Logic

Michælmas 2003

Contents

Chapter 1

Introduction

The notes were typed up by me, John Fremlin `john@fremlin.de`.

These notes are based on the first three chapters of the part II mathematics course "Logic, Computation and Set Theory" given by Dr Leader in Cambridge in Michælmas 2003. These notes are not connected to Dr Leader in any way. If there are any mistakes in them, it is more than very likely that they are my fault, not Dr Leader's.

Furthermore these notes are very definitely no substitute for actually going to Dr Leader's lectures (which are very good), because they do not include all of the material and especially examples covered, or any of the asides. Additionally, the material on computation and set theory is not included in these notes.

Finally, I would like to thank Dr Leader for taking such care to polish his crystal-clear lectures, and for being a very patient supervisor.

Chapter 2

Propositional logic

Definition 2.1 (Primitive propositions)**.** *$P = \{p_1, p_2, p_3, \cdots\}$ is the set of primitive propositions.*

Definition 2.2 (Proposition)**.** *A proposition is a subset of strings of symbols from the alphabet $(,), \Rightarrow, \perp, p_1, p_2, \cdots$.*

Definition 2.3 (Language)**.** *The language L (or $L(P)$) is the set of propositions*

1. *$P \subset L$*
2. *$\perp \in L$*
3. *if $p, q \in L$, $(p \Rightarrow q) \in L$*

L_n is the set of propositions of length $\leq n$.

Definition 2.4 (Shorthands)**.**

$\neg p$	$(p \Rightarrow \perp)$	*"not p"*
$p \vee q$	$((\neg p) \Rightarrow q)$	*"p or q"*
$p \wedge q$	$\neg(p \Rightarrow (\neg q))$	*"p and q"*

Definition 2.5 (Valuation)**.** *A valuation is a function. $v : L \mapsto \{0, 1\}$.*

1. *$v(\perp) = 0$*
2. *$v(p \Rightarrow q) = \begin{cases} 0 & \textit{if } v(p) = 1, v(q) = 0 \\ 1 & \textit{otherwise} \end{cases}$*

Theorem 2.6 (Valuations agreeing on the basic propositions are the same)**.** *If valuations v, v' have $v(p) = v'(p)$ for all $p \in P$ then $v \cong v'$.*

Proof. $v = v'$ on L_1. If $v(p) = v'(p)$ and $v(q) = v'(q)$ then $v(p \Rightarrow q) = v'(p \Rightarrow q)$ so by induction $\forall L_n$.

□

Theorem 2.7 (A function defined on the primitive propositions can be extended to a valuation)**.** *Given $w : P \mapsto \{0, 1\}$ there exists a valuation v such that $v(p) = w(p)$ for all $p \in P$.*

Proof. Let $v(p) = w(p)$ for all $p \in P$ and let $v(\perp) = 0$. Extend.

□

Definition 2.8 (Model)**.** *If* $v(p) = 1$*,* p *is true in* v*.* v *is a model of* p*.*

Definition 2.9 (Tautology)**.** *If* $v(p) = 1$ *for all valuations* v *then* p *is a tautology.* $\models p$*.*

Observation 2.10 (Techniques for proving something is a tautology)**.** *Draw a truth table, also note that if* $v(p \Rightarrow q) = 0$ *then* $p = 1$ *and* $q = 0$*.*

Definition 2.11 (Semantic implication, entails)**.** *If* $S \subseteq L$*,* $t \in L$ *and* $v(s) = 1$ *for all* $s \in S$ *means* $v(t) = 1$ *then* S *entails or semantically implies* t *(*$S \models t$*). That is, every model of* S *is a model of* t*.*

Chapter 3

Syntactic implication

Definition 3.1 (Axioms)**.** *1.* $p \Rightarrow (q \Rightarrow p)$ *is true* $\forall p, q \in L$

2. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ $\forall p, q, r \in L$

3. $(\neg\neg p) \Rightarrow p$ $\forall p \in L$

Observation 3.2 (Consistent with semantic implication)**.** *All the axioms are tautologies.*

Definition 3.3 (Modus ponens)**.** *From* p *and* $p \Rightarrow q$ *can deduce* q*.*

Definition 3.4 (Proof)**.** *Let* $S \subseteq L$ *be called the set of hypotheses or premises. A proof of a conclusion* $t \in L$ *from* S *is a finite set* $t_1, \cdots, t_n$ *with* $t_n = t$ *and each* t_i *is either*

1. *an axiom*
2. *a member of* S
3. *such that there exist* $j, k < m : t_k = (t_j \Rightarrow t_m)$

Then $S \vdash t$ *(*S *proves or syntactically implies* t*). If* $\emptyset \vdash t$ *then* t *is a theorem (written* $\vdash t$*).*

Theorem 3.5. $(p \Rightarrow q, q \Rightarrow r) \vdash (p \Rightarrow r)$

Proof.

1	$(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$	Axiom 2
2	$q \Rightarrow r$	Hypothesis
3	$(q \Rightarrow r) \Rightarrow (p \Rightarrow (q \Rightarrow r))$	Axiom 1
4	$p \Rightarrow (q \Rightarrow r)$	Modus ponens on 2, 3
5	$(p \Rightarrow q) \Rightarrow (p \Rightarrow r)$	Modus ponens on 4,1
6	$p \Rightarrow q$	Hypothesis
7	$p \Rightarrow r$	Modus ponens on 6,5

□

Theorem 3.6.

$$\vdash (p \Rightarrow p)$$

Proof.

1	$p \Rightarrow ((p \Rightarrow p) \Rightarrow p) \Rightarrow ((p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p))$	Axiom 2
2	$p \Rightarrow ((p \Rightarrow p) \Rightarrow p)$	Axoim 1
3	$(p \Rightarrow (p \Rightarrow p)) \Rightarrow (p \Rightarrow p)$	Modus ponens on 2,1
4	$p \Rightarrow (p \Rightarrow p)$	Axiom 1
5	$p \Rightarrow p$	Modus ponens on 4,3

□

Theorem 3.7 (Deduction theorem)**.** *Let $S \subseteq L$, $p, q \in L$. Then $S \vdash (p \Rightarrow q)$ iff $S \cup [p] \vdash q$.*

Proof. $S \vdash (p \Rightarrow q)$. Given a proof of $p \Rightarrow q$ from S add lines

p	Hypothesis
q	Modus ponens

Thus proving q from $S \cup [p]$.

$S \cup [p] \vdash q$

Let $t_1, t_2, ..., t_n$ be a proof of q from $S \cup [p]$. Show that $S \vdash (p \Rightarrow t_i)$ for every i.

If $t_i = p$ certainly $S \vdash (p \Rightarrow p)$ as $\vdash (p \Rightarrow p)$.

Otherwise if t_i is an axiom or $t_i \in S$, write

t_i	Axiom or Hypothesis
$t_i \Rightarrow (p \Rightarrow t_i)$	Axiom 1
$p \Rightarrow t_i$	Modus ponens

So $S \vdash (p \Rightarrow t_i)$.

Otherwise t_i was got from Modus Ponens, i.e. there exist j such that $t_j \Rightarrow t_i$. By induction on i assume $S \vdash (p \Rightarrow t_j)$ and $S \vdash (p \Rightarrow (t_j \Rightarrow t_i))$ so write

$(p \Rightarrow (t_j \Rightarrow t_i)) \Rightarrow ((p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i))$	Axiom 2
$(p \Rightarrow t_j) \Rightarrow (p \Rightarrow t_i)$	Modus ponens
$p \Rightarrow t_i$	Modus ponens

□

Example 3.8. *To show $\{p \Rightarrow q, q \Rightarrow r\} \vdash (p \Rightarrow q)$ show $\{p \Rightarrow q, q \Rightarrow r, p\} \vdash r$ using modus ponens twice.*

Theorem 3.9 (Soundness theorem)**.** *Let $S \subseteq L$, $t \in L$ then $S \vdash t$ implies $S \models t$.*

Proof. Given a valuation v that is a model for S, i.e. $v(s) = 1 \forall s \in S$ we want $v(t) = 1$.

Certainly axioms (are tautologies) and elements of S are true. Also modus ponens: if $v(p) = 1$ and $v(p \Rightarrow q) = 1$ then $v(q) = 1$. So $v(p) = 1$ for all p in a proof of t from S.

□

Definition 3.10. *$S \subseteq L$ is inconsistent if $S \vdash \perp$. Otherwise it is consistent.*

Definition 3.11 (Deductively closed)**.** *A set $S \subseteq L$ is deductively closed if it contains all its consequences. If $S \vdash p$ then $p \in S$.*

Theorem 3.12 (S consistent implies it has a model)**.** *Let $S \subseteq L$ be consistent. Then S has a model.*

Proof. Key idea: the theorem fails if both p and $\neg p$ are in S. So try to extend S keeping it consistent to swallow up one of p or $\neg p$ for each $p \in L$.

Claim. For any consistent $S \subseteq L$ and any $p \in L$ at least one of $S \cup \{p\}$ and $S \cup \{\neg p\}$ is consistent.

Proof of claim. Suppose $S \cup \{p\}$ is inconsistent. Then $p \vdash \perp$. So $S \vdash (p \Rightarrow \perp)$ so S and $S \cup \{\neg p\}$ prove the same things so $S \cup \{\neg p\}$ is consistent.

L is countable. Let $t_1, t_2, t_3, \cdots$ be an ordering of L. Let $S_0 = S$. Let S_{n+1} be $S_n \cup \{t_n\}$ or $S_n \cup \{\neg t_n\}$ choosing one which is consistent. Let $\bar{S} = \cup_{n \geq 1} S_n$. Then for each $p \in L$ at least one of $p \in \bar{S}$ or $\neg p \in \bar{S}$. $\bar{S}$ is consistent because proofs are finite. Also $\bar{S}$ deductively closed. If $p \notin S$ then S does not prove p (as $\neg p \in S$).

Define $v\colon L \mapsto \{0,1\} : v(p) = \begin{cases} 1 & \text{if } p \in S \\ 0 & \text{otherwise} \end{cases}$. v is a valuation. Proof. $v(\perp) = 0$. If $v(p) = 1, v(q) = 0$ then $p \in \bar{S}$, $q \notin \bar{S}$. So $(p \Rightarrow q) \notin \bar{S}$ so $v(p \Rightarrow q) = 0$. If $v(q) = 1$ then $q \vdash (p \Rightarrow q)$ so $(p \Rightarrow q) \in \bar{S}$ so $v(p \Rightarrow q) = 1$. If $v(p) = 0$ then $p \notin \bar{S}$ so $\neg p \in \bar{S}$. Enough to show $\neg p \Rightarrow (p \Rightarrow q)$. That is, $(p, \neg p) \vdash q$.

$p \Rightarrow \perp$	Hypothesis
$\perp \Rightarrow \neg\neg q$	Axiom 1
$(\neg\neg q) \Rightarrow q$	Axiom 3

So $v(p \Rightarrow q) = 1$. So v is a valuation. So there is a model for S.

□

Observation 3.13. *Previous theorem used fact that P is countable (so that L is countable) but this is not necessary by Zorn's lemma (next chapter).*

Corollary 3.14 (Adequacy theorem)**.** *Let $S \subseteq L$, $t \in L$. Then $S \models t$ implies $S \vdash t$.*

Proof. If $S \models t$ then $S \cup (\neg t) \models \perp$ (has no model) so $S \cup (\neg t) \vdash \perp$ (is inconsistent). $S \vdash ((\neg t) \Rightarrow \perp)$ by deduction theorem. $S \vdash (\neg\neg t)$. So $S \vdash t$ by axiom.

□

Theorem 3.15 (Completeness theorem for propositional logic)**.** *Let $S \subseteq L$, $t \in L$. Then $S \models t$ iff $S \vdash t$.*

Proof. Adequacy and soundness theorems.

□

3.0.1 Two consequences of completeness

Theorem 3.16 (Compactness theorem)**.** *Let $S \subseteq L$, $t \in L : S \models t$. Then some finite $S' \subseteq S$ has $S' \models t$.*

Proof. If $S \models t$ then $S \vdash t$. But proofs are finite so some finite $S' \subseteq S$ has $S' \vdash t$. Then $S' \models t$.

□

Corollary 3.17 (Equivalent formulation of compactness)**.** *If every finite subset of S has a model, then S is consistent.*

Proof. There is no finite subset of S, such that $S \vdash \perp$. So $S \nvdash \perp$.

□

Theorem 3.18 (Decidability theorem)**.** *There is an algorithm to determine, for any $S \subseteq L$ and $t \in L$ whether or not $S \vdash t$.*

Note that this is not obvious at all.

Proof. Trivial by replacing $\vdash$ with $\models$. To decide if $S \models t$ just write down a truth table.

□

Chapter 4

Posets and Zorn's lemma

Definition 4.1 (Poset)**.** *A partially ordered set or poset is a pair $(X, \leq)$ where X is a set and $\leq$ is a relation on X satisfying:*

1. *Reflexivity: $x \leq x$, $\forall x \in X$.*
2. *Antisymmetry: if $x \leq y$ and $y \leq x$ then $x = y$, $\forall x, y \in X$.*
3. *Transitivity: if $x \leq y$ and $y \leq z$ then $x \leq z$, $\forall x, y, z \in X$.*

Write $x < y$ for $x \leq y$ and $x \neq y$. Alternatively in terms of $<$, $\nexists x : x < x$, $x < y$ and $y < z$ implies $x < z$.

Example 4.2. $(\mathbb{N}, \leq)$, $(\mathbb{Q}, \leq)$ *and* $(\mathbb{R}, \leq)$ *are posets (in fact total orders).*

Example 4.3. $(\mathbb{N}^+, |)$ *where ($x|y$ means x divides y) is not a poset.*

Example 4.4. *S a set. $X \subseteq \mathbb{P}(S)$ with $A \leq B$ if $A \subseteq B$.*

Definition 4.5 (Hasse diagram)**.** *A Hasse diagram for a poset is a drawing of the points in the poset with an upwards line from x to y if y covers x (meaning $x < y$ and $\nexists z : x < z < y$).*

Sometimes a Hasse diagram can be drawn for an infinite poset. For example $(\mathbb{N}, \leq)$ but $(\mathbb{Q}, \leq)$ has an empty Hasse diagram.

Definition 4.6 (Chain)**.** *A chain in a poset X is a set $A \subseteq X$ that is totally ordered ($\forall x, y \in A$: have $x \leq y$ or $y \leq x$).*

For example in $(\mathbb{R}, \leq)$ any subset, like $(\mathbb{Q}, \leq)$ is a chain. Note that a chain need not be countable.

Definition 4.7 (Antichain)**.** *An antichain is a subset $A \subseteq X$ in which no two distinct elements are comparable. $\forall x, y : x \neq y$, neither $x \leq y$ nor $y \leq x$.*

Definition 4.8 (Upper bound)**.** *For $S \subseteq X$ and $x \in X$, say x is an upper bound for S if $y \leq x$ $\forall y \in S$.*

Definition 4.9 (Least upper bound, supremum, $\wedge S$)**.** *x is a least upper bound for $S \subseteq X$ if x is an upper bound for S and every upper bound y for S satisfies $x \leq y$.*

Clearly unique if it exists. Write $x = \wedge S = \sup S$ the supremum or join of S.

Definition 4.10 (Complete)**.** *A poset is complete if every set has a supremum.*

Observation 4.11. *Every complete poset X has a greatest element, $\wedge X$ and a least element $\wedge\emptyset$.*

Definition 4.12 (Monotone, order preserving)**.** *A function $f : X \mapsto X$, X a poset, is monotone or order preserving if $x \leq y$ implies $f(x) \leq f(y)$.*

Theorem 4.13 (Knaster-Tarski fixed point theorem)**.** *X a complete poset, $f : X \mapsto X$ order preserving. Then f has a fixed point.*

Proof. Let $E = \{x \in X : x \leq f(x)\}$. Possibly $E = \emptyset$.

Claim. If $x \in E$ then $f(x) \in E$. Proof. $x \leq f(x)$ so $f(x) \leq f(f(x))$ as f order preserving. So $f(x) \in E$.

Let $s = \wedge E$.

Claim. $s \in E$. True if $f(s)$ an upper bound for E (so $s \leq f(s)$). If $x \in E$, $x \leq s$ so $f(x) \leq f(s)$. But $x \in E$ so $x \leq f(x) \leq f(s)$. So $f(s)$ is an upper bound for E.

So $f(s)$ in E by first claim. So $f(s) \leq s$ but second claim showed $s \leq f(s)$ so $f(s) = s$.

□

Corollary 4.14 (Schröder-Bernstein theorem)**.** *A, B have injections $f : A \mapsto B$ and $g : B \mapsto A$ then A, B biject.*

Proof. Want partitions $A = P \cup Q$ and $B = R \cup S$ such that f_p bijects P with R and g_s bijects S with Q.

Then define obvious bijection $h : A \mapsto B$ by taking $h = f$ on P and $h = g^{-1}$ on Q.

Set $P \subseteq A : A \setminus g(B \setminus f(P)) = P$, $R = f(P)$, $S = B \setminus R$, $Q = g(S)$. Consider $(X = \mathbb{P}(A), \subseteq)$. X complete. Define $\theta : X \mapsto X$. $\theta(P) = A \setminus g(B \setminus f(P))$. Then θ is order preserving so it has a fixed point by Knaster-Tarski.

□

Definition 4.15 (Chain-complete)**.** *A (non-empty) poset X is chain-complete if every non-empty chain has a supremum.*

Observation 4.16. *Not all functions on chain-complete posets have fixed points. Any function on an anti-chain is order preserving.*

Observation 4.17. *The non-empty condition is a little pedantic but necessary.*

Definition 4.18 (Inflationary)**.** *$f : X \mapsto X$ is inflationary if $x \leq f(x)$ $\forall x \in X$.*

Not necessarily related to order preserving.

Theorem 4.19 (Bourbaki-Witt theorem)**.** *X is a chain-complete poset, $f : X \mapsto X$ inflationary. Then f has a fixed point.*

Proof. This proof is like battling Godzilla on a tightrope, it has to be carefully choreographed. Although the theorem seems fairly plausible, it has many big consequences.

Fix $x_0 \in X$. Say $A \subseteq X$ closed if

1. $x_0 \in A$
2. $x \in A$ implies $f(x) \in A$
3. C a non-empty chain in A implies $\wedge C \in A$.

Note that any intersection of closed sets is closed.

Let $E = \cap_{A \text{closed}} A$ is closed. Therefore if $A \subseteq E$ then $A = E$.

Assume E is a chain. Let $s = \wedge E$. Then $s \in E$ as E is closed. Therefore $f(s) \in E$. So $f(s) \leq s$. So $f(s) = s$ as f inflationary. So done.

Claim. E is a chain.

Say $x \in E$ is normal if $\forall y \in E : y < x$ then $f(y) \leq x$.

There are two properties of normality we want prove. All $x \in E$ are normal. Secondly, it should satisfy the condition we might naturally describe as "normal": if x normal then $\forall y \in E$ either $y \leq x$ or $y \geq f(x)$.

Once we have done this, we are finished. $\forall x, y \in E$, $y \leq x$ or $y \geq f(x) \geq x$. So E is a chain.

Claim. If x normal then $\forall y \in E$ either $y \leq x$ or $y \geq f(x)$.

Proof of claim. Let $A = \{y \in E : y \leq x \text{ or } y \geq f(x)\}$. Will show A is closed. Any closed subset of E is E so A closed implies $A = E$.

1. $x_0 \in A$. $x_0 \leq x$ ($\forall x \in E$).

2. Given $y \in A$ we need $f(y) \in A$. So have $y \leq x$ or $y \geq f(x)$ and want $f(y) \leq x$ or $f(y) \geq f(x)$.

   If $y < x$ then $f(y) \leq x$ as x is normal.
   If $y = x$ then $f(y) \geq f(x)$.
   If $y \geq f(x)$ then $f(y) \geq y \geq f(x)$.

   So $f(y) \in A$.

3. Given a (non-empty) chain $C \subseteq A$, want $s = \wedge A \in A$.

   If all $y \in C$ have $y \leq x$ then certainly $s \leq x$ because s a supremum. Otherwise some $y \in C$ has $y \geq x$ and not $y \leq x$ so $y \geq f(x)$ as $y \in A$. So $s \geq y \geq f(x)$. So $s \in A$.

So A closed, so A closed subset of smallest possible closed set E so $A = E$.

Claim. Every $x \in E$ is normal.

Proof of claim. Let $N = \{x \in E : x \text{ is normal }\}$. We will show that N is closed so $N = E$.

N is closed:

1. No $y \in E$ has $y < x_0$. So x_0 is normal, $x_0 \in N$.

2. Given x normal want $f(x)$ normal. So must show $y < f(x)$ implies $f(y) \leq f(x)$. By first claim $y < f(x)$ implies $y \leq x$. So $y = x$ or $y < x$. So $f(y) = f(x)$ or $f(y) \leq x \leq f(x)$ (because x is normal).

3. Given a (non-empty) chain $C \subseteq N$ need $s = \wedge C \in N$. That is, we need that if $y < s$ then $f(y) \leq s\ \forall y \in E$.

   For $y < s$ cannot have $y \geq x\ \forall x \in C$ (definition of supremum). So some $x \in C$ has not $y \geq x$, so $y < x$ by the first claim. So $f(y) \leq x$ (x normal) so certainly $f(y) \leq s$.

So N closed so $N = E$. So E is a chain.

$\square$

Observation 4.20. *"Now forget the proof" - Dr Leader*

Definition 4.21 (Maximal element of a poset)**.** *Given a poset X an element x is maximal if no $y \in X$ has $y > x$.*

Corollary 4.22 (Every chain-complete poset has a maximal element)**.** *Every chain-complete poset has a maximal element.*

Observation 4.23. *Very non-obvious theorem which trivially implies Bourbaki-Witt (x maximal implies $f(x) = x$).*

Proof. By contradiction. For each $x \in X$ have $\bar{x} \in X$ with $\bar{x} > x$. Then the function $x \mapsto \bar{x}$ is inflationary. So it has a fixed point. Contradiction.

□

Lemma 4.24 (One important chain-complete poset)**.** *Let X be any poset and let P be the collection of all chains of X ordered by inclusion. Then P is chain complete.*

Proof. Let $\{C_i : i \in I\}$ be a chain in P. C_i is a chain in X for all $i \in I$. Note that I need not be countable. Further $\forall i, j \in I$ $C_i \subseteq C_j$ or $C_j \subseteq C_i$.

Now let $C = \cup_{i \in I} C_i$. C is clearly a least upper bound for $\{C_i\}$. We need to show that it is a chain.

Let $x, y \in C$. So $\exists i, j : x \in C_i$ and $y \in C_j$. So $C_i \subseteq C_j$ or $C_j \subseteq C_i$. So x, y related. So C a chain.

□

Corollary 4.25 (Kuratowski's lemma)**.** *Every poset X has a maximal chain.*

Proof. The set of chains of X is a chain-complete poset.

□

Corollary 4.26 (Zorn's lemma)**.** *Let X be a (non-empty) poset in which every chain has an upper bound. Then X has a maximal element.*

Proof. Let C be a maximal chain in X. Let x be an upper bound for C. Then x is maximal. If $y > x$ then $C \cup \{y\}$ is a chain properly containing C. Contradiction.

□

Observation 4.27. *Non-emptiness actually not needed as it follows from the condition that every chain has an upper bound.*

Corollary 4.28 (Every vector space V has a basis)**.** *Every vector space V has a basis.*

Proof. Let $X = \{A \subseteq V : A$ is linearly independent $\}$ ordered by inclusion. We seek the existence of maximal element $A \in X$ using Zorn's lemma. Then we are done because if A does not span V it is not maximal.

1. $\emptyset$ is linearly independent. So $\emptyset \in X$. So $X \neq \emptyset$.

2. Given a chain $\{A_i : i \in I\}$ in X we seek an upper bound S. Let $S = \cup_{i \in I} A_i$. Then $S \supseteq A_i$ $\forall i$ so we just need $S \in X$ (that is, S linearly independent).

   Suppose $\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n = 0$ for some $x_1, \cdots, x_n \in A$ and $\lambda_1, \cdots, \lambda_n$ not all zero. Have $A_m \in X$ such that A_m contains all the x_i because X is a chain. But this contradicts A_m being linearly independent. So $S \in X$. So every chain has an upper bound.

□

Corollary 4.29 (Completeness theorem for L(P) when the set P of primitive propositions may be uncountable)**.** *Let $S \subseteq L(P)$ for any P. Then S consistent implies S has a model.*

Proof. Want $\bar{S} \supset S$, that is consistent, with $t \in \bar{S}$ or $\not t \in \bar{S}$ for all $t \in L$. Then done by setting $v(t) = \chi_{\bar{S}}(t)$.

Try to get a maximal consistent $\bar{S} \supset S$. Then for any $t \in L$ have $\bar{S} \cup \{t\}$ or $\bar{S} \cup \{\not t\}$ consistent. So $\bar{S}$ satisfies $t \in \bar{S}$ or $\not t \in \bar{S}$ for all $t \in L$.

Thus let $X = \{T \subseteq L : T \supseteq S, T \text{ consistent }\}$.

We want to use Zorn's lemma to show that T has a maximal element.

1. $X \neq \emptyset$ since $S \in X$.

2. Given a non-empty chain $\{T_i : i \in I\}$ in X. Seek an upper bound T. Let $T = \cup_{i \in I} T_i$. Then $T \supset T_i \; \forall i$. Just need $T \in X$.

   $S \subseteq T$ as $S \subseteq T_i \; \forall i$ (and $I \neq \emptyset$).

   Claim. T consistent.

   Proof of claim. Suppose $T \vdash \perp$. Then have $t_1, \cdots, t_n \in T$ with $\{t_1, \cdots, t_n\}$ inconsistent. Have $t_j \in T_{i_j}$ for some $i_j \in I$. But one of the T_{i_j} contains the others because they are in the same chain, call this one T_k. Then T_k is inconsistent which is a contradiction.

So we can apply Zorn's lemma.

□

Observation 4.30 (Zorn's lemma and the axiom of choice)**.** *In the proof of Zorn's lemma (i.e. more precisely the proof that chain-complete posets have maximal elements) we made an infinite number of arbitrary choices: for each $x \in X$ we picked $\bar{x} > x$". Note that in the IA Numbers and Sets course the axiom of choice was used to simultaneously pick orderings for a countable number of sets.*

The axiom of choice says: Given a set I and a family $\{A_i : i \in I\}$ of non-empty sets, there is a function $f : I \mapsto \cup_{i \in I} A_i$ such that $f(i) \in A_i \; \forall i$.

This is different from the other rules that are used to build sets because it claims the existence of an object which is not necessarily specified uniquely.

Therefore it is sometimes interesting to see if a proof depends on the axiom of choice.

Note that the axiom of choice follows from the other axioms for finite sets but not for infinite ones. Furthermore it is not possible to deduce Axiom of Choice for infinite sets from the other axioms(?).

From Zorn's lemma we can deduce the axiom of choice. Given a family $\{A_i\}_{i \in I}$, define a partial choice function (PCF) $f : J \mapsto \cup_{i \in I} A_i$ with $f(i) \in A_i \; \forall i \in J$ for some $J \subseteq I$. Order partial choice functions with $f \leq g$ iff $J_f \subseteq J_g$ and $f = g$ on J_f. Then the set of all PCFs is a poset on which we can apply Zorn's lemma to find a maximal PCF.

Zorn's lemma was hard to prove because Bourbaki-Witt was hard, not because the Axiom of Choice was used.

Furthermore Zorn's lemma is easy to prove from the Axiom of Choice using well-ordering and ordinals (chapter 6).

Chapter 5

Predicate logic

Observation 5.1. *"The completeness theorem is an absolute highlight of all of mathematics. It's brilliant" - Dr Leader*

Definition 5.2 (Arity)**.** *The number of arguments to a function is its arity.*

Definition 5.3 (Group)**.** *A group is a set A with functions $m : A^2 \mapsto A, i : A \mapsto A, e : A^0 \mapsto A$.*

$$[Associativity](\forall x, y, z)(m(x, m(y, z)) = m(m(x, y), z) \tag{5.1}$$

$$[Identity](\forall x)(m(x, e) = x \wedge m(e, x) = x) \tag{5.2}$$

$$[Inverse](\forall x)(m(x, i(x)) = e \wedge e = m(i(x), x)) \tag{5.3}$$

Definition 5.4 (Poset)**.** *A poset is a set A with a relation $\leq \subseteq A^2$. Conveniently $\leq (x, y)$ is written $x \leq y$.*

$$[Reflexivity](\forall x)(x \leq x) \tag{5.4}$$

$$[Anti-symmetry](\forall x, y)((x \leq y \wedge y \leq x) \Rightarrow (x = y)) \tag{5.5}$$

$$[Transitivity](\forall x, y, z)((x \leq y \wedge y \leq z) \Rightarrow (x \leq z)) \tag{5.6}$$

Definition 5.5 (Language L, functions Ω, predicate Π, arity function α)**.** *Let the set of functions Ω and predicates Π be distinct sets, and let the arity function be $\alpha : \Omega \cup \Pi \mapsto \mathbb{N}$. Then the language $L = L(\Omega, \Pi, \alpha)$ is the set of all formulae.*

Example 5.6. *For groups, $\Omega = \{m, i, e\}, \Pi = \emptyset$. For posets, $\Omega = \emptyset, \Pi = \{\leq\}$.*

Definition 5.7 (Term)**.** *A term is a subset of strings of symbols from the alphabet $\Omega \cup \Pi$.*

1. *Every variable is a term $(x_0, x_1, \cdots)$.*
2. *If $f \in \Omega$, $\alpha(f) = n$ and $t_1, \cdots, t_n$ are terms then $f(t_1, \cdots, t_n)$ is a term.*

Observation 5.8. *Note that the term $f(t_1, \cdots, t_n)$ is not the value of the function f with these arguments. It is just a string. To emphasize this you can write it $ft_1, \cdots, t_n$.*

Definition 5.9 (Atomic formula)**.** *An atomic formula is one of*

1. $\perp$.
2. $(s = t)$ *if* s, t *are terms.*
3. $\phi(t_1, \cdots, t_n)$ *if* $\phi \in \Pi$ *and* $\alpha(\phi) = n$ *and* $t_1, \cdots, t_n$ *are terms.*

Definition 5.10 (Formula)**.**

1. *Atomic formulae are formulae.*
2. *If* p *and* q *are formulae then so is* $(p \Rightarrow q)$.
3. *If* p *a formula and* x *a variable then* $(\forall x)p$ *is a formula.*

Definition 5.11 (Shorthands)**.**

$\neg p$	$(p \Rightarrow \perp)$	*"not p"*
$p \vee q$	$((\neg p) \Rightarrow q)$	*"p or q"*
$p \wedge q$	$\neg(p \Rightarrow (\neg q))$	*"p and q"*
$(\exists x)p$	$\neg(\forall x)(\neg p)$	*"exists x such that p"*

Definition 5.12 (Free and bound variables)**.** *An occurrence of a variable* x *in a formula is free if it is not within the brackets of a "*$\forall x$*". Otherwise it is bound.*

Definition 5.13 (Sentence)**.** *A sentence is a formula with no free variable (for example the axioms for groups and posets).*

Definition 5.14 (L-structure)**.** *Let* $L = L(\Omega, \Pi, \alpha)$ *be a language. An* L*-structure is a non-empty set* A*, for each* $f \in \Omega$ *a function* $f_A : A^{\alpha(f)} \mapsto A$ *and for each* $\phi \in \Pi$ *a subset* $\phi_A \subseteq A^{\alpha(\phi)}$.

Example 5.15. L *the language of groups: an* L*-structure is a set* A *with functions* $m_A : A^2 \mapsto A, i_A : A \mapsto A, e_A \in A$.

L *the language of posets: an* L*-structure is a non-empty set with a relation* $\leq_A \subseteq A^2$.

Definition 5.16 (Closed term)**.** *A closed term is a term with no variables. For example* $m(e, i(e))$*,* not $m(x, i(x))$.

Definition 5.17 (Interpretation of a closed term)**.** *The interpretation of a closed term in an* L*-structure* A *written* $t_A \in A$ *is defined inductively. If* $f \in \Omega$, $\alpha(f) = n$ *and* $t_1, \cdots, t_n$ *closed terms then* $f(t_1, \cdots, t_n)_A = f_A(t_{1_A}, \cdots, t_{n_A})$.

Note that if c *is constant symbol then* c_A *is already defined.*

Definition 5.18 (Interpretation of a sentence)**.** *For a sentence* $p \in L$ *and an* L*-structure* A *the interpretation of* p *in* A *is a* $p_A \in \{0, 1\}$ *defined inductively*

1. $\perp_A = 0$
2. *For closed terms* s, t $(s = t)_A = \begin{cases} 1 & \text{if } s_A = t_A \\ 0 & \text{otherwise} \end{cases}$.
3. *For* $\phi \in \Pi$, $\alpha(\phi) = n$ *and closed terms* $t_1, \cdots, t_n$ *set*

$$\phi(t_1, \cdots, t_n) = \begin{cases} 1 & \text{if} (t_{1_A}, \cdots, t_{n_A}) \in \phi_A \\ 0 & \text{otherwise} \end{cases}$$

4. *For sentences* p, q *set* $(p \Rightarrow q)_A = \begin{cases} 0 & \text{if } p_A = 1, q_A = 0 \\ 1 & \text{otherwise} \end{cases}$.

5. $((\forall x)p)_A = \begin{cases} 1 & \text{if for all } a \in A \text{ have } p[\bar{a}/x]_A = 1 \\ 0 & \text{otherwise} \end{cases}$

   where we extend L *to* L' *by adding a new constant symbol* $\bar{a}$ *and make* A *an* L'*-structure by setting* $\bar{a}_A = a$ *and for any term* t*,* $p[t/x]$ *is the formula obtained by replacing each free occurrence of* x *with* t*.*

Observation 5.19. *"Now forget all this nonsense and think of it only as in the original idea." - Dr Leader.*

Definition 5.20 (Truth, models, holds)**.** *If* $p_A = 1$ *we say* p *holds in* A *or* p *is true in* A *or* A *is a model of* p *written* $A \models p$*.*

Definition 5.21 (Theory, tautology)**.** *For a set* T *of sentences (a theory) say* A *is a model of* T *written* $A \models T$ *if* $A \models p \ \forall p \in T$*.*

For T *a theory,* p *a sentence, say* T *entails* p *written* $T \models p$ *if every model of* T *is a model of* p*.*

If $\emptyset \models p$ *we say* p *is a tautology.*

Observation 5.22. *What is called in propositional logic a valuation is like in predicate logic an interpretation.*

Definition 5.23 (Axiomatize, axioms)**.** *Say that the members of a theory* T *are axioms, and that the theory axiomatizes the things which are models of it.*

Example 5.24 (Theory of groups)**.** *Let* L *be the language of groups and let*

$T = \{(\forall x, y, z)(m(x, m(y, z)) = m(m(x, y), z),$
$(\forall x)(m(x, e) = x \wedge m(e, x) = x),$
$(\forall x)(m(x, i(x)) = e \wedge e = m(i(x), x))\}$

Then an L*-structure* A *is a model of* T *iff* A *is a group.* T *axiomatizes the class of groups.*

Suppose we change the third axiom to be just $(\forall x)(m(x, i(x)) = e)$ *to produce* T'*. Does* T' *axiomatize the class of groups? (Think about it but the answer is yes).*

Example 5.25 (Theory of posets)**.** *Let* $L =$ *language of posets and let* $T = \{(\forall x, y)((x \leq y \wedge y \leq x) \Rightarrow (x = y)), (\forall x)(x \leq x), (\forall x, y, z)(((x \leq y) \wedge (y \leq z)) \Rightarrow (x \leq x))\}$*. Then a model for* T *is precisely a poset.*

Example 5.26 (Theory of fields)**.** *Let* $\Omega = \{+, \times, -, 0, 1\}$. $\Pi = \emptyset$*. For* T *take*

1. *Abelian group under* $+, -, 0$
2. *Associative*
3. *Commutative*
4. *Distributive over* $+$
5. $\neg(0 = 1)$
6. $(\forall x)((\neg(x = 0)) \Rightarrow ((\exists y)(x \times y = y \times x = 1))$

Then T axiomatizes the class of fields.

Example 5.27 (Theory of graphs). *Language of $\Omega = \emptyset$ and $\Pi = \{\sim\}$. $T = \{(\forall x)(\neg(x \sim x)), (\forall x, y)((x \sim y) \Rightarrow (y \sim x))\}$.*

Then an L-structure on G is a T-model iff G is a graph.

Observation 5.28. *This is called first-order logic. We can qualify over elements but not over subsets. For example we cannot say "for all subgroups of A".*

Observation 5.29. *Could have an alternative language for groups with $\Omega = \{m, e\}$ and third element of the theory being $(\forall x)(\exists y)(m(x, y) = e \wedge m(y, x) = e)$.*

Observation 5.30. *Many natural theories have T infinite. For example, we have fields of characteristic zero. L language of fields. T = axioms of a field, with $\neg(1 + 1 = 0)$,$\neg(1 + 1 + 1 = 0)$ etc.*

Observation 5.31. *Fields of non-zero characteristic. L language of fields, T axioms for a field. Can we axiomatize fields of charactistic $\neq 0$? (Exercise.)*

5.1 Proofs

Definition 5.32 (Logical axioms). *Three old ones, two for $=$ and two for $\forall$.*

1. $p \Rightarrow (q \Rightarrow p)$ *for any formulae* p, q.
2. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow q))$ *for any formulae* p, q, r.
3. $(\neg\neg p) \Rightarrow p$ *for any formula* p.
4. $(\forall x)(x = x)$ *for any variable* x.
5. $(\forall x, y)((x = y) \Rightarrow (p \Rightarrow p[y/x]))$ *where x, y variables, p a formula in which y does not occur bound.*
6. $((\forall x)p) \Rightarrow p[t/x]$ *where x is a variable, p a formula, t a term with no free variable occurring that is bound in p.*
7. $((\forall x)(p \Rightarrow q)) \Rightarrow (p \Rightarrow (\forall x)q)$ *where x is a variable, p, q formulae with x not occurring free in p.*

Definition 5.33 (Rules of deduction, modus ponens and generalization). *Modus ponens. From p, $p \Rightarrow q$ deduce q.*

Generalization. From p deduce $(\forall x)p$ as long as x does not occur in any of the premises used to prove p.

Definition 5.34 (Proof). *For $S \subseteq L$ and $p \in L$ a proof of p from S consists of a finite sequence of lines each of which is a logical axiom or a member of S or is obtained from earlier lines by a deduction rule.*

Write $S \vdash p$ if there is a proof of p from S.

Observation 5.35. *If we allowed $\emptyset$ to be an L-structure we would have a contradiction.*

Theorem 5.36 (Deduction theorem). *Let $S \subseteq L$ and $p, q \in L$. Then $S \vdash (p \Rightarrow q)$ iff $S \cup \{p\} \vdash q$.*

Proof. If $S \vdash (p \Rightarrow q)$ then have by modus ponens $S \cup \{p\} \vdash q$.

If $S \cup \{p\} \vdash q$ then as in the first chapter we show that for each line in r in a proof of q from $S \cup \{p\}$ in fact $S \vdash (p \Rightarrow r)$.

We do this inductively. The only new case is if we have used generalization. So in proof of q from $S \cup \{p\}$ we have

$$r$$

$$(\forall x)r$$

and we know that $S \vdash (p \Rightarrow r)$.

Note that the proof of r from $S \cup \{p\}$ did not use a free x in any hypothesis, so also our proof of $p \Rightarrow r$ from S did not use one. Therefore we can deduce $S \vdash ((\forall x)(p \Rightarrow r))$ by generalization.

If x is not free in p: deduce $S \vdash (p \Rightarrow ((\forall x)r))$ by the seventh axiom. Otherwise x is free in p. So in our proof of $(\forall x)r$ from $S \cup \{p\}$ cannot have used p (as generalization was used). So $S \vdash ((\forall x)r)$ so $S \vdash (p \Rightarrow ((\forall x)r))$ by the first axiom and modus ponens.

□

Theorem 5.37 (Soundness theorem)**.** *S is a set of sentences, and p a sentence. Then $S \vdash p$ implies $S \models p$.*

Proof. Given a model of S, p holds in this model by induction on the lines in the proof.

□

Theorem 5.38 (Model Existence Lemma or Completeness Theorem)**.** *Let S be a consistent set of sentences. Then S has a model.*

Definition 5.39 (Witness)**.** *A witness for $(\exists x)p$ is $p[t/x]$ for a closed term t.*

Proof. Have S in language $L = L(\Omega, \Pi)$. Extend S to maximal consistent $S_1 \subseteq L$ by Zorn's lemma.

Then S_1 is complete (that is for any $p \in L$ either $S_1 \cup \{p\}$ is consistent or $S_1 \cup \{\neg p\}$ consistent. For each $((\exists x)p) \in S$ add a new constant c to the language to form $L_1 = L(\Omega \cup C_1, \Pi)$ and add the sentence $p[c/x]$ to S_1 to form T_1.

Then T_1 is consistent. T_1 has witnesses for S_1.

Now extend T_n to a complete S_{n+1} and continue inductively.

Let $\bar{S} = \cup_{n=1}^{\infty} S_n$ in language $\bar{L} = L(\Omega \cup C_1 \cup C_2 \cup \cdots, \Pi)$.

Claim. $\bar{S}$ consistent. Proof of claim. Suppose $\bar{S} \vdash \perp$. Then some finite $S' \subseteq \bar{S}$ has $S' \vdash \perp$ whence some $S_n \vdash \perp$. Contradiction.

Claim. $\bar{S}$ complete. Proof of claim. For any sentence $p \in \bar{L}$ have $p \in L_n$ for some n as p mentions only finitely many symbols. But S_{n+1} complete in language L_n so $S_{n+1} \vdash p$ or $S_{n+1} \vdash (\neg p)$. But $\bar{S} \supseteq S$. Done.

Claim. $\bar{S}$ has witnesses. Proof of claim. Basically the same as for consistency.

For closed terms $s, t \in \bar{L}$ say $s \sim t$ if $\bar{S} \vdash (s = t)$, clearly an equivalence relation. Write $[t]$ for equivalence class of t.

Let $A = \{[t] : t \text{ a closed term of } \bar{L}\}$.

For each $f \in \Omega(\bar{L})$ with arity n and $t_1, \cdots, t_n$ closed terms, set $f_A([t_1], \cdots, [t_n]) = [f(t_1, \cdots, t_n)]$. (Clearly well defined.)

For each $\phi \in \Pi(\bar{L})$ with arity n and $t_1, \cdots, t_n$ closed terms, set $\phi_A([t_1], \cdots, [t_n]) = \{([t_1], \cdots, [t_n]) \in A^n : \bar{S} \vdash \phi(t_1, \cdots, t_n)\}$. (Clearly well defined.)

To show that A is a model for S we will show that for any sentence $p \in I$ we have $p_A = 1$ iff $\bar{S} \vdash p$. This is an easy induction.

1. $s = t$. $\bar{S} \vdash (s = t)$ iff $s \sim t$ iff $s_A = t_A$ iff $[s] = [t]$ iff $(s = t)_A = 1$.
2. $\phi(t_1, \cdots, t_n)$ similarly.
3. $\perp$. $\bar{S} \nvdash \perp$ and $\perp_A = 0$.
4. $(p \Rightarrow q)$. $\bar{S} \vdash (p \Rightarrow q)$ iff $\bar{S} \vdash p$ and $\bar{S} \nvdash q$ (as $\bar{S}$ is complete). By induction hypothesis $p_A = 0$ or $q_A = 1$ iff $(p \Rightarrow q)_A = 1$.
5. $(\exists x)p$. $\bar{S} \vdash (\exists x)p$ iff $\bar{S} \vdash p[t/x]$ or some closed term t, so $p[t/x]_A = 1$ by induction hypothesis, equivalently $(\exists x)p$ holds in A (since A is the set of all closed terms quotiented).

□

Corollary 5.40 (Adequacy theorem)**.** *Let S be a theory and p a sentence. Then $S \models p$ implies $S \vdash p$.*

Proof. If $S \models p$ then $S \cup \{\neg p\} \models \perp$ implies $S \cup \{\neg p\} \vdash \perp$. So by the deduction theorem $S \vdash (\neg\neg p)$ so $S \vdash p$.

□

Theorem 5.41 (Gödel's Completeness Theorem, the completeness theorem of first order logic)**.** *S a theory, p a sentence. Then $S \vdash p$ iff $S \models p$.*

Proof. By adequacy and soundness.

□

Corollary 5.42 (Compactness theorem)**.** *S a theory. If every finite subset of S has a model then so does S.*

Proof. Trivial if we replace "has a model" with "is consistent".

□

Corollary 5.43 (Upward Löwenheim-Skolem theorem)**.** *Let S be a theory with an infinite model. Then S has an uncountable model.*

Proof. Add to the language uncountably many new constants, say $\{c_i\}_{i \in I}$. Let $S' = S \cup \{\neg(c_i = c_j) : i, j \in I, i \neq j\}$.

We want a model for S'. But every finite $F \subset S'$ certainly has a model since F only mentions finitely many of the c_i. So by compactness the infinite model for S' exists, and it is also a model for S.

□

Observation 5.44. *The same trick of adding constants $c_1, \cdots$ shows that no set of sentences (in the language of groups, for example) can axiomatize (i.e. have as a model) the class of finite groups.*

In other words, "finiteness is not a first order property". Equivalently any theory that has arbitrarily large finite models must have an infinite model (called "overspill").

Corollary 5.45 (Downward Löwenheim-Skolem theorem)**.** *Let S be a consistent theory in a countable language (that is Ω, Π countable). Then S has a countable model.*

Proof. The model constructed in the proof of the model existence lemma was maximal and countable.

□

5.2 Peano Arithmetic

Definition 5.46 (Language of Peano arithmetic)**.** $\Omega = \{0, s, +, \times\}$ *where s is the successor function.*

Definition 5.47 (Axioms of Peano Arithmetic)**.** *1.* $(\forall x)(\neg(s(x) = 0))$

2. $(\forall x, y)((s(x) = s(y)) \Rightarrow (x = y))$
3. $(\forall y_1) \cdots (\forall y_n)((p[0/x] \wedge (\forall x)(p \Rightarrow p[s(x)/x])) \Rightarrow (\forall x)p)$*, that is, induction with parameters* $(\forall y_1) \cdots (\forall y_n)$ *for free variables in* p*.*
4. $(\forall x)(x + 0 = x)$
5. $(\forall x, y)(x + s(y) = s(x + y))$
6. $(\forall x)(x \times 0 = 0)$
7. $(\forall x, y)(x \times s(y) = (x \times y) + x)$

The first three axioms are sometimes called weak Peano Arithmetic.

Observation 5.48. *We might have first guessed that the induction axiom should have been* $(p[0/x] \wedge (\forall x)(p \Rightarrow p[s(x)/x])) \Rightarrow (\forall x)p$*. But this is not how we do induction in real life.*

Definition 5.49 (Axiom scheme)**.** *The induction axiom is in fact a different axiom for each* p*. An axiom like this specifying an infinite set of axioms is sometimes called an axiom scheme.*

Observation 5.50. *PA has an infinite model* ($\mathbb{N}$) *so by the Upward-Löwenheim-Skolem theorem PA has an uncountable model which is therefore not* $\mathbb{N}$*. But we would like* $\mathbb{N}$ *to be characterized uniquely by these axioms. The problem is that the induction axiom is not powerful enough - it only refers to countably many subsets of* $\mathbb{N}$ *(those defined by a* p*) whereas normal induction refers to all subsets.*

Therefore induction is not a first order property.