \\ w'(x_i) & j = i \\ v(x_1) & j = 1 \end{cases}.$$
   So w is x_1-equivalent to w' and x_i-equivalent to v, noting that v, v' are x_i-equivalent and w, v' are x_i-equivalent. As x_i does not occur in t we have, by 2.3.3 and (5),
$$w(t) = v(t) = w'(x_1).$$
   We can now apply the induction hypothesis to w, w', and ψ. We obtain that $w[\psi(t)] = w'[\psi(x_1)] = F$. As w, v are x_i-equivalent, it follows that
$$v[(\forall x_i)\psi(t)] = F.$$
   So $v[\phi(t)] = F$, as required. We now prove the converse direction. We cannot argue by symmetry here. So suppose $v[\phi(t)] = F$. There is a valuation w which is x_i-equivalent to v with $w[\psi(t)] = F$. Let w' be the valuation x_1-equivalent to w with
$$w'(x_1) = w(t) = v(t) = v'(x_1).$$
   The fact that $w(t) = v(t)$ is as before. By the inductive hypothesis, $w'[\psi(x_1)] = w(\psi(t)) = F$. As w' is x_i-equivalent to v' we have
$$v'[(\forall x_i)\psi(x_1)] = F.$$
   So $v'[\phi(x_1)] = F$. This completes the inductive step.

□

Proof of 2.3.6. Suppose v is a valuation with $v[\phi(t)] = F$. Show $v[(\forall x_1)\phi(x_1)] = F$. Then

$$v[((\forall x_1)\phi(x_1) \to \phi(t))] = T.$$

Take v' x_1-equivalent to v and $v'(x_1) = v(t)$. Then by 2.3.7, $v'[\phi(x_1)] = F$, so $v[(\forall x_1)\phi(x_1)] = F$. □

2.4 The formal system $K_{\mathcal{L}}$

Definition 2.4.1. Suppose $\mathcal{L}$ is a first-order language. The formal system $K_{\mathcal{L}}$ has as formulas $\mathcal{L}$-formulas, and the following.

1. Axioms. For ϕ, χ, ψ $\mathcal{L}$-formulas,
   - (A1) $(\phi \to (\psi \to \phi))$,
   - (A2) $((\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi)))$,
   - (A3) $(((\neg\phi) \to (\neg\psi)) \to (\psi \to \phi))$,
   - (K1) $((\forall x_i)\phi(x_i) \to \phi(t))$, where t is a term free for x_i in ϕ and ϕ can have other free variables, and
   - (K2) $((\forall x_i)(\phi \to \psi) \to (\phi \to (\forall x_i)\psi))$, if x_i is not free in ϕ.
2. Deduction rules.
   - (a) Modus Ponens (MP), from formulas ϕ and $(\phi \to \psi)$ deduce ψ, and
   - (b) **Generalisation** (Gen), from formula ϕ deduce $(\forall x_i)\phi$.

A proof in $K_{\mathcal{L}}$ is a finite sequence of $\mathcal{L}$-formulas each of which is an axiom, or deduced from previous formulas in the proof using a rule of deduction. A theorem of $K_{\mathcal{L}}$ is the last formula in some proof. Write $\vdash_{K_{\mathcal{L}}} \phi$ for ϕ is a theorem in $K_{\mathcal{L}}$.

Note. Books do not always use $K_{\mathcal{L}}$, that is they write $\vdash \phi$.

Definition 2.4.2. Suppose Σ is a set of $\mathcal{L}$-formulas and ψ an $\mathcal{L}$-formula. A deduction of ψ from Σ is a finite sequence of formulas, ending with ψ, each of which is one of

1. an axiom,
2. a formula in Σ, or
3. obtained from earlier formulas in the deduction using MP or Gen, with the restriction that when Gen is applied it does not involve a variable occurring freely in a formula in Σ.

Write $\Sigma \vdash_{K_{\mathcal{L}}} \psi$ if there is a deduction from Σ to ψ.

Lecture 13 is a problem class.

Lecture 13 Thursday 01/11/18

Lecture 14 Friday 02/11/18

Remark 2.4.3.

1. If Σ consists of closed formulas, do not need to worry about the restriction on Gen.
2. $\phi \vdash (\forall x_1)\phi$.

Theorem 2.4.4. Suppose ϕ is an $\mathcal{L}$-formula which is a substitution instance of a tautology in propositional logic. Then $\vdash_{K_{\mathcal{L}}} \phi$.

Example. $((\neg(\neg\phi)) \to \phi)$ for an $\mathcal{L}$-formula ϕ, as this is a substitution instance of $((\neg(\neg p_1)) \to p_1)$. There is a tautology χ with propositional variables $p_1, \ldots, p_n$ and $\mathcal{L}$-formulas $\psi_1, \ldots, \psi_n$ such that ϕ is obtained from χ by substituting ψ_i for p_i for $i = 1, \ldots, n$. By Completeness of propositional logic in 1.3.4 there is a proof in L of χ by $\chi_1, \ldots, \chi_r$, where each χ_i is a propositional formula, that is in L, and $\chi_r = \chi$. If we substitute $\psi_1, \ldots, \psi_n$ for $p_1, \ldots, p_n$ in all χ_j we obtain a sequence of $\mathcal{L}$-formulas $\phi_1, \ldots, \phi_r$ which is a proof of $\phi = \phi_r$ in $K_{\mathcal{L}}$.

Theorem 2.4.5 (Soundness theorem of $K_{\mathcal{L}}$)**.** If $\vdash_{K_{\mathcal{L}}} \phi$ then $\vDash \phi$, that is it is logically valid.

Proof. Like in the proof for L, we need to show

1. axioms are logically valid, and
2. deduction rules preserve logical validity.

For axioms, A1, A2, A3 are substitution instances of propositional tautologies in 2.2.1 so are logically valid by 2.4.4. K1 is logically valid by 2.3.6. K2 is $((\forall x_i)(\phi \to \psi) \to (\phi \to (\forall x_i)\psi))$ if x_i is not free in ϕ. Suppose we have valuation v such that $v[(\phi \to (\forall x_i)\psi)] = F$. So $v[\phi] = T$ and $v[(\forall x_i)\psi] = F$. So there is a valuation v' x_i-equivalent to v with $v'[\psi] = F$. v and v' agree on all variables free in ϕ. So by 2.3.3 $v[\phi] = v'[\phi] = T$, so $v'[(\phi \to \psi)] = F$. So $v[(\forall x_i)(\phi \to \psi)] = F$. So $v[K_2] = T$. For deduction rules, MP is if $\vDash \phi$ and $\vDash (\phi \to \psi)$ then $\vDash \psi$, and Gen is if $\vDash \phi$ then $\vDash (\forall x_i)\phi$. (TODO Exercise) □

TODO Exercise: Suppose $\Sigma \vdash \psi$ then for every valuation v with $v[\sigma] = T$ for all $\sigma \in \Sigma$ we have $v[\psi] = T$.

Corollary 2.4.6. There is no $\mathcal{L}$-formula ϕ with $\vdash_{K_{\mathcal{L}}} \phi$ and $\vdash_{K_{\mathcal{L}}} (\neg\phi)$.

Theorem 2.4.7 (Deduction theorem)**.** Suppose $\mathcal{L}$ is a first-order language, Σ is a set of $\mathcal{L}$-formulas, and ϕ, ψ are $\mathcal{L}$-formulas. Then if $\Sigma \cup \{\phi\} \vdash \psi$ then $\Sigma \vdash (\phi \to \psi)$.

Proof. Follows proof of deduction theorem for L in 1.2.5 by induction on the length of the deduction.

1. Base case is one line deduction. Argue exactly as in 1.2.5. Note that $\vdash_{K_{\mathcal{L}}} (\phi \to \phi)$ by 2.4.4.
2. Inductive step. Suppose ψ follows from earlier formulas in the deduction using MP or Gen. MP is exactly as in 1.2.5. For Gen, suppose ψ is obtained using Gen then ψ is $(\forall x_i)\theta$ and $\Sigma \cup \{\phi\} \vdash \theta$ and x_i is not free in any formula in $\Sigma \cup \{\phi\}$. By induction we have $\Sigma \vdash (\phi \to \theta)$. By K2 $\Sigma \vdash ((\forall x_i)(\phi \to \theta) \to (\phi \to (\forall x_i)\theta))$. By Gen $\Sigma \vdash (\forall x_i)(\phi \to \theta)$ for x_i not free in any formula in Σ. So by MP we get $\Sigma \vdash (\phi \to (\forall x_i)\theta)$ which is $\Sigma \vdash (\phi \to \psi)$.

□

Lecture 15 Monday 05/11/18

2.5 Gödel's completeness theorem

Definition 2.5.1. A set Σ of $\mathcal{L}$-formulas is consistent if there is no formula ϕ with $\Sigma \vdash_{K_{\mathcal{L}}} \phi$ and $\Sigma \vdash_{K_{\mathcal{L}}} (\neg\phi)$.

By Soundness theorem 2.4.5 $\emptyset$ is consistent, so $K_{\mathcal{L}}$ is consistent.

Remark 2.5.2. If Σ is inconsistent then $\Sigma \vdash \chi$ for any $\mathcal{L}$-formula χ.

Recall that a closed $\mathcal{L}$-formula is one without free variables, sometimes called a sentence of $\mathcal{L}$. Show that if Σ is a set of closed $\mathcal{L}$-formulas which is consistent then there is an $\mathcal{L}$-structure $\mathcal{A}$ with $\mathcal{A} \vDash \sigma$ for all $\sigma \in \Sigma$. For a simplification, suppose that $\mathcal{L}$ is countable, that is the variables are $x_0, x_1, \dots$ and there are countably many relation, function, and constant symbols. So we can enumerate the $\mathcal{L}$-formulas, or any subset thereof, as a list indexed by $\mathbb{N}$. Enumerate the closed $\mathcal{L}$-formulas as $\psi_0, \psi_1, \dots$.

Proposition 2.5.3. Suppose Σ is a consistent set of closed $\mathcal{L}$-formulas and ϕ is a closed $\mathcal{L}$-formula.

1. Compare 1.3.6. If $\Sigma \nvdash_{K_{\mathcal{L}}} \phi$ then $\Sigma \cup \{(\neg\phi)\}$ is consistent.
2. Compare Lindenbaum's lemma 1.3.7. There is a consistent set $\Sigma^* \supseteq \Sigma$ of closed $\mathcal{L}$-formulas such that, for every closed $\mathcal{L}$-formula ψ either $\Sigma^* \vdash \psi$ or $\Sigma^* \vdash (\neg\psi)$.

Proof.

1. As in 1.3.6, used deduction theorem and $\vdash_{K_{\mathcal{L}}} (((\neg\phi) \to \phi) \to \phi)$.
2. Uses 1 and the enumeration $\psi_0, \psi_1, \dots$ of the closed $\mathcal{L}$-formulas.

□

Theorem 2.5.4. Suppose Σ is a consistent set of closed $\mathcal{L}$-formulas. Then there is a countable $\mathcal{L}$-structure $\mathcal{A}$ with $\mathcal{A} \vDash \Sigma$, that is $\mathcal{A} \vDash \sigma$ for all $\sigma \in \Sigma$.

Theorem 2.5.5. Let Σ be a set of closed $\mathcal{L}$-formulas and ϕ a closed $\mathcal{L}$-formula. If every model of Σ is a model of ϕ, that is if $\mathcal{A} \vDash \Sigma$ or $\mathcal{A} \vDash \sigma$ for all $\sigma \in \Sigma$ then $\mathcal{A} \vDash \phi$, then $\Sigma \vdash_{K_{\mathcal{L}}} \phi$.

Notation is $\Sigma \vDash \phi$. Then $\Sigma \vDash \phi$ gives $\Sigma \vdash \phi$. The converse is Soundness theorem.

Proof. May assume Σ is consistent, otherwise, everything is a consequence of Σ. By assumption there is no model of $\Sigma \cup \{(\neg\phi)\}$. So by 2.5.4, $\Sigma \cup \{(\neg\phi)\}$ is inconsistent. So by 2.5.3(1), $\Sigma \vdash \phi$. □

Theorem 2.5.6 (Gödel's completeness theorem for $K_{\mathcal{L}}$, 1929)**.** If ϕ is an $\mathcal{L}$-formula with $\vDash \phi$, then ϕ is a theorem of $K_{\mathcal{L}}$, that is $\vdash_{K_{\mathcal{L}}} \phi$.

Proof. If ϕ is closed this follows from 2.5.5 with $\Sigma = \emptyset$. Suppose ϕ has free variables amongst $x_1, \dots, x_n$ and consider the closed formula ψ, $(\forall x_1) \dots (\forall x_n) \phi$. As $\vDash \phi$ we obtain $\vDash \psi$. So by the closed case $\vdash \psi$, that is

$$\vdash (\forall x_1) \dots (\forall x_n) \phi. \tag{6}$$

If θ is any formula then $\vdash ((\forall x_i) \theta \to \theta)$ by the K1 axiom. So from (6) and this fact and MP applied n times we obtain $\vdash_{K_{\mathcal{L}}} \phi$. □

Corollary 2.5.7 (Compactness theorem for $K_{\mathcal{L}}$)**.** Suppose Σ is a set of closed $\mathcal{L}$-formulas and every finite subset of Σ has a model. Then Σ has a model.

Proof. Suppose Σ has no model. By 2.5.4 Σ is inconsistent so there is a formula ϕ with $\Sigma \vdash \phi$ and $\Sigma \vdash (\neg\phi)$. Deductions only involve finitely many formulas in Σ. So there is a finite $\Sigma_0 \subseteq \Sigma$ with $\Sigma_0 \vdash \phi$ and $\Sigma_0 \vdash (\neg\phi)$. But then Σ_0 is inconsistent so has no model, a contradiction. □

Lecture 16
Thursday
08/11/18

Sketch of proof of 2.5.4. Proof is in a series of steps. Notation is cumulative.

1. Let $b_0, b_1, \dots$ be new constant symbols. Form $\mathcal{L}^+$ by adding these to the symbols of $\mathcal{L}$. Regard Σ as a set of $\mathcal{L}^+$-formulas. Check Σ is still consistent in the formal system $K_{\mathcal{L}^+}$. Note that $\mathcal{L}^+$ is still a countable language.

2. Adding witnesses. Use a lemma that there is a consistent set of closed $\mathcal{L}^+$-formulas $\Sigma_\infty \supseteq \Sigma$ such that for every $\mathcal{L}^+$-formula $\theta(x_i)$ with one free variable there is some b_j with

$$\Sigma_\infty \vdash_{K_{\mathcal{L}^+}} ((\neg (\forall x_i) \theta(x_i)) \to (\neg \theta(b_j))).$$

   Think of $\theta(x_i)$ as $(\neg \chi(x_i))$. Then this formula is essentially $((\exists x_i) \chi(x_i) \to \chi(b_j))$, so b_j witnesses the existence of x_i satisfying x_i.

3. By Lindenbaum's lemma 2.5.3 there is a consistent set $\Sigma^* \supseteq \Sigma_\infty$ of closed $\mathcal{L}^+$-formulas such that for every closed ϕ either $\Sigma^* \vdash_{K_{\mathcal{L}^+}} \phi$ or $\Sigma^* \vdash_{K_{\mathcal{L}^+}} (\neg\phi)$.

4. Building a structure. Let $A = \left\{\bar{t}\right\}$ where t is a closed term of $\mathcal{L}^+$. Note that

   (a) a term is closed if it only involves constant symbols and function symbols, and no variables,

   (b) use the $\bar{\cdot}$ to distinguish when we are thinking of a term as an element of A, and

   (c) as $\mathcal{L}^+$ is countable, A is countable.

   Make A into an $\mathcal{L}^+$ structure.

   (a) Each constant symbol c of $\mathcal{L}^+$ is interpreted as $\bar{c} \in A$.

   (b) Suppose R is an n-ary relation symbol. Define the relation $\overline{R} \subseteq A^n$ by $\left(\overline{t_1}, \dots, \overline{t_n}\right) \in \overline{R}$ iff $\Sigma^* \vdash R(t_1, \dots, t_n)$, a closed atomic $\mathcal{L}^+$-formula, where $t_1, \dots, t_n$ are closed $\mathcal{L}^+$-terms.

(c) Suppose f is an m-ary function symbol. Define a function $\overline{f} : A^m \to A$ by $\overline{f}\left(\overline{t_1}, \dots, \overline{t_m}\right) = \overline{f\left(t_1, \dots, t_m\right)}$ for closed terms $t_1, \dots, t_m$.

Call this structure $\mathcal{A}$. Note that if v is a valuation in $\mathcal{A}$ and t is a closed term, then $v(t) = \overline{t}$ by (a) and (c) here.

5. Use the main lemma that for every closed $\mathcal{L}^+$-formula ϕ

$$\Sigma^* \vdash_{K_{\mathcal{L}^+}} \phi \qquad \iff \qquad \mathcal{A} \vDash \phi. \tag{7}$$

Proof by induction on number of connectives and quantifiers in ϕ.

(a) Base case. ϕ is atomic, that is ϕ is $R\left(t_1, \dots, t_n\right)$ for some closed terms t_i, and relation symbol R. (7) holds by (b) in definition of $\mathcal{A}$.

(b) Inductive step. Assume (7) holds for closed formulas involving fewer connectives and quantifiers.

i. ϕ is $(\neg\psi)$.

ii. ϕ is $(\psi \to \chi)$.

iii. ϕ is $(\forall x_i)\,\psi$.

In cases i and ii ψ, χ are closed. So (7) holds for these.

i. ϕ is $(\neg\psi)$, so $\mathcal{A} \vDash \phi$ iff $\mathcal{A} \nvDash \psi$ by 2.3.3, iff $\Sigma^* \nvdash \psi$ by (7), iff $\Sigma^* \vdash (\neg\psi)$ by step 3.

ii. TODO Exercise.

iii. ϕ is $(\forall x_i)\,\psi$.

A. x_i is not free in ψ. So ψ is closed and we can use inductive hypothesis.

B. x_i is free in ψ. So $\psi(x_i)$ has a single free variable.

Suppose for a contradiction that $\mathcal{A} \vDash \phi$ and $\Sigma^* \nvdash \phi$. Then by step 3 $\Sigma^* \vdash (\neg\phi)$. By step 2, $\Sigma^* \vdash ((\neg(\forall x_i)\,\psi(x_i)) \to (\neg\psi(b_j)))$ for some constant symbol b_j, that is $\Sigma^* \vdash ((\neg\phi) \to (\neg\psi(b_j)))$. So $\Sigma^* \vdash (\neg\psi(b_j))$. $(\neg\psi(b_j))$ is closed and by case i, (7) applies. We obtain

$$\mathcal{A} \vDash (\neg\psi(b_j)). \tag{8}$$

This contradicts $\mathcal{A} \vDash (\forall x_i)\,\psi$. Take a valuation v is $\mathcal{A}$ with $v(x_i) = \overline{b_j}$, then v does not satisfy ψ, by (8).

$\square$

TODO Exercise: think about this where Σ consists of the group axioms. What is $\mathcal{A}$? Is it a group?

Lecture 17 Friday 09/11/18

2.6 Equality

Example. In the language of groups, have a binary relation symbol $E(x_1, x_2)$ for equality $x_1 = x_2$.

Definition 2.6.1. Suppose $\mathcal{L}^E$ is a first-order language with a distinguished binary relation symbol E.

1. An $\mathcal{L}^E$-structure in which E is interpreted as equality $=$ is a **normal** $\mathcal{L}^E$-structure.

2. The following are the axioms of equality, Σ_E.

   (a) $(\forall x_1)\,E(x_1, x_2)$.

   (b) $(\forall x_1)(\forall x_2)(E(x_1, x_2) \to E(x_2, x_1))$.

   (c) $(\forall x_1)(\forall x_2)(\forall x_3)(E(x_1, x_2) \to (E(x_2, x_3) \to E(x_1, x_3)))$.

3. For each n-ary relation symbol R of $\mathcal{L}^E$,

$$(\forall x_1)\dots(\forall x_n)(\forall y_1)\dots(\forall y_n)\left(\left(R(x_1, \dots, x_n) \wedge E(x_1, y_1) \wedge \dots \wedge E(x_n, y_n)\right) \to R(y_1, \dots, y_n)\right).$$

4. For each m-ary function symbol f of $\mathcal{L}^E$,

$$(\forall x_1)\dots(\forall x_m)(\forall y_1)\dots(\forall y_m)\left(\left(E\left(x_1,y_1\right)\wedge\dots\wedge E\left(x_m,y_m\right)\right)\to E\left(f\left(x_1,\dots,x_m\right),f\left(y_1,\dots,y_m\right)\right)\right).$$

Definition 2.6.2.

1. If $\mathcal{A}$ is a normal $\mathcal{L}^E$-structure then $\mathcal{A}\vDash\Sigma_E$.
2. Suppose $\mathcal{A}=\left\langle A;\overline{E},\dots\right\rangle$ is an $\mathcal{L}^E$-structure and $\mathcal{A}\vDash\Sigma_E$. Then $\overline{E}$ is an equivalence relation on A. Denote, for $a\in A$ $\widehat{a}=\left\{b\in A\mid\overline{E}\left(a,b\right)\right\}$, the equivalence class of a. Let $\widehat{A}=\{\widehat{a}\mid a\in A\}$. Make $\widehat{A}$ into an $\mathcal{L}^E$-structure $\widehat{\mathcal{A}}$.
   (a) If R is an n-ary relation symbol and $\widehat{a_1},\dots,\widehat{a_n}\in\widehat{A}$ then say $\overline{R}\left(\widehat{a_1},\dots,\widehat{a_n}\right)$ holds in $\widehat{\mathcal{A}}$ iff $\overline{R}\left(a_1,\dots,a_n\right)$ holds in $\mathcal{A}$. This is well-defined by Σ_E.
   (b) Similarly if f is an m-ary function symbol and $\widehat{a_1},\dots,\widehat{a_m}\in\widehat{A}$ let $\overline{f}\left(\widehat{a_1},\dots,\widehat{a_m}\right)=\overline{f}\,(\widehat{a_1,\dots,}a_m)$. This is also well-defined by Σ_E.
   (c) If c is a constant symbol, then interpret c as $\widehat{\overline{c}}$ in $\widehat{A}$, where $\overline{c}$ is the interpretation in $\mathcal{A}$.

   Note that in $\widehat{\mathcal{A}}$ $\overline{E}\left(\widehat{a_1},\widehat{a_2}\right)$ iff $\overline{E}\left(a_1,a_2\right)$ in $\mathcal{A}$, iff $\widehat{a_1}=\widehat{a_2}$. So $\widehat{\mathcal{A}}$ is a normal $\mathcal{L}^E$-structure.

Lemma 2.6.3. Suppose $\mathcal{A}$ is an $\mathcal{L}^E$-structure with $\mathcal{A}\vDash\Sigma_E$. Let v be a valuation in $\mathcal{A}$. Let $\widehat{\mathcal{A}}$ be as given above. Let $\widehat{v}$ be the valuation in $\widehat{\mathcal{A}}$ with $\widehat{v}\left(x_i\right)=\widehat{v\left(x_i\right)}$. Then for every $\mathcal{L}^E$-formula ϕ $\widehat{v}$ satisfies ϕ in $\widehat{\mathcal{A}}$ iff v satisfies ϕ in $\mathcal{A}$. In particular, if ϕ is closed then $\mathcal{A}\vDash\phi$ iff $\widehat{\mathcal{A}}\vDash\phi$.

Note. If t is any term then $\widehat{v}\left(t\right)=\widehat{v\left(t\right)}$ by definition of $\overline{f}$ on the structure $\widehat{\mathcal{A}}$.

Proof. The result 2.6.3 is proved by induction on the number of connectives and quantifiers in ϕ.

1. Base step. ϕ is an atomic formula $R\left(t_1,\dots,t_n\right)$, where R is an n-ary relation symbol and $t_1,\dots,t_n$ are terms. Then $v\left[\phi\right]=T$ iff $\overline{R}\left(v\left(t_1\right),\dots,v\left(t_n\right)\right)$ holds in $\mathcal{A}$, iff $\overline{R}\left(\widehat{v\left(t_1\right)},\dots,\widehat{v\left(t_n\right)}\right)$ holds in $\mathcal{A}$ by definition of $\overline{R}$ in $\widehat{\mathcal{A}}$, iff $\overline{R}\left(\widehat{v}\left(t_1\right),\dots,\widehat{v}\left(t_n\right)\right)$ in $\mathcal{A}$, iff $\widehat{v}\left[\phi\right]=T$, as required.
2. Inductive step.
   (a) ϕ is $(\neg\psi)$. (TODO Exercise)
   (b) ϕ is $(\theta\to\chi)$ (TODO Exercise)
   (c) ϕ is $\left(\forall x_i\right)\psi$.
   $\Longrightarrow$ If $v\left[\left(\forall x_i\right)\psi\right]=F$ there is a v' x_i-equivalent to v with $v'\left[\psi\right]=F$. Then $\widehat{v'}$ is x_i-equivalent to $\widehat{v}$ and by the induction hypothesis $\widehat{v'}\left[\psi\right]=F$. So $\widehat{v}\left[\left(\forall x_i\right)\psi\right]=F$.
   $\Longleftarrow$ Suppose $\widehat{v}\left[\left(\forall x_i\right)\psi\right]=F$. So there is a valuation w in $\widehat{\mathcal{A}}$ which is x_i-equivalent to $\widehat{v}$ and $w\left[\psi\right]=F$. There is a valuation v' in $\mathcal{A}$ x_i-equivalent to v with $\widehat{v'}=w$. We just change $v\left(x_i\right)$ so $\widehat{v'\left(x_i\right)}=w\left(x_i\right)$. Then $v'\left[\psi\right]=F$ by inductive hypothesis. So $v\left[\left(\forall x_i\right)\psi\right]=F$.

∎

Lemma 2.6.4. Suppose Δ is a set of closed $\mathcal{L}^E$-formulas. Then Δ has a normal model, that is a normal $\mathcal{L}^E$-structure $\mathcal{B}$ with $\mathcal{B}\vDash\sigma$ for all $\sigma\in\Delta$, iff $\Delta\cup\Sigma_E$ has a model.

Proof.

$\Longrightarrow$ Trivial as Σ_E holds in a normal $\mathcal{L}^E$-structure.

$\Longleftarrow$ If $\mathcal{A}\vDash\Delta\cup\Sigma_E$ then by 2.6.3 $\widehat{\mathcal{A}}\vDash\Delta$ and $\widehat{\mathcal{A}}$ is a normal $\mathcal{L}^E$-structure.

∎

Theorem 2.6.5 (Compactness theorem for normal models)**.** Suppose $\mathcal{L}^E$ is a countable language with equality and Δ is a set of closed $\mathcal{L}^E$-formulas such that every finite subset of Δ has a normal model. Then Δ has a normal model.

Proof. Every normal $\mathcal{L}^E$-structure is a model of Σ_E, so every finite subset of $\Delta \cup \Sigma_E$ has a model. By 2.5.7 $\Delta \cup \Sigma_E$ has a model $\mathcal{A}$. Then by 2.6.3 or 2.6.4 $\widehat{\mathcal{A}}$ is a normal model of Δ. $\square$

From now on, write $\mathcal{L}^=$ instead of $\mathcal{L}^E$ and $x_1 = x_2$ instead of $E(x_1, x_2)$ etc. Lecture 18 Monday 12/11/18

Theorem 2.6.6 (Countable downward Löwenheim-Skolem theorem)**.** Suppose $\mathcal{L}^=$ is a countable first-order language with equality, and $\mathcal{B}$ a normal $\mathcal{L}^=$ structure. Then there is a countable normal $\mathcal{L}^=$-structure $\mathcal{A}$ such that for every closed $\mathcal{L}^=$-formula ϕ $\mathcal{B} \vDash \phi$ iff $\mathcal{A} \vDash \phi$.

Example. $\mathcal{B} = \langle \mathbb{R}; +, \cdot, 0, 1, \leq, \exp \rangle$ has $\mathcal{A} = ?$.

Proof. Let Σ be the closed ϕ such that $\mathcal{B} \vDash \phi$, called the **theory** of $\mathcal{B}$. Then $\Sigma \supseteq \Sigma_E$ with the axioms of equality, and Σ is consistent. By 2.5.4 Σ has a countable model $\mathcal{C}$. Then $\widehat{\mathcal{C}}$ is a countable normal model of Σ by 2.6.3. So if ϕ is closed and $\mathcal{B} \vDash \phi$ then $\widehat{\mathcal{C}} \vDash \phi$. Conversely if ϕ is closed and $\mathcal{B} \nvDash \phi$ then $\mathcal{B} \vDash (\neg\phi)$ by 2.3.3, so $\widehat{\mathcal{C}} \vDash (\neg\phi)$ so $\widehat{\mathcal{C}} \nvDash \phi$. Take $\mathcal{A} = \widehat{\mathcal{C}}$. $\square$

2.7 Examples and applications

Let $\mathcal{L}^=$ be a first-order language with equality and a binary relation symbol $\leq$.

Definition 2.7.1. A **linear order** or **loset** $\mathcal{A} = \langle A; \leq_A \rangle$ is a normal model of

1. ϕ_1, $(\forall x_1)(\forall x_2)(((x_1 \leq x_2) \wedge (x_2 \leq x_1)) \leftrightarrow (x_1 = x_2))$,
2. ϕ_2, $(\forall x_1)(\forall x_2)(\forall x_3)(((x_1 \leq x_2) \wedge (x_2 \leq x_3)) \rightarrow (x_1 \leq x_3))$, and
3. ϕ_3, $(\forall x_1)(\forall x_2)((x_1 \leq x_2) \vee (x_2 \leq x_1))$.

It is **dense** if also

4. ϕ_4, $(\forall x_1)(\forall x_2)(\exists x_3)((x_1 < x_2) \rightarrow ((x_1 < x_3) \wedge (x_3 < x_2)))$,

where $(x_1 < x_2)$ is an abbreviation for $((x_1 \leq x_2) \wedge (x_1 \neq x_2))$. It is **without endpoints** if

5. ϕ_5, $(\forall x_1)(\exists x_2)(x_1 < x_2)$, and
6. ϕ_6, $(\forall x_1)(\exists x_2)(x_2 < x_1)$.

Let $\Delta = \{\phi_1, \ldots, \phi_6\}$. $\mathcal{Q} = \langle \mathbb{Q}; \leq \rangle$ is a normal model of Δ. $\mathcal{R} = \langle \mathbb{R}; \leq \rangle$ is also a model of Δ.

Will prove the following.

Theorem 2.7.2.

1. For every closed $\mathcal{L}^=$-formula ϕ $\mathcal{Q} \vDash \phi$ iff $\mathcal{R} \vDash \phi$.
2. There is an algorithm to decide, given a closed $\mathcal{L}^=$-formula ϕ, whether $\mathcal{Q} \vDash \phi$ or $\mathcal{Q} \vDash (\neg\phi)$.

Definition 2.7.3.

1. Losets $\mathcal{A} = \langle A; \leq_A \rangle$ and $\mathcal{B} = \langle B; \leq_B \rangle$ are **isomorphic** if there is a bijection $\alpha : A \to B$ such that for all $a, a' \in A$ $a \leq_A a'$ iff $\alpha(a) \leq_B \alpha(a')$.
2. If $\mathcal{A}, \mathcal{B}$ are isomorphic and ϕ is closed then $\mathcal{A} \vDash \phi$ iff $\mathcal{B} \vDash \phi$.

Theorem 2.7.4 (Cantor)**.** If $\mathcal{A}, \mathcal{B}$ are countable dense losets without endpoints, then $\mathcal{A}, \mathcal{B}$ are isomorphic.

Lemma 2.7.5 (Los-Vaught test)**.** Let $\Sigma = \Sigma_E \cup \Delta$. Then for every closed $\mathcal{L}^=$-formula ϕ, we have either $\Sigma \vdash \phi$ or $\Sigma \vdash (\neg\phi)$. Say Σ is complete.

Proof. Suppose not. Then as Σ is consistent, it has a model, we can use 2.5.3 to get $\Sigma_1 = \Sigma \cup \{(\neg\phi)\}$ and $\Sigma_2 = \Sigma \cup \{(\neg(\neg\phi))\}$ are consistent. So $\Sigma \cup \{\phi\}$ is consistent. By 2.5.4, 2.6.4 it follows that Σ_1, Σ_2 have countable normal models $\mathcal{A}_1, \mathcal{A}_2$. So $\mathcal{A}_1, \mathcal{A}_2$ are countable dense l without endpoints and $\mathcal{A}_1 \vDash (\neg\phi)$ and $\mathcal{A}_2 \vDash \phi$. This contradicts 2.7.4 and 2.7.3(2). $\square$

Proof of 2.7.2(1). Show $\mathcal{Q} \vDash \phi$ iff $\Sigma \vdash \phi$.

$\Longleftarrow$ As $\mathcal{Q} \vDash \Sigma$ this is 2.4.5.

$\Longrightarrow$ If $\Sigma \nvdash \phi$ then by 2.7.5 $\Sigma \vdash (\neg\phi)$. So $\mathcal{Q} \vDash (\neg\phi)$, so $\mathcal{Q} \nvDash \phi$.

Similarly $\mathcal{R} \vDash \phi$ iff $\Sigma \vdash \phi$. So $\mathcal{R} \vDash \phi$ iff $\Sigma \vdash \phi$, iff $\mathcal{Q} \vDash \phi$. $\square$

Lecture 19 Thursday 15/11/18

Lecture 19 is a problem class.

Lecture 20 Friday 16/11/18

Want an algorithm which decides, given closed θ, whether $\langle \mathbb{Q}; \leq \rangle \vDash \theta$ or $\langle \mathbb{Q}; \leq \rangle \nvDash \theta$, that is $\langle \mathbb{Q}; \leq \rangle \vDash (\neg\theta)$, by 2.3.3. Σ is a **recursively enumerable** set of formulas, that is we can write an algorithm to systematically generate the formulas in Σ. Note that the set of axioms for $K_{\mathcal{L}}$ is also recursively enumerable. So the set of deductions from Σ is recursively enumerable. Therefore the set of consequences of Σ is recursively enumerable. Method is to run the algorithm which generates all consequences of Σ. By 2.7.2(1) at some point, we will see either θ or $(\neg\theta)$. At this point, the method stops.

Note.

1. Depends on
   (a) the Completeness theorem, and
   (b) the axioms Δ for $\langle \mathbb{Q}; \leq \rangle$,
2. Works for some other structures. Can have better algorithms.
3. But there is no such algorithm for $\langle \mathbb{N}; +, \cdot, 0 \rangle$. This is Gödel's incompleteness theorem.

3 Set theory

3.0 Basic set theory

0. Extensionality. Sets A and B are equal iff $(\forall x)\,((x \in A) \leftrightarrow (x \in B))$.
1. Natural numbers $\mathbb{N} = \{0, 1, \ldots\}$. Think of $0 = \emptyset$ and $n + 1 = \{0, \ldots, n\}$. Note that for $m, n \in \mathbb{N}$, $m < n$ iff $m \in n$, iff $m \subsetneq n$.
2. Ordered pairs. The ordered pair (x, y) is the set $\{\{x\}, \{x, y\}\}$. For example, for any x, y, z, w, $(x, y) = (z, w)$ iff $x = z$ and $y = w$. If A, B are sets, then $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$. $A^2 = A \times A$ and $A^{n+1} = A^n \times A$. The set of finite sequences of elements of A is $\cup_{n \in \mathbb{N}} A^n$. $A^0 = \{\emptyset\}$.
3. Functions. Think of a function $f : A \to B$ as a subset of $A \times B$. $A = dom(f)$ is the domain and $B = ran(f)$ is the range. If $X \subseteq A$ $f[X] = \{f(a) \mid a \in X\} \subseteq B$. Set of functions from A to B is $B^A \subseteq \wp(A \times B)$, where $\wp$ is the powerset, that is the set of all subsets.

3.1 Cardinality

Definition 3.1.1. Sets A, B are **equinumerous**, or of the **same cardinality**, if there is a bijection $f : A \to B$. Write $A \approx B$ or $|A| = |B|$.

Definition 3.1.2. A set A is **finite** if it is equinumerous with some element of $\mathbb{N}$. $n = \{0, \ldots, n-1\}$. A set A is **countably infinite** if it is equinumerous with $\mathbb{N}$. **Countable** is finite or countably infinite.

Proposition 3.1.3. The following are basic facts.

1. Every subset of a countable set is countable.
2. A set A is countable iff there is an injective function $f : A \to \mathbb{N}$.
3. If A, B are countable, then $A \times B$ is countable.
4. If $A_0, A_1, \dots$ are countable then $\cup_{i \in \mathbb{N}} A_i$ is countable.

Proof of 4 uses axiom of choice.

Example.

1. $\mathbb{Q}$ is countable.
2. $\cup_{n \in \mathbb{N}} A^n$ is countable if A is countable.
3. $\mathbb{R}$ is not countable by Cantor.

Theorem 3.1.4 (Cantor)**.** If X is any set, then $\wp(X)$ is the set of all subsets of X. There is no surjective function $f : X \to \wp(X)$.

Proof. Suppose there is such an f. Let $Y = \{y \in X \mid y \notin f(y)\}$. There is $z \in X$ with $f(z) = Y$. If $z \in Y$ then $z \notin f(z) = Y$. If $z \notin Y$ then $z \notin f(z)$ so $z \in Y$. Contradiction. □

Lecture 21 Monday 19/11/18

Definition 3.1.5. For sets A, B write $|A| \le |B|$ or $A \le B$ if there is an injective function $f : A \to B$.

Note. $|x| \le |\wp(x)|$ use $x \mapsto \{x\}$. So, as $|x| \ne |\wp(x)|$ by 3.1.4, we have $|x| < |\wp(x)|$.

Example. If $|A| \le |B|$ and $|B| \le |C|$ then $|A| \le |C|$.

Theorem 3.1.6 (Schröder-Bernstein)**.** Suppose A, B are sets and $f : A \to B$ and $g : B \to A$ are injective functions. Then $A \approx B$. That is $|A| \le |B|$ and $|B| \le |A|$ then $|A| = |B|$.

Proof. Let $h = g \circ f : A \to A$. Let $A_0 = A \setminus g[B]$ and for $n > 0$ let $A_n = h[A_{n-1}]$. Let $A^* = \cup_{n \in \mathbb{N}} A_n$ and $B^* = f[A^*]$. Note that $h[A^*] \subseteq A^*$ so $g[B^*] = h[A^*] \subseteq A^*$. Claim that $g[B \setminus B^*] = A \setminus A^*$. Once we have this f gives a bijection $A^* \to B^*$ and g gives a bijection $B \setminus B^* \to A \setminus A^*$. So

$$k(a) = \begin{cases} f(a) & a \in A^* \\ g^{-1}(a) & a \in A \setminus A^* \end{cases}$$

is a bijection.

1. Let $a \in A \setminus A^*$. As $a \notin A_0$ there is $b \in B$ with $g(b) = a$. Then $b \notin B^*$ as $b \in B^* = f[A^*]$ gives $a = g(b) \in h[A^*] \subseteq A^*$, a contradiction, so $g[B \setminus B^*] \supseteq A \setminus A^*$.
2. Let $b \in B$. Suppose $g(b) \in A^*$. Show $b \in B^*$. As $g(b) \notin A_0 = A \setminus g[B]$ we have $g(b) \in A_n$ for some $n > 0$. So $g(b) = h(a)$ for some $a \in A_{n-1}$. So $g(b) = g(f(a))$, so $b = f(a)$ for some $a \in A^*$. Thus $b \in f[A^*] = B^*$.

□

Example. The following sets are equinumerous.

1. $S_1 = \{0,1\}^{\mathbb{N}}$, the set of all sequences of zeroes and ones.
2. $S_2 = \mathbb{R}$.
3. $S_3 = \wp(\mathbb{N})$.
4. $S_4 = \wp(\mathbb{N} \times \mathbb{N})$.
5. $S_5 = \mathbb{N}^{\mathbb{N}}$, the set of all sequences of natural numbers.

Find injective functions $f_{i,j} : S_i \to S_j$ for $i, j \in \{1, \dots, 5\}$. Then use 3.1.6. As $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ we get $S_3 \approx S_4$. Also $S_1 \subseteq S_5 \subseteq S_4$. Have a bijection $f_{3,1} : \wp(\mathbb{N}) \to \{0,1\}^{\mathbb{N}}$. For $X \subseteq \mathbb{N}$ $f_{3,1}(X) = (a_n)_{n\in\mathbb{N}}$ where

$$a_n = \begin{cases} 0 & n \notin X \\ 1 & n \in X \end{cases}.$$

$f_{1,2} : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$ by $(a_n)_{n\in\mathbb{N}} \mapsto 0.a_1a_2\dots$, the decimal expansion, is injective. $f_{2,5} : \mathbb{R} \to \mathbb{N}^{\mathbb{N}}$ by

$$n.m_1m_2 \dots \mapsto \begin{cases} (0, n, m_1, m_2, \dots) & n \geq 0 \\ (1, -n, m_1, m_2, \dots) & n < 0 \end{cases}.$$

The following are questions.

1. If A, B are sets do we have $|A| \leq |B|$ or $|B| \leq |A|$? If we assume axiom of choice, yes.
2. Is there $X \subseteq \mathbb{R}$ with $|\mathbb{N}| < |X| < |\mathbb{R}|$? Continuum hypothesis says no.

3.2 Axioms for set theory

Zermelo-Fraenkel axioms say how we are allowed to build sets. All can be expressed in a first-order language with equality using a single binary relation symbol $\in$. Have to avoid Russell paradox, $S = \{x \mid x \notin x\}$. If this is a set, is $S \in S$? $(\exists S)(\forall x)((x \in S) \leftrightarrow (x \notin x))$ leads to inconsistency.

Axiom 1 (Axiom of extensionality)**.** Two sets are equal iff they have the same elements.

$$(\forall x)(\forall y)((x = y) \leftrightarrow (\forall z)((z \in x) \leftrightarrow (z \in y))).$$

Axiom 2 (Empty set axiom)**.**

$$(\exists x)(\forall y)(y \notin x).$$

There is a unique set x with this property, $\emptyset$.

Lecture 22 Thursday 22/11/18

Axiom 3 (Pairing axiom)**.** Given sets x, y then we can form $z = \{x, y\}$.

$$(\forall x)(\forall y)(\exists z)(\forall w)((w \in z) \leftrightarrow ((w = x) \vee (w = y))).$$

Note.

1. Use twice to form $(x, y) = \{\{x\}, \{x, y\}\}$.
2. Use to produce $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{0, 1\}$.

Axiom 4 (Union axiom)**.** For any set A there is a set $B = \cup A$.

$$(\forall A)(\exists B)(\forall x)((x \in B) \leftrightarrow (\exists z)((z \in A) \wedge (x \in z))).$$

So $B = \cup\{z \mid z \in A\}$. If $A = \{x, y\}$ then $B = x \cup y$.

Example. $3 = \{0, 1, 2\} = \{0, 1\} \cup \{2\}$.

Axiom 5 (Power set axiom)**.** For any set A, there is a set $\wp(A)$ whose elements are the subsets of A.

$$(\forall A)(\exists B)(\forall z)((z \in B) \leftrightarrow (z \subseteq A)).$$

$(z \subseteq A)$ means $(\forall y)((y \in z) \to (y \in A))$.

Axiom 6 (Axiom scheme of specification)**.** Suppose $P(x, y_1, \dots, y_r)$ is a formula in our language. Then we have an axiom

$$(\forall A)(\forall y_1)\dots(\forall y_r)(\exists B)(\forall x)((x \in B) \leftrightarrow ((x \in A) \wedge P(x, y_1, \dots, y_r))).$$

So this guarantees we can form the subset of A, $B = \{x \in A \mid P(x, y_1, \dots, y_r)\}$, for all given sets $A, y_1, \dots, y_r$.

Example.

1. Let C be any non-empty set and $A \in C$. Then $\cap C = \{x \in A \mid P(x, C) = (\forall z)((z \in C) \to (x \in z))\}$.
2. $A \times B = \{w \in \wp(\wp(A \cup B)) \mid (\exists a)(\exists b)((a \in A) \wedge (b \in A) \wedge (w = \{\{a\}, \{a, b\}\}))\}$.

Definition 3.2.1. For a set a the **successor** of a is $a^\dagger = a \cup \{a\}$. A set A is **inductive** if

$$\left((\emptyset \in A) \wedge (\forall x)\left((x \in A) \to \left(x^\dagger \in A\right)\right)\right).$$

Example. $2 = \{0, 1\} = \{0\} \cup \{1\} = 1^\dagger$.

Axiom 7 (Axiom of infinity)**.**

$$(\exists A)\left((\emptyset \in A) \wedge (\forall x)\left((x \in A) \to \left(x^\dagger \in A\right)\right)\right).$$

Definition 3.2.2. Let A be an inductive set. We can form using specification the set

$$\mathbb{N} = \{x \in A \mid \text{if } B \text{ is an inductive set, then } x \in B\}.$$

Informally, this is the intersection of all inductive sets. This does not depend on the choice of A. Also denote this by ω.

Theorem 3.2.3.

1. $\mathbb{N}$ is an inductive set, and if B is an inductive set, then $\mathbb{N} \subseteq B$.
2. Proof by induction works. Suppose $P(x)$ is a property of sets, that is a formula, such that
   (a) $P(\emptyset)$ holds, and
   (b) for every $k \in \mathbb{N}$, if $P(k)$ holds, then $P\left(k^\dagger\right)$ holds.

   Then $P(n)$ holds for all $n \in \mathbb{N}$.

Proof.

1. TODO Exercise: use definition.
2. Consider $B \subseteq \mathbb{N}$ given by $B = \{x \in \mathbb{N} \mid P(x)\}$. (a), (b) say that B is an inductive set. So by 1, $\mathbb{N} \subseteq B$. Thus $\mathbb{N} = B$.

$\square$

Could develop arithmetic in $\mathbb{N}$, using $n^\dagger$ as $n + 1$, etc, and in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ in the usual way using Zermelo-Fraenkel 1 to 7. (TODO Exercise: hard, for $m, n \in \mathbb{N}$ write $m \le n$ to mean $((m = n) \vee (m \in n))$, then this is a well-ordering on $\mathbb{N}$)

3.3 Well orderings

Definition 3.3.1. A loset $\langle A; \le \rangle$ is a **well-ordering** or a **woset** if every non-empty subset of A has a least element.

$$(\forall X)(((X \subseteq A) \wedge (X \ne \emptyset)) \to (\exists x)((x \in X) \wedge (\forall y)((y \in X) \to (x \in y)))).$$

Example. $\langle \mathbb{Z}; \le \rangle$ is not a woset. $\langle \mathbb{N}; \le \rangle$ is a woset.

Suppose $\mathcal{A}_1 = \langle A_1; \le_1 \rangle$ and $\mathcal{A}_2 = \langle A_2; \le_2 \rangle$ are losets.

Lecture 23 Friday 23/11/18

Definition 3.3.2. Say $\mathcal{A}_1, \mathcal{A}_2$ are **similar** or isomorphic if there is a bijection $\alpha : A_1 \to A_2$ with for all $a, b \in A_1$ $a <_1 b$ iff $\alpha(a) <_2 \alpha(b)$. Write $\mathcal{A}_1 \simeq \mathcal{A}_2$. Say α is a **similarity**. If $a <_1 b$ gives $\alpha(a) <_2 \alpha(b)$ say α is **order-preserving**.

Definition 3.3.3.

1. **Reverse-lexicographic product** $\mathcal{A}_1 \times \mathcal{A}_2 = \langle A_1 \times A_2; \leq \rangle$. $(a_1, a_2) \leq (a_1', a_2')$ iff $a_2 <_2 a_2'$ or $((a_2 = a_2')$ and $(a_1 \leq_1 a_1'))$. In $\mathcal{A}_2$ replace each element by a copy of $\mathcal{A}_1$.

2. **Sum**. Regard A_1, A_2 as disjoint, by replacing them by similar orderings on disjoint sets, such as $\{(a, 0) : a \in A_1\}$ and $\{(b, 1) \mid b \in A_2\}$, and define $\mathcal{A}_1 + \mathcal{A}_2 = \langle A_1 \cup A_2; \leq \rangle$ where $\leq$ is the union of $\leq_1, \leq_2$ and $a_1 \leq a_2$ for $a_1 \in A_1$ and $a_2 \in A_2$.

Example.

1. $\mathbb{N} + \mathbb{N}$.
$$\begin{array}{ccccccccc} \mathbb{N} & & & 0 & 1 & \dots & & & \\ & & \mathbb{N} & & & & 0 & 1 & \dots \\ \mathbb{N} & + & \mathbb{N} & 0 & 1 & \dots & 0 & 1 & \dots \end{array}.$$

2. $\{0, 1\} \times \mathbb{N}$.
$$\begin{array}{cccccccccc} & & \mathbb{N} & & 0 & & 1 & & \dots & \\ \{0,1\} & \times & \mathbb{N} & 0 & & 1 \quad 0 & & 1 & \dots & \dots \end{array}.$$
Thus $\{0, 1\} \times \mathbb{N} \simeq \mathbb{N}$.

3. $\mathbb{N} \times \{0, 1\}$.
$$\begin{array}{ccccccccc} \{0,1\} & & & & 0 & & & 1 & \\ \{0,1\} & \times & \mathbb{N} & 0 & 1 & \dots & 0 & 1 & \dots \end{array}.$$
Thus $\mathbb{N} \times \{0, 1\} \simeq \mathbb{N} + \mathbb{N}$.

Lemma 3.3.4.

1. $\mathcal{A}_1 + \mathcal{A}_2$, $\mathcal{A}_1 \times \mathcal{A}_2$ are losets.

2. If $\mathcal{A}_1, \mathcal{A}_2$ are wosets then so are $\mathcal{A}_1 + \mathcal{A}_2$ and $\mathcal{A}_1 \times \mathcal{A}_2$.

Proof. (TODO Exercise: complete proof) $\mathcal{A}_1 \times \mathcal{A}_2$ is a woset. Let $\emptyset \neq X \subsetneq A_1 \times A_2$. Let $Y = \{b \in A_2 \mid \exists a \in A_1,\ (a, b) \in X\} \subseteq A_2$. Let y be the least element of Y. Let $Z = \{z \in A_1 \mid (z, y) \in X\}$. This has a least element x. Then (x, y) is the least element of X. □

Definition 3.3.5. Suppose $\mathcal{A} = \langle A; \leq \rangle$ is a loset. A subset $X \subseteq A$ is an **initial segment** of A if for all $x \in X$, for all $a \in A$, if $a < x$, then $a \in X$. It is **proper** if $X \neq A$.

Example. Let $b \in A$.

1. $A[b] = \{x \in A \mid x < b\}$ is a proper initial segment.

2. $A[\leq b] = \{x \in A \mid x \leq b\}$ is an initial segment.

Lemma 3.3.6. If $\mathcal{A} = \langle A; \leq \rangle$ is a woset, then every proper initial segment X is of the form $A[b]$ for some $b \in A$.

Note. Not true for losets in general.

Example. $\{x \in \mathbb{Q} \mid x < \pi\} \subseteq \mathbb{Q}$ is not of the form $\mathbb{Q}[b]$ for some $b \in \mathbb{Q}$.

Proof. Let b be the minimal element of $A \setminus X$. □

Theorem 3.3.7. Suppose $\mathcal{A}_1 = \langle A_1; \leq_1 \rangle$ and $\mathcal{A}_2 = \langle A_2; \leq_2 \rangle$ are wosets. Then exactly one of the following holds.

1. $\mathcal{A}_1, \mathcal{A}_2$ are similar,

2. $\mathcal{A}_1$ is similar to a proper initial segment of $\mathcal{A}_2$, or

3. $\mathcal{A}_2$ is similar to a proper initial segment of $\mathcal{A}_1$.

In each case the similarity is unique.

Proof. For uniqueness, suppose we have order preserving $\alpha, \beta : A_1 \to A_2$ whose images are initial segments of A_2. Show $\alpha = \beta$.

1. Check that if $b \in A_1$ then $\alpha(A_1[b]) = A_2[\alpha(b)]$.
2. If $\alpha \neq \beta$ take $b \in A_1$ minimal with $\alpha(b) \neq \beta(b)$, so $\alpha(A_1[b]) = \beta(A_1[b])$. By step 1 $A_2[\alpha(b)] = A_2[\beta(b)]$. Conclude that $\alpha(b) = \beta(b)$, a contradiction.

This shows

1. by taking $A_1 = A_2$ and α the identity obtain that A_1 is not similar to a proper initial segment of itself, and
2. it follows that we cannot have two of 1, 2, 3 holding.

For existence, suppose A_2 is not similar to an initial segment of A_1. Show A_1 is similar to a proper initial segment of A_2. Look at C, where C is the $c \in A_1$ such that there is a similarity between $A_1[\leq c]$ and an initial segment of A_2. If $c \in C$ there is a unique $\alpha_c : A_1[\leq c] \to A_2$ with image an initial segment, by uniqueness part. Note that

1. C is an initial segment of A_1,
2. if $c_1 < c_2 \in C$ then α_{c_1} is the restriction of α_{c_2} to $A_1[\leq c_1]$, and
3. let $\alpha = \cup \{\alpha_c \mid c \in C\}$, then α is a similarity between C and an initial segment of A_2.

If $C = A_1$, done. Suppose $C \neq A_1$. Let a be the minimal element of $A_1 \setminus C$. $\alpha(C) \neq A_2$ otherwise A_2 is similar to C so 3 holds. So $\alpha(C) = A_2[b]$ for some $b \in A_2$. Can extend α by sending a to b and get $A_1[\leq a] \simeq A_2[\leq b]$. Thus $a \in C$, a contradiction. $\square$

Lecture 24 Monday 26/11/18

Note. In the notation of 3.3.7, we have, in particular, an injective function $A_1 \to A_2$ for cases 1 and 2 or an injective function $A_2 \to A_1$. So either $|A_1| \leq |A_2|$ or $|A_2| \leq |A_1|$.

Axiom of choice gives any set A can be well-ordered. Putting this together with 3.3.7 gives for any sets A_1, A_2 $|A_1| \leq |A_2|$ or $|A_2| \leq |A_1|$.

3.4 Ordinals

We now define some very particular wosets which generalise the natural numbers,

$$0 = \emptyset, \qquad 1 = 0^\dagger = \{\emptyset\}, \qquad 2 = 1^\dagger = \{0, 1\}, \qquad 3 = 2^\dagger = \{0, 1, 2\}, \qquad \dots.$$

to the transfinite. For $m, n \in \omega$ $m < n$ iff $m \in n$.

Definition 3.4.1.

1. A set X is a **transitive set** if every element of X is also a subset of X, that is if $y \in x \in X$ then $y \in X$.
2. A set α is an **ordinal** if
   (a) α is a transitive set, and
   (b) the relation $<$ on α given by, for $x, y \in \alpha$,
   $$x < y \qquad \iff \qquad x \in y$$
   is a strict well-ordering on α.

Note. As part of the definition, we have $\alpha \notin \alpha$ for an ordinal α.

It is standard to use lower case Greek letters for ordinals. The ordering on an ordinal α is sometimes denoted by $\in_\alpha$.

Lemma 3.4.2. If α is an ordinal, then so is $\alpha^\dagger = \alpha \cup \{\alpha\}$.

Proof. As α is a transitive set, then so is $\alpha^\dagger = \alpha \cup \{\alpha\}$. Moreover, the ordering $\in$ restricted to $\alpha^\dagger$ is an ordering. We have the ordering on α with the extra element α added on the end as the greatest element. This is a well-ordering, as the ordering on α is a well-ordering. □

We also denote the ordinal $\alpha^\dagger$ by $\alpha+1$. It is of course similar to the ordered set $\alpha+1$ as defined previously.

Corollary 3.4.3. If $n \in \omega$, then n is an ordinal.

Proof. As $\emptyset$ is an ordinal, this follows by induction 3.2.3 using 3.4.2 above. □

Proposition 3.4.4.

1. If α is an ordinal then $\alpha \notin \alpha$.
2. If α is an ordinal and $\beta \in \alpha$ then β is an ordinal.
3. If α, β are ordinals and $\alpha \subsetneq \beta$ then $\alpha \in \beta$.
4. If α is an ordinal then α is the set of β such that β is an ordinal and $\beta \in \alpha$.

Proof.

1. Otherwise α has an element $x = \alpha$ with $x \in x$. But in terms of the ordering on α this says $x < x$, which is impossible.
2. First show β is a transitive set. So let $x \in \beta$ and $y \in x$. We want $y \in \beta$. But we have $y \in x \in \beta \in \alpha$. Using twice that α is a transitive set we get that $x, y \in \alpha$. So as the restriction of $\in$ to α is an ordering we get $y \in \beta$. As α is a transitive set $\in_\beta$ is simply the restriction of $\in_\alpha$ to β, so this is a well-ordering.
3. Note that as $\alpha \subsetneq \beta$, $\beta \setminus \alpha$ is non-empty, so has a least element γ, under $\in_\beta$. We aim to show that $\alpha = \gamma$. Think about α and β as natural numbers to see why this is plausible. If $x \in \gamma$ then $x \in \beta$, so $x \in \alpha$, as γ is the least element of $\beta \setminus \alpha$. Thus $\gamma \subseteq \alpha$. Conversely suppose there is some $y \in \alpha \setminus \gamma$. Then, as $\in$ is an ordering on β and $y \notin \gamma$, either $y = \gamma$ or $\gamma \in y$. But in either case we get $\gamma \in \alpha$ as α is a transitive set. A contradiction. So $\alpha \subseteq \gamma$.
4. Trivial, by 2.

□

Definition 3.4.5. If α, β are ordinals we write $\alpha < \beta$ to indicate that $\alpha \in \beta$, and $\alpha \leq \beta$ has the obvious meaning.

Note. By 3.4.4 above $\alpha \leq \beta$ iff $\alpha \subseteq \beta$.

The following theorems can be paraphrased informally as saying that the class of all ordinals is well-ordered by $\leq$.

Theorem 3.4.6. Suppose α, β, γ are ordinals.

1. If $\alpha < \beta$ and $\beta < \gamma$ then $\alpha < \gamma$.
2. If $\alpha \leq \beta$ and $\beta \leq \alpha$ then $\alpha = \beta$.
3. Exactly one of $\alpha < \beta$, $\alpha = \beta$, $\beta < \alpha$ holds.
4. If X is a non-empty set of ordinals, then X has a least element δ, and moreover, $\delta = \cap X$.

Proof.

1. If $\alpha \in \beta \in \gamma$ then $\alpha \in \gamma$ as γ is a transitive set.
2. Otherwise we have $\alpha \in \beta$ and $\beta \in \gamma$ whence $\alpha \in \alpha$, contradicting 3.4.4.
3. Certainly we already know that no more than one of these holds. Consider $\alpha \cap \beta$. This is also an ordinal by 4. (TODO Exercise) Show that if $\alpha \neq \beta$ then $\alpha \subsetneq \beta$ or $\beta \subsetneq \alpha$. If, for example $\alpha \cap \beta = \alpha$ then $\alpha \subseteq \beta$ and so $\alpha \leq \beta$. So for a contradiction, suppose $\alpha \cap \beta$ is a proper subset of both α and β. Thus, by 3.4.4(3), $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$. So $\alpha \cap \beta \in \alpha \cap \beta$, a contradiction, all using $\alpha \cap \beta$ is an ordinal.
4. Let $\alpha \in X$ be any element and consider $\alpha \cap X$. So this is the set of elements of X which are less than α. If this is empty then α is the least element of X. Otherwise, it is a non-empty subset of α so has a least element β. It is then obvious that β is the least element of X. If δ is the least element of X, then $\delta \subseteq \eta$ for all $\eta \in X$. It follows that $\delta = \cap X$.

□

Corollary 3.4.7.

1. If X is a non-empty set of ordinals, then $\cup X$ is an ordinal.
2. ω is an ordinal.

Proof.

1. By 3.4.6, X is well-ordered by $\in$. So it is enough to show that $\cup X$ is a transitive set. If $y \in z \in \cup X$, there is $x \in X$ with $z \in x$. So $y \in z \in x$ and therefore $y \in x$. So $y \in \cup X$, as required.
2. Check that $\cup \omega = \omega$, and use 1.

□

So we can now form ordinals

$$\omega^{\dagger} = \{0, 1, \dots, \omega\}, \qquad \left(\omega^{\dagger}\right)^{\dagger} = \left\{0, 1, \dots, \omega, \omega^{+}\right\}, \qquad \dots .$$

Just as the natural numbers provided us with canonical examples of finite sets, we will now show that ordinals do the same thing for all wosets.

Theorem 3.4.8. If $\langle A; \leq \rangle$ is a woset, then there is a unique ordinal α which is similar to $\langle A; \leq \rangle$.

Proof. For uniqueness, suppose $\langle A; \leq \rangle$ is similar to ordinals α, β. Then α and β are similar. Without loss of generality, may assume $\alpha \leq \beta$, so if $\alpha \neq \beta$ we have that $\alpha < \beta$. α is therefore a proper initial segment of β, and so β is similar to a proper initial segment of itself, which contradicts 3.3.7. This establishes the uniqueness part of the statement. Now for existence, we show that there is some ordinal similar to A. Let

$$X = \{x \in A \mid \text{the initial segment } A[x] \text{ is similar to an ordinal}\}.$$

Note that if $A \neq \emptyset$, then the least element of A is in X. Note that by uniqueness, if $x \in X$ then $A[x]$ is similar to a unique ordinal α_x. Let

$$S = \{\alpha_x \mid x \in X\}.$$

So S is a set of ordinals. In fact, S is an ordinal. To see this note that we need to only show that it is a transitive set, that is if $\beta \in \alpha_x \in S$ then $\beta \in S$. Let $\alpha_x \in S$ and let $\pi : A[x] \to \alpha_x$ be a similarity. If $\beta \in \alpha_x$ let $y = \pi^{-1}(\beta)$. Then the restriction of π to $A[y]$ gives a similarity $A[y] \to \{\delta \in \alpha_x \mid \delta < \beta\} = \beta$. So $\beta = \alpha_y \in S$. So now write α instead of S. By what we already did, this argument also shows that X is an initial segment of A. If we knew that $A = X$, then we would be done as the function $X \to \alpha$ given by $x \mapsto \alpha_x$ is easily seen to be a similarity $A \to \alpha$. So suppose that $X \neq A$, so X is a proper initial segment of A. By 3.3.6 we have that $X = A[z]$ for some $z \in A \setminus X$. Know that $x \mapsto \alpha_x$ gives a similarity $X \to \alpha$. But then $z \in X = A[z]$, by definition of X, a contradiction. So $X = A$ and $A \simeq \alpha$. □

There is a problem with this proof. Why is S a set? No combination of the axioms we have given so far actually justifies the existence of such a set. There is no alternative but to assume another axiom about how we are allowed to create new sets from old ones. Lecture 25 Thursday 29/11/18

Definition 3.4.9. Suppose $F(x, y, z_1, \dots, z_r)$ is a property of sets, expressible in our first-order language such that, whenever $s_1, \dots, s_r$ are sets, for every set b there is a unique set a where $F(a, b, s_1, \dots, s_r)$ holds. F is called an **operation** on sets, with $z_1, \dots, z_r$ being **parameter variables**, and the $s_1, \dots, s_r$ are referred to as the **parameters** of the operation, and $F(x, y, s_1, \dots, s_r)$ gives us a function on sets $b \mapsto a$.

Example. $F(a, b)$ says a is the power set of b has no parameter variables. $F(a, b, c)$ says a is the set of functions from b to c has a parameter c.

Axiom 8 (Axiom of replacement)**.** Suppose $F(x, y, z_1, \dots, z_r)$ is an operation on sets as above and $s_1, \dots, s_r$ are sets and B is a set. Then there is a set A such that

$$A = \{a \mid \exists b \in B,\ F(a, b, s_1, \dots, s_r)\}.$$

So here the set A is obtained from B by replacing each $b \in B$ by the corresponding set a for which $F(a, b, s_1, \dots, s_r)$ holds. If we allow ourselves this axiom then the set S in the above proof of 3.4.8 is justified. Obtain S from X using the operation $F(a, b)$ to say either b is a woset similar to the ordinal a, or b is not a woset and $a = \emptyset$. Then apply this to $B = \{A[x] \mid x \in X\}$ to get $S = \{x \mid \exists y \in X,\ F(x, A[y])\}$.

3.5 Transfinite induction

Theorem 3.5.1 (Transfinite induction)**.** Suppose $P(x)$ is a property of sets. Assume that for all ordinals α, if $P(\beta)$ holds for all ordinals $\beta < \alpha$, then $P(\alpha)$ holds. Then $P(\gamma)$ holds for all ordinals γ.

Proof. Note that if $\alpha = 0 = \emptyset$ then $P(\beta)$ holds for all $\beta < \alpha$, vacuously. So by assumption $P(0)$ holds. Suppose for a contradiction that there is some ordinal γ such that $P(\gamma)$ does not hold. There is a least such γ, call it α, by applying 3.4.6(4) to $\{\beta \mid \beta \le \gamma,\ \neg P(\beta)\}$. Thus, for an ordinal $\beta < \alpha$, $P(\beta)$ holds. By assumption, $P(\alpha)$ holds, a contradiction. □

Theorem 3.5.2. Suppose α is an infinite ordinal, that is $\omega \le \alpha$. Then $\alpha \approx \alpha \times \alpha$.

Corollary 3.5.3.

1. If $\langle A; \le \rangle$ is an infinite woset then $|A| = |A \times A|$.
2. Assuming axiom of choice, if A is any infinite set then $|A| = |A \times A|$.

Proof.

1. By 3.4.8, there is an ordinal α with $\alpha \approx A$. So $|A| = |A \times A|$ follows from 3.5.2.
2. By axiom of choice, A can be well-ordered, so 2 follows from 1.

□

2 is called the **fundamental theorem of cardinal arithmetic**. Lecture 26 Friday 30/11/18

Proof of Theorem 3.5.2. Assume if $\omega \ne \beta < \alpha$ then $\beta \approx \beta \times \beta$, by transfinite induction hypothesis, and deduce $\alpha \approx \alpha \times \alpha$. May assume if $\beta < \alpha$ then $|\beta| < |\alpha|$. Implies $\left|\beta^\dagger\right| < |\alpha|$. Enough to show $|\alpha \times \alpha| \le |\alpha|$, by 3.1.6.

1. Prove that suppose we have a well-ordering $\le$ of $A = \alpha \times \alpha$ such that for all $x \in A$ $|A[x]| = \{y \in A \mid y \le x\} < |\alpha|$, then $|\alpha \times \alpha| = |\alpha|$. By 3.4.6 there is an ordinal γ which is similar to $\langle A; \le \rangle$. Let $f : \gamma \to A$ be the similarity. Show $\gamma \subseteq \alpha$, so $|\gamma| \le |\alpha|$, so $|A| \le |\alpha|$. Let $\eta \in \gamma$, so $\eta < \gamma$. As f is a similarity, it gives a bijection $\eta = \{\delta \in \gamma \mid \delta < \eta\} \to A[f(\eta)]$. So $|\eta| = |A[f(\eta)]| < |\alpha|$. Thus $\eta < \alpha$, otherwise $\alpha \le \eta$, so $\alpha \subseteq \eta$ and then $|\alpha| \le |\eta|$, a contradiction. Thus $\eta \in \alpha$.

2. Find an ordering $\leq$ on $\alpha \times \alpha = A$ as in step 1. For $\lambda < \alpha$ let $A_\lambda = \{(\theta, \zeta) \in \alpha \times \alpha \mid \max(\theta, \zeta) = \lambda\}$. Define $\leq$ on A by $(\theta', \zeta') < (\theta, \zeta)$ iff $\max(\theta', \zeta') < \max(\theta, \zeta)$ or $\max(\theta', \zeta') = \lambda = \max(\theta, \zeta)$ and one of

   (a) $\zeta = \zeta' = \lambda$ and $\theta' < \theta$,

   (b) $\zeta' < \zeta = \lambda$, or

   (c) $\theta = \theta' = \lambda$ and $\zeta < \zeta'$.

   (TODO Exercise: check $\leq$ is a well-ordering on A) Show property in step 1 holds. Let $x = (\theta, \zeta) \in A$. Let $\lambda = \max(\theta, \zeta)$. May assume $\lambda \geq \omega$. Let $\mu = \lambda^\dagger$. So $\mu < \alpha$ and by inductive hypothesis $|\mu \times \mu| = |\mu| < |\alpha|$. $\{y \in A \mid y < x\} \subseteq \{(\theta', \zeta') \in A \mid \max(\theta', \zeta') \leq \lambda\} \subseteq \mu \times \mu$. Thus $|A[x]| \leq |\mu \times \mu| < |\alpha|$.

□

3.6 Transfinite recursion

Allows us to construct, for ordinals α, sets $G(\alpha)$ so that $G(\alpha)$ is obtained from sets $G(\beta)$ for $\beta < \alpha$ by applying some operation $F : G(0), \dots, G(\beta) \to G(\alpha)$, where $G \restriction \alpha = G(0), \dots, G(\beta)$. G is also an operation. $G \restriction \alpha : \alpha \to \{G(\beta) \mid \beta < \alpha\}$, which is a set by axiom of replacement. Let F be an operation on sets. Denote by $F(b)$ the result of applying F to the set b by 3.4.9.

Theorem 3.6.1 (Transfinite recursion)**.** Suppose F is an operation. Then there is an operation G such that for all ordinals α we have $G(\alpha) = F(G \restriction \alpha)$. If G' is another such operation then $G(\alpha) = G'(\alpha)$ for all ordinals α.

In practice, we usually do not write F down explicitly as a first-order formula.

Remark 3.6.2. An application is Lindenbaum's lemma, compare 1.3.7 and 2.5.3. Suppose $\mathcal{L}$ is a first order language whose alphabet of symbols can be well-ordered. Suppose Σ is a consistent set of closed $\mathcal{L}$-formulas. Then there is a consistent set $\Sigma^* \supseteq \Sigma$ of closed $\mathcal{L}$-formulas such that for every closed $\mathcal{L}$-formula ψ either $\Sigma^* \vdash \psi$ or $\Sigma^* \vdash (\neg\psi)$.

Proof. The set of $\mathcal{L}$-formulas can be well-ordered. Any subset of a woset is well-ordered so the set of closed $\mathcal{L}$-formulas is well-ordered. Any woset is similar to some ordinal by 3.4.8. So we can write the set of closed $\mathcal{L}$-formulas as $\{\phi_\alpha \mid \alpha < \lambda\}$ for some ordinal λ. □