B1.1 Logic
Lecture 1

Martin Bays
(Slides adapted from slides written by
Prof. J. Koenigsmann)

Oxford, MT 2023

Introduction

1. What is mathematical logic for?

- Provides a uniform, unambiguous **language** for mathematics;

- gives a precise formal definition of a **proof**;

- explains and guarantees **exactness, rigour and certainty** in mathematics;

- establishes the **foundations** of mathematics.

$$\text{B1 (Foundations)} \\ = \text{B1.1 (Logic)} + \text{B1.2 (Set theory)}$$

N.B.: Course does not teach you to think logically, but it explores what it *means* to think logically.

2. Historical motivation

- *19th cent.*:
  Search for conceptual foundations in analysis: attempts to formalise the notions of **infinity, infinitesimal, limit, ...**

  > "*The definitive clarification of the nature of the infinite has become necessary, not merely for the special interests of the individual sciences but for the honour of human understanding itself.*" – Hilbert 1926

- Hilbert's 2nd Problem, 1900 ICM address: prove consistency of an axiom system for arithmetic.

  > *"I am convinced that it must be possible to find a direct proof for the compatibility of the arithmetical axioms." – Hilbert 1900*

2. Historical motivation (cont)

- Early attempts to formalise mathematics:
  - *Cantor*'s **naive** set theory;
  - *Frege*'s Begriffsschrift and Grundgesetze.

  For any expressible property $P(x)$, Frege's system posited the existence of the set

$$\{x : P(x)\}.$$

- **Russell's paradox**:
  consider the set $R := \{s : s \notin s\}$

$$\begin{array}{lcll} R \in R & \Rightarrow & R \notin R & \text{contradiction} \\ R \notin R & \Rightarrow & R \in R & \text{contradiction} \end{array}$$

  $\leadsto$ *fundamental crisis in the foundations of mathematics*

3. Hilbert's Program

1. find a uniform formal **language** for all mathematics
2. find a complete system of **inference rules/ deduction rules**
3. find a complete system of mathematical **axioms**
4. prove that the resulting system is **consistent**, i.e. does not lead to contradictions

⋆ **complete:** every mathematical sentence can be proved or disproved using 2. and 3.

⋆ 1., 2. and 3. should be **finitary/effective/computable/algorithmic** so, e.g., in 3. you can't take as axioms *the system of all true sentences in mathematics*

4. Solutions to Hilbert's program

Step 1. (formal language for mathematics)
possible in the framework of
ZF = *Zermelo-Fraenkel set theory* or
ZFC = **ZF** + *Axiom of* **C***hoice*

(this is an empirical fact)
$\rightsquigarrow$ B1.2 Set Theory

Step 2. (complete proof system)
possible in **1st-order logic**:
Gödel's Completeness Theorem
$\rightsquigarrow$ B1.1 Logic - this course

Step 3. (complete axiom system)
not possible ($\rightsquigarrow$ C1.2):
Gödel's 1st Incompleteness Theorem:
there is no effective axiomatization of arithmetic

Step 4. (proving consistency)
not possible ($\rightsquigarrow$ C1.2):
Gödel's 2nd Incompleteness Theorem

5. Decidability

Step 3. of Hilbert's program fails:
there is no effective axiomatization
for the entire body of mathematics

But: many important parts of mathematics **are** completely and effectively axiomatizable; they are **decidable**, i.e. there is an *algorithm = program = effective procedure* to decide whether a sentence is true or false
$\rightsquigarrow$ allows proofs by computer

Example: $Th(\mathbb{C}; +, \cdot)$, the **1st-order theory** of the field $\mathbb{C}$.

Axioms = *field axioms*
+ *all non-constant polynomials have a zero*
+ *the characteristic is* 0

Every **algebraic** property of $\mathbb{C}$ follows from these axioms.
Similarly for $Th(\mathbb{R})$.
$\rightsquigarrow$ C1.1 Model Theory

6. Why *mathematical* logic?

1. Language and deduction rules are tailored for *mathematical objects* and mathematical ways of reasoning

2. The *method* is mathematical:
   we will develop logic as a *calculus* with sentences and formulas
   $\Rightarrow$ Logic is itself a mathematical discipline,
   not meta-mathematics or philosophy,
   no ontological questions like
   what is a number?

3. Logic has *applications* in other areas of mathematics, and also in theoretical computer science

PART I: Propositional Calculus

1. The language of propositional calculus

... is a very coarse language with limited expressive power;

... allows you to break a complicated sentence down into its subclauses, but not any further;

... will be refined in PART II *Predicate Calculus*, the true language of 1st order logic;

... is nevertheless well suited for entering formal logic.

1.1 Propositional variables

The propositional calculus implements logic of the following kind:

- 1. Socrates is alive or Socrates is dead.
  2. Socrates is not alive.
  Therefore: Socrates is dead.

- 1. If Socrates is a vampire and vampires are immortal, then Socrates is not dead.
  2. Socrates is dead.
  Therefore: Either Socrates is not a vampire, or vampires are not immortal.

We use *propositional variables* to denote propositions - e.g. p_0 for "Socrates is a vampire".

A *proposition* is something which can be true or false.

1.2 The alphabet of propositional calculus

The alphabet of the propositional language $\mathcal{L}_{\mathsf{prop}}$ consists of the following symbols:

the propositional variables $p_0, p_1, \ldots, p_n, \ldots$

negation $\neg$ - the unary connective *not*

four binary connectives $\rightarrow$, $\wedge$, $\vee$, $\leftrightarrow$
implies, and, or and *if and only if* respectively

two punctuation marks (and)
left parenthesis and *right parenthesis*.

Note that these are *abstract symbols*.
Note also that we use $\rightarrow$, and not $\Rightarrow$.

1.3 Strings

- A **string (of $\mathcal{L}_{\text{prop}}$)** is any finite sequence of symbols from the alphabet of $\mathcal{L}_{\text{prop}}$.

- **Examples**

$$\begin{array}{rl} \text{(i)} & \to p_{17}() \\ \text{(ii)} & ((p_0 \wedge p_1) \to \neg p_2) \\ \text{(iii)} &))\neg)p_{32} \end{array}$$

- The **length** of a string is the number of symbols in it.
  So the strings in the examples have length $4, 10, 5$ respectively.
  (A propositional variable has length 1.)

- We now single out from all strings those which make grammatical sense (*formulas*).

1.4 Formulas

The notion of a **formula of** $\mathcal{L}_{\text{prop}}$ is defined (*recursively*) by the following rules:

I. Every propositional variable is a formula.

II. If the string A is a formula then so is $\neg A$.

III. If the strings A and B are both formulas then so are the strings

$$\begin{array}{cl} (A \to B) & \text{read } A \textit{ implies } B \\ (A \wedge B) & \text{read } A \textit{ and } B \\ (A \vee B) & \text{read } A \textit{ or } B \\ (A \leftrightarrow B) & \text{read } A \textit{ if and only if } B. \end{array}$$

IV. Nothing else is a formula,
i.e. a string ϕ is a formula if and only if ϕ can be obtained from propositional variables by finitely many applications of the *formation rules* II. and III.

Examples

- The string $((p_0 \wedge p_1) \to \neg p_2)$ is a formula (Example (ii) in 1.3).
  Proof:

$$\begin{tikzcd}
p_0 \arrow[dr, no head] & & p_1 \arrow[dl, no head, "\mathrm{III.}"'] & & p_2 \arrow[d, no head, "\mathrm{II.}"] \\
& (p_0 \wedge p_1) \arrow[drr, no head] & & & \neg p_2 \arrow[dl, no head, "\mathrm{III.}"'] \\
& & & ((p_0 \wedge p_1) \to \neg p_2) &
\end{tikzcd}$$

$\square$

- Parentheses are important, e.g. $(p_0 \wedge (p_1 \to \neg p_2))$ is a different formula and $p_0 \wedge (p_1 \to \neg p_2)$ is not a formula at all.

Examples

- The strings $\to p_{17}()$ and $))\neg)p_{32}$ from Example (i) and (iii) in 1.3 are not formulas.

  Indeed, if ϕ is a formula, then ϕ arises from one of I., II, or III., and so one of the following must hold:

  1. ϕ is a propositional variable.

  2. The first symbol of ϕ is $\neg$.

  3. The first symbol of ϕ is (.

The unique readability theorem
A formula can be constructed in only one way:
For each formula ϕ **exactly one** *of the following holds*

(a) ϕ is p_i for some unique $i \in \mathbb{N}$;

(b) ϕ is $\neg\psi$ for some **unique** formula ψ;

(c) ϕ is $(\psi \star \chi)$ for some **unique** pair of formulas ψ, χ and a **unique** binary connective $\star \in \{\rightarrow, \wedge, \vee, \leftrightarrow\}$.

Proof: Problem sheet 1.

2. Valuations

In natural language, the **truth** or **falsity** of a sentence using logical connectives is determined by the truth or falsity of its subclauses:
"Socrates is dead or Socrates is a vampire" is true because "Socrates is dead" is true.

The propositional calculus abstracts this to a recursive definition of the **truth value** T ('true') or F ('false') of a formula ϕ in terms of the truth values of the propositional variables occuring in ϕ.

2.1 Definition

1. A **valuation** v is a function

$$v : \{p_0, p_1, p_2, \ldots\} \to \{T, F\}.$$

2. Given a valuation v we extend v uniquely to a function

$$\tilde{v} : \mathrm{Form}(\mathcal{L}_{\mathrm{prop}}) \to \{T, F\}.$$

(Form($\mathcal{L}_{\mathrm{prop}}$) denotes the set of all formulas of $\mathcal{L}_{\mathrm{prop}}$)

defined recursively as follows:

(i) If ϕ is a formula of length 1, i.e. a propositional variable, then $\tilde{v}(\phi) := v(\phi)$.

(ii) If ϕ is a formula of length $n > 1$, and $\tilde{v}$ has been defined on formulas of length $< n$:
by the Unique Readability Theorem,
either $\phi = \neg\psi_1$ for a unique ψ_1,
or $\phi = (\psi_1 \star \psi_2)$ for a unique pair ψ_1, ψ_2 and a unique $\star \in \{\to, \wedge, \vee, \leftrightarrow\}$.
Then the ψ_i are formulas of length $< n$, and we define $\tilde{v}(\phi)$ in terms of the $\tilde{v}(\psi_i)$ by the **truth tables** on the following slide.

Truth Tables

Define $\widetilde{v}(\phi)$ by the following truth tables:

Negation

ψ	$\neg\psi$
T	F
F	T

i.e. if $\widetilde{v}(\psi) = T$ then $\widetilde{v}(\neg\psi) = F$
and if $\widetilde{v}(\psi) = F$ then $\widetilde{v}(\neg\psi) = T$

Binary Connectives

ψ	χ	$\psi \to \chi$	$\psi \wedge \chi$	$\psi \vee \chi$	$\psi \leftrightarrow \chi$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	T	F	T	F
F	F	T	F	F	T

so, e.g., if $\widetilde{v}(\psi) = F$ and $\widetilde{v}(\chi) = T$
then $\widetilde{v}(\psi \vee \chi) = T$ etc.

Remark: These truth tables correspond roughly to our ordinary use of the words *'not'*, *'if - then'*, *'and'*, *'or'* and *'if and only if'*, except, perhaps, the truth table for implication ($\to$).

2.2 Example

Construct the full truth table for the formula

$$\phi := ((p_0 \vee p_1) \to \neg(p_1 \wedge p_2))$$

$\widetilde{v}(\phi)$ only depends on $v(p_0), v(p_1)$ and $v(p_2)$.

p_o	p_1	p_2	$(p_0 \vee p_1)$	$(p_1 \wedge p_2)$	$\neg(p_1 \wedge p_2)$	ϕ
T	T	T	T	T	F	F
T	T	F	T	F	T	T
T	F	T	T	F	T	T
T	F	F	T	F	T	T
F	T	T	T	T	F	F
F	T	F	T	F	T	T
F	F	T	F	F	T	T
F	F	F	F	F	T	T

2.3 Example Truth table for

$$\phi := ((p_0 \to p_1) \to (\neg p_1 \to \neg p_0))$$

p_0	p_1	$(p_0 \to p_1)$	$\neg p_1$	$\neg p_0$	$(\neg p_1 \to \neg p_0)$	ϕ
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

3. Logical Validity

3.1 Definition

- A valuation v **satisfies** a formula ϕ if $\tilde{v}(\phi) = T$.

- A formula ϕ is **logically valid** if ϕ is satisfied by *every* valuation (e.g. Example 2.3, not Example 2.2). Such a ϕ is also called a **tautology**. *Notation:* $\models \phi$

- A formula ϕ is **satisfiable** if ϕ is satisfied by *some* valuation. So:

  ϕ is satisfiable iff $\neg\phi$ is *not* a tautology.

- A formula ϕ is a **logical consequence** of a formula ψ if, for *every* valuation v:

  $$\text{if } \tilde{v}(\psi) = T \text{ then } \tilde{v}(\phi) = T.$$

  Notation: $\psi \models \phi$

3.2 Lemma $\psi \models \phi$ *if and only if* $\models (\psi \to \phi)$.

Proof. '$\Rightarrow$': Assume $\psi \models \phi$.
Let v be any valuation.

- If $\tilde{v}(\psi) = T$ then (by def.) $\tilde{v}(\phi) = T$, so then $\tilde{v}((\psi \to \phi)) = T$ by tt $\to$.

  ('tt $\star$' refers to the truth table of the connective $\star$)

- If $\tilde{v}(\psi) = F$ then $\tilde{v}((\psi \to \phi)) = T$ by tt $\to$.

Thus, for every valuation v, $\tilde{v}((\psi \to \phi)) = T$, so $\models (\psi \to \phi)$.

'$\Leftarrow$': Conversely, suppose $\models (\psi \to \phi)$.
Let v be any valuation s.t. $\tilde{v}(\psi) = T$.
Since $\tilde{v}((\psi \to \phi)) = T$, also $\tilde{v}(\phi) = T$ by tt $\to$.
Hence $\psi \models \phi$. $\square$

3.3 Definition Let Γ be any (possibly infinite) set of formulas and let ϕ be any formula.
Then ϕ is a **logical consequence** of Γ if, for every valuation v:

$$\text{If } \tilde{v}(\psi) = T \text{ for all } \psi \in \Gamma \text{ then } \tilde{v}(\phi) = T.$$

Notation: $\Gamma \models \phi$

Note:

$$\models \phi \;\Leftrightarrow\; \emptyset \models \phi,$$
$$\psi \models \phi \;\Leftrightarrow\; \{\psi\} \models \phi.$$

Lemma 3.2 generalises to:

3.4 Lemma
$\Gamma \cup \{\psi\} \models \phi$ *if and only if* $\Gamma \models (\psi \to \phi)$.

Proof. Similar to the proof of Lemma 3.2. Exercise. $\square$

3.5 Example

	$\models ((p_0 \to p_1) \to (\neg p_1 \to \neg p_0))$	(Ex. 2.3)
Hence	$(p_0 \to p_1) \models (\neg p_1 \to \neg p_0)$	by 3.2
Hence	$\{(p_0 \to p_1), \neg p_1\} \models \neg p_0$	by 3.4

3.6 Example

$$\phi \models (\psi \to \phi)$$

Proof. For any v:
if $\widetilde{v}(\phi) = T$ then, by tt $\to$, $\widetilde{v}((\psi \to \phi)) = T$
(no matter what $\widetilde{v}(\psi)$ is). $\square$

4. Logical Equivalence

4.1 Definition
Two formulas ϕ, ψ are **logically equivalent** if $\phi \models \psi$ and $\psi \models \phi$, i.e. if $\widetilde{v}(\phi) = \widetilde{v}(\psi)$ for *every* valuation v.

Notation: $\phi \models\!\!\!=\!\!\!\mid \psi$

Exercise: $\phi \models\!\!\!=\!\!\!\mid \psi$ if and only if $\models (\phi \leftrightarrow \psi)$.

4.2 Lemma

(i) For any formulas ϕ, ψ

$$(\phi \vee \psi) \models\!\!\!=\!\!\!\mid \neg(\neg\phi \wedge \neg\psi).$$

(ii) Hence every formula is logically equivalent to one without '$\vee$'.

Proof. (i) Either use truth tables,
or observe that for any valuation v:

$$\begin{array}{lll} & \widetilde{v}(\neg(\neg\phi \wedge \neg\psi)) = F & \\ \text{iff} & \widetilde{v}((\neg\phi \wedge \neg\psi)) = T & \text{by tt } \neg \\ \text{iff} & \widetilde{v}(\neg\phi) = \widetilde{v}(\neg\psi) = T & \text{by tt } \wedge \\ \text{iff} & \widetilde{v}(\phi) = \widetilde{v}(\psi) = F & \text{by tt } \neg \\ \text{iff} & \widetilde{v}(\phi \vee \psi) = F & \text{by tt } \vee \end{array}$$

(ii) Induction on the length of the formula ϕ.
Clear for length 1.
For the induction step observe that

$$\text{if } \psi \models\!\!\!=\!\!\!| \ \psi' \text{ then } \neg\psi \models\!\!\!=\!\!\!| \ \neg\psi',$$

and $(\phi \vee \psi) \models\!\!\!=\!\!\!| \ \neg(\neg\phi \wedge \neg\psi)$ by (i),
and for $(\phi \star \psi)$ where $\star$ is not $\vee$ observe:

$$\text{if } \phi \models\!\!\!=\!\!\!| \ \phi' \text{ and } \psi \models\!\!\!=\!\!\!| \ \psi' \text{ then}$$
$$(\phi \star \psi) \models\!\!\!=\!\!\!| \ (\phi' \star \psi').$$

$\square$

4.3 Some convenient notation

If $\phi_1, \ldots, \phi_n$ are formulas, we can write their disjunction as

$$(\ldots((\phi_1 \vee \phi_2) \vee \phi_3) \ldots \vee \phi_n).$$

This is rather cumbersome notation, so we abbreviate it to

$$\bigvee_{i=1}^{n} \phi_i.$$

Formally, we make the following recursive definitions:

$$\bigvee_{i=1}^{1} \phi_i = \phi_1 \text{ and } \bigwedge_{i=1}^{1} \phi_i = \phi_1,$$

and for $n > 1$,

$$\bigvee_{i=1}^{n} \phi_i = (\bigvee_{i=1}^{n-1} \vee \phi_n) \text{ and } \bigwedge_{i=1}^{n} \phi_i = (\bigwedge_{i=1}^{n-1} \wedge \phi_n).$$

So $\tilde{v}(\bigvee_{i=1}^{n} \phi_i) = T$ iff for some i, $\tilde{v}(\phi_i) = T$ and $\tilde{v}(\bigwedge_{i=1}^{n} \phi_i) = T$ iff for all i, $\tilde{v}(\phi_i) = T$.

4.4 Some logical equivalences

Let A, B, A_i be formulas. Then

1. $\neg(A \vee B) \models\!\!\!\!=\!\!\!\!\mid (\neg A \wedge \neg B)$
   More generally,
   $$\neg \bigvee_{i=1}^{n} A_i \models\!\!\!\!=\!\!\!\!\mid \bigwedge_{i=1}^{n} \neg A_i,$$
   hence also
   $$\neg \bigwedge_{i=1}^{n} A_i \models\!\!\!\!=\!\!\!\!\mid \bigvee_{i=1}^{n} \neg A_i.$$
   These are called *De Morgan's Laws*.

2. $(A \to B) \models\!\!\!\!=\!\!\!\!\mid (\neg A \vee B)$

3. $(A \leftrightarrow B) \models\!\!\!\!=\!\!\!\!\mid ((A \to B) \wedge (B \to A))$

4. $(A \vee B) \models\!\!\!\!=\!\!\!\!\mid ((A \to B) \to B)$

5. $(\phi \wedge \bigvee_{i=1}^{n} \psi_i) \models\!\!\!\!=\!\!\!\!\mid \bigvee_{i=1}^{n}(\phi \wedge \psi_i)$
   ("$\wedge$ distributes over $\vee$";
   similarly, $\vee$ distributes over $\wedge$.)

5. Adequacy of the Connectives

The connectives $\neg$ (unary) and $\rightarrow, \wedge, \vee, \leftrightarrow$ (binary) are the *logical part* of our language for propositional calculus.

Question:

- Do we have "enough connectives"?
- That is, can we express everything which is logically conceivable using only these connectives?
- More precisely, is every possible truth table implemented by some formula of $\mathcal{L}_{\text{prop}}$?

Answer: yes.

5.1 Definition

(i) We denote by V_n the set of all functions

$$v: \{p_0, \ldots, p_{n-1}\} \to \{T, F\},$$

i.e. "partial" valuations assigning values only to the first n propositional variables. Note $\# V_n = 2^n$.

(ii) An n-**ary truth function** is a function

$$J: V_n \to \{T, F\}.$$

There are precisely 2^{2^n} such functions.

(iii) Let $\mathrm{Form}_n(\mathcal{L}_{\mathrm{prop}})$ be the set of formulas which contain only propositional variables from the set $\{p_0, \ldots, p_{n-1}\}$.

Then any $\phi \in \mathrm{Form}_n(\mathcal{L}_{\mathrm{prop}})$ determines the truth function

$$\begin{array}{rccc} J_\phi: & V_n & \to & \{T, F\} \\ & v & \mapsto & \widetilde{v}(\phi). \end{array}$$

(So J_ϕ corresponds to the truth table for ϕ.)

5.2 Theorem
Our language $\mathcal{L}_{\text{prop}}$ *is* **adequate**,
i.e. for every $n > 0$ *and* every *truth function*
$J : V_n \to \{T, F\}$ *there is some*
$\phi \in \text{Form}_n(\mathcal{L}_{\text{prop}})$ *with* $J_\phi = J$.

Proof: Let $J : V_n \to \{T, F\}$ be any n-ary truth function.

If $J(v) = F$ for all $v \in V_n$ take $\phi := (p_0 \wedge \neg p_0)$.
Then, for all $v \in V_n$: $J_\phi(v) = \tilde{v}(\phi) = F = J(v)$.

Otherwise let $U := \{v \in V_n \mid J(v) = T\} \neq \emptyset$.
For each $v \in U$ and each $i < n$ define the formula

$$\psi_i^v := \begin{cases} p_i & \text{if } v(p_i) = T \\ \neg p_i & \text{if } v(p_i) = F \end{cases}$$

and let $\psi^v := \bigwedge_{i=0}^{n-1} \psi_i^v$.

Then for any valuation $w \in V_n$ one has the following equivalence ($\star$):

$$\begin{array}{lll} \widetilde{w}(\psi^v) = T & \text{iff} & \begin{array}{l}\text{for all } i < n: \\ \widetilde{w}(\psi_i^v) = T\end{array} \qquad \text{(by tt } \wedge\text{)} \\ & \text{iff} & w = v \qquad\qquad\quad \text{(by def. of } \psi_i^v\text{)} \end{array}$$

Now define $\phi := \bigvee_{v \in U} \psi^v$.
Then for any valuation $w \in V_n$:

$$\begin{array}{llll} \widetilde{w}(\phi) = T & \text{iff} & \text{for some } v \in U : \widetilde{w}(\psi^v) = T & \text{(by tt } \vee\text{)} \\ & \text{iff} & \text{for some } v \in U : w = v & \text{(by } (\star)\text{)} \\ & \text{iff} & w \in U & \\ & \text{iff} & J(w) = T & \end{array}$$

Hence $J_\phi(w) = J(w)$ for all $w \in V_n$;
i.e. $J_\phi = J$.

$\square$

5.3 Definition

(i) A formula which is a conjunction of p_i's and $\neg p_i$'s is called a **conjunctive clause** - e.g. ψ^v in the proof of 5.2.

(ii) A formula which is a disjunction of conjunctive clauses is said to be in **disjunctive normal form** (‘**dnf**’) - e.g. ϕ in the proof of 5.2.

So in fact the proof of 5.2 yields the following stronger statement:

5.4 Theorem - 'The dnf-Theorem'
For any truth function

$$J : V_n \to \{T, F\}$$

there is a formula $\phi \in \mathsf{Form}_n(\mathcal{L}_{\mathsf{prop}})$ **in dnf** *with* $J_\phi = J$.

In particular, every formula is logically equivalent to one in dnf.

5.5 Definition
Suppose S is a set of (truth-functional) connectives – so each $s \in S$ is given by some truth table.

(i) Write $\mathcal{L}_{\text{prop}}[S]$ for the language with connectives S instead of $\{\neg, \to, \wedge, \vee, \leftrightarrow\}$ and define $\text{Form}(\mathcal{L}_{\text{prop}}[S])$ and $\text{Form}_n(\mathcal{L}_{\text{prop}}[S])$ accordingly.

(ii) We say that S is **adequate** (or **truth-functionally complete**) if for all $n \geq 1$ and for all n-ary truth functions J there is some $\phi \in \text{Form}_n(\mathcal{L}_{\text{prop}}[S])$ with $J_\phi = J$.

5.6 Examples

1. $S = \{\neg, \wedge, \vee\}$ is adequate, by the dnf-Theorem.

2. Hence, by Lemma 4.2(i), $S = \{\neg, \wedge\}$ is adequate:

$$(\phi \vee \psi) \models\!\!\!=\!\!\!\mid \neg(\neg\phi \wedge \neg\psi)$$

   Similarly, $S = \{\neg, \vee\}$ is adequate:

$$(\phi \wedge \psi) \models\!\!\!=\!\!\!\mid \neg(\neg\phi \vee \neg\psi)$$

3. We can express $\vee$ in terms of $\to$ (4.4.4), so $\{\neg, \to\}$ is adequate.

4. $S = \{\vee, \wedge, \to\}$ is **not** adequate: any $\phi \in \text{Form}(\mathcal{L}_{\text{prop}}[S])$ has T in the top row of tt ϕ, so no such ϕ gives $J_\phi = J_{\neg p_0}$.

5. There are precisely two binary connectives, say $\uparrow$ and $\downarrow$, such that $S = \{\uparrow\}$ and $S = \{\downarrow\}$ are adequate.

6. A deductive system for propositional calculus

- We introduced '*logical consequence*' – $\Gamma \models \phi$ means: whenever (each formula of) Γ is true, so is ϕ.

- But we don't know yet how to give an actual **proof** of ϕ from the **hypotheses** Γ.

- A **proof** of ϕ should be a finite sequence $\phi_1, \phi_2, \ldots, \phi_n$ of statements such that $\phi_n = \phi$, and for each $i = 1, \ldots, n$:

  - either $\phi_i \in \Gamma$,
  - or ϕ_i is some **axiom** (which should *clearly* be true),
  - or ϕ_i should follow from previous ϕ_j's by some **rule of inference**.

6.1 Definition

Let $\mathcal{L}_0 := \mathcal{L}_{\text{prop}}[\{\neg, \to\}]$ (which is an adequate language). Then the **system** L_0 consists of the following axioms and rules:

Axioms

An **axiom** of L_0 is any formula of the following form ($\alpha, \beta, \gamma \in \text{Form}(\mathcal{L}_0)$):

A1 $(\alpha \to (\beta \to \alpha))$

A2 $((\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)))$

A3 $((\neg\beta \to \neg\alpha) \to (\alpha \to \beta))$

Rules of inference

Just one rule, **modus ponens**:

MP For any $\alpha, \beta \in \text{Form}(\mathcal{L}_0)$:
From α and $(\alpha \to \beta)$, infer β.

6.2 Definition

Let $\Gamma \subseteq \text{Form}(\mathcal{L}_0)$.

- A finite sequence $\alpha_1, \ldots, \alpha_m \in \text{Form}(\mathcal{L}_0)$ is a **proof** (or **deduction/derivation**) in L_0 of α_m from the **hypotheses** Γ if for each $i = 1, \ldots, m$, at least one of the following holds:

  (a) α_i is an axiom of L_0.
  (b) $\alpha_i \in \Gamma$.
  (c) α_i follows by MP from earlier formulas, i.e. there are $j, k < i$ such that $\alpha_j = (\alpha_k \to \alpha_i)$.

- $\alpha \in \text{Form}(\mathcal{L}_0)$ is **provable** from Γ if there is a proof $\alpha_1, \ldots, \alpha_m = \alpha$ of α from Γ.

  We denote this by:

$$\Gamma \vdash \alpha.$$

In the case $\Gamma = \emptyset$, we just write

$$\vdash \alpha,$$

and we say that α is a **theorem** (of the system L_0).

6.3 Example For any $\phi \in \text{Form}(\mathcal{L}_0)$

$$(\phi \to \phi)$$

is a theorem of L_0.

Proof:

α_1 $(\phi \to (\phi \to \phi))$
[A1 with $\alpha = \beta = \phi$]
α_2 $(\phi \to ((\phi \to \phi) \to \phi))$
[A1 with $\alpha = \phi$, $\beta = (\phi \to \phi)$]
α_3 $((\phi \to ((\phi \to \phi) \to \phi))$
$\to ((\phi \to (\phi \to \phi)) \to (\phi \to \phi)))$
[A2 with $\alpha = \phi$, $\beta = (\phi \to \phi)$, $\gamma = \phi$]
α_4 $((\phi \to (\phi \to \phi)) \to (\phi \to \phi))$
[MP α_2, α_3]
α_5 $(\phi \to \phi)$
[MP α_1, α_4]

Thus, $\alpha_1, \alpha_2, \ldots, \alpha_5$ is a deduction of $(\phi \to \phi)$ in L_0.

$\square$

6.4 Example

For any $\phi, \psi \in \text{Form}(\mathcal{L}_0)$:

$$\{\phi, \neg\phi\} \vdash \psi$$

Proof:

α_1 $(\neg\phi \to (\neg\psi \to \neg\phi))$
[A1 with $\alpha = \neg\phi, \beta = \neg\psi$]
α_2 $\neg\phi$ [$\in \Gamma$]
α_3 $(\neg\psi \to \neg\phi)$ [MP α_1, α_2]
α_4 $((\neg\psi \to \neg\phi) \to (\phi \to \psi))$
[A3 with $\alpha = \phi, \beta = \psi$]
α_5 $(\phi \to \psi)$ [MP α_3, α_4]
α_6 ϕ [$\in \Gamma$]
α_7 ψ [MP α_5, α_6]

$\square$

6.5 The Soundness Theorem for L_0

L_0 is **sound**, *i.e. for any $\Gamma \subseteq$ Form($\mathcal{L}_0$) and for any $\alpha \in$ Form($\mathcal{L}_0$):*

$$\textit{If } \Gamma \vdash \alpha \textit{ then } \Gamma \models \alpha.$$

In particular, any theorem of L_0 is a tautology.

Proof:
We show by induction on m:

($\star$) If α has a proof of length m from Γ in L_0, then $\Gamma \models \alpha$.

For $m = 0$, there is nothing to prove (no proof has length 0).

So suppose $m \geq 1$ and ($\star$) holds for all $m' < m$, and suppose $\alpha_1, \ldots, \alpha_m$ is a proof in L_0. We have to show that $\Gamma \models \alpha_m$.

Case 1: α_m is an axiom.
One verifies by truth tables (exercise) that our axioms are tautologies, so $\Gamma \models \alpha_m$.

Case 2: $\alpha_m \in \Gamma$.
Then $\Gamma \models \alpha_m$.

Case 3: α_m is obtained by MP.
So say $i, j < m$ and $\alpha_j = (\alpha_i \to \alpha_m)$.

By the inductive hypothesis,
since $\alpha_1, \ldots, \alpha_i$ is a proof of length $i < m$,
we have $\Gamma \models \alpha_i$.
Similarly $\Gamma \models \alpha_j$, i.e. $\Gamma \models (\alpha_i \to \alpha_m)$.

But $\{\alpha_i, (\alpha_i \to \alpha_m)\} \models \alpha_m$ by Lemma 3.4, and it follows (from the definition of $\models$) that $\Gamma \models \alpha_m$.

$\square$

For the proof of the converse

Completeness Theorem

$$\textit{If } \Gamma \models \alpha \textit{ then } \Gamma \vdash \alpha.$$

we first prove

6.6 The Deduction Theorem for L_0

For any $\Gamma \subseteq \mathrm{Form}(\mathcal{L}_0)$ *and*
for any $\alpha, \beta \in \mathrm{Form}(\mathcal{L}_0)$*:*

$$\textit{If } \Gamma \cup \{\alpha\} \vdash \beta \textit{ then } \Gamma \vdash (\alpha \to \beta).$$

6.6 The Deduction Theorem for L_0

For any $\Gamma \subseteq \text{Form}(\mathcal{L}_0)$ *and*
for any $\alpha, \beta \in \text{Form}(\mathcal{L}_0)$*:*

$$\textit{If } \Gamma \cup \{\alpha\} \vdash \beta \textit{ then } \Gamma \vdash (\alpha \to \beta).$$

Proof:
We prove by induction on m:

If $\alpha_1, \ldots, \alpha_m$ *is a proof in* L_0 *from* $\Gamma \cup \{\alpha\}$
then $\Gamma \vdash (\alpha \to \alpha_i)$ *for all* $i \leq m$*.*

For $m = 0$, this holds trivially. So suppose $m > 0$.

IH: Holds for $m - 1$.
Then $\Gamma \vdash (\alpha \to \alpha_i)$ for $i < m$,
and we must show $\Gamma \vdash (\alpha \to \alpha_m)$.

Case 1: α_m is an Axiom
Then $\vdash (\alpha \to \alpha_m)$, indeed:

1	α_m	[Axiom]
2	$(\alpha_m \to (\alpha \to \alpha_m))$	[Instance of A1]
3	$(\alpha \to \alpha_m)$	[MP 1,2]

is a proof of $(\alpha \to \alpha_m)$ from hypotheses $\emptyset$.

Note generally that if $\Delta \vdash \psi$ and $\Delta' \supseteq \Delta$, then also $\Delta' \vdash \psi$.

Thus $\Gamma \vdash (\alpha \to \alpha_m)$.

Case 2: $\alpha_m \in \Gamma \cup \{\alpha\}$
If $\alpha_m \in \Gamma$ then same proof as above works (with justification on line 1 changed to '$\in \Gamma$').

If $\alpha_m = \alpha$, then, by Example 6.3, $\vdash (\alpha \to \alpha_m)$, hence $\Gamma \vdash (\alpha \to \alpha_m)$.

Case 3: α_m is obtained by MP from some earlier α_j, α_k, i.e. there are $j, k < m$ such that $\alpha_j = (\alpha_k \to \alpha_m)$.

By IH, we have

$$\begin{array}{ll} & \Gamma \vdash (\alpha \to \alpha_k) \\ \text{and} & \Gamma \vdash (\alpha \to \alpha_j), \\ \text{i.e.} & \Gamma \vdash (\alpha \to (\alpha_k \to \alpha_m)) \end{array}$$

So say

$$\beta_1, \ldots, \beta_{r-1}, (\alpha \to \alpha_k)$$

and

$$\gamma_1, \ldots, \gamma_{s-1}, (\alpha \to (\alpha_k \to \alpha_m))$$

are proofs in L_0 from Γ.

Then

1	β_1	
⋮	⋮	
r-1	β_{r-1}	
r	$(\alpha \to \alpha_k)$	
r+1	γ_1	
⋮	⋮	
r+s-1	γ_{s-1}	
r+s	$(\alpha \to (\alpha_k \to \alpha_m))$	
r+s+1	$((\alpha \to (\alpha_k \to \alpha_m)) \to$ $((\alpha \to \alpha_k) \to (\alpha \to \alpha_m)))$	[A2]
r+s+2	$((\alpha \to \alpha_k) \to (\alpha \to \alpha_m))$	[MP r+s, r+s+1]
r+s+3	$(\alpha \to \alpha_m)$	[MP r, r+s+2]

is a proof of $(\alpha \to \alpha_m)$ in L_0 from Γ. □

6.7 Remarks

- Only needed instances of A1, A2 and the rule MP.
  So any system that includes A1, A2 and MP satisfies the Deduction Theorem.

- Proof gives a precise **algorithm** for converting any proof showing $\Gamma \cup \{\alpha\} \vdash \beta$ into one showing $\Gamma \vdash (\alpha \to \beta)$.

- Converse is easy:

  If $\Gamma \vdash (\alpha \to \beta)$ then $\Gamma \cup \{\alpha\} \vdash \beta$.

  Proof:

$\vdots$	$\vdots$	proof from Γ
r	$\alpha \to \beta$	
r+1	α	$[\in \Gamma \cup \{\alpha\}]$
r+2	β	[MP r, r+1]

$\square$

6.8 Example of use of DT

If $\Gamma \vdash (\alpha \to \beta)$ and $\Gamma \vdash (\beta \to \gamma)$
then $\Gamma \vdash (\alpha \to \gamma)$.

Proof:

By the deduction theorem ('DT'), it suffices to show that $\Gamma \cup \{\alpha\} \vdash \gamma$.

$\vdots$	$\vdots$	proof from Γ
r	$(\alpha \to \beta)$	
r+1	$\vdots$	
$\vdots$	$\vdots$	proof from Γ
r+s	$(\beta \to \gamma)$	
r+s+1	α	[$\in \Gamma \cup \{\alpha\}$]
r+s+2	β	[MP r, r+s+1]
r+s+3	γ	[MP r+s, r+s+2]

$\square$

From now on we may treat DT as an additional inference rule in L_0.

6.9 Definition
The **sequent calculus** SQ is the system where a **proof** (or **derivation**) of $\phi \in \mathrm{Form}(\mathcal{L}_0)$ from $\Gamma \subseteq \mathrm{Form}(\mathcal{L}_0)$ is a finite sequence of **sequents**,
i.e. expressions of the form

$$\Delta \vdash_{SQ} \psi$$

with $\Delta \subseteq \mathrm{Form}(\mathcal{L}_0)$,
such that $\Gamma \vdash_{SQ} \phi$ is the last sequent,
and each sequent is obtained from previous sequents according to the following rules:

Ass: If $\psi \in \Delta$ then infer $\Delta \vdash_{SQ} \psi$.

MP: From $\Delta \vdash_{SQ} \psi$ and $\Delta' \vdash_{SQ} (\psi \to \chi)$
infer $\Delta \cup \Delta' \vdash_{SQ} \chi$.

DT: From $\Delta \cup \{\psi\} \vdash_{SQ} \chi$
infer $\Delta \vdash_{SQ} (\psi \to \chi)$.

PC: From $\Delta \cup \{\neg\psi\} \vdash_{SQ} \chi$
and $\Delta' \cup \{\neg\psi\} \vdash_{SQ} \neg\chi$,
infer $\Delta \cup \Delta' \vdash_{SQ} \psi$.
('PC' stands for *proof by contradiction*.)

Note: no axioms.

6.10 Example of a proof in SQ

1	$\neg\beta \vdash_{SQ} \neg\beta$	[Ass]
2	$(\neg\beta \to \neg\alpha) \vdash_{SQ} (\neg\beta \to \neg\alpha)$	[Ass]
3	$(\neg\beta \to \neg\alpha), \neg\beta \vdash_{SQ} \neg\alpha$	[MP 1,2]
4	$\alpha, \neg\beta \vdash_{SQ} \alpha$	[Ass]
5	$(\neg\beta \to \neg\alpha), \alpha \vdash_{SQ} \beta$	[PC 3,4]
6	$(\neg\beta \to \neg\alpha) \vdash_{SQ} (\alpha \to \beta)$	[DT 5]
7	$\vdash_{SQ} ((\neg\beta \to \neg\alpha) \to (\alpha \to \beta))$	[DT 6]

So $\vdash_{SQ}$ A3.

Notation: To avoid confusion, we sometimes write '$\Gamma \vdash_{L_0} \phi$' for '$\Gamma \vdash \phi$ in L_0'

6.11 Theorem

L_0 and SQ are equivalent, i.e. for all Γ, ϕ:

$$\Gamma \vdash_{L_0} \phi \textit{ iff } \Gamma \vdash_{SQ} \phi.$$

Proof: Omitted

The following lemma is a key step in the proof of 6.11; it shows that L_0 implements the rule (PC) of the sequence calculus. It is the only place in the proof of the completeness theorem where (A3) is used.

6.12 Lemma
For any $\alpha, \beta \in \text{Form}(L_0)$,

$$\vdash ((\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)).$$

Proof: Omitted.

7. Consistency, Completeness and Compactness

7.1 Definition
$\Gamma \subseteq \text{Form}(\mathcal{L}_0)$ is **inconsistent**
if for some formula α,
$\Gamma \vdash \alpha$ and $\Gamma \vdash \neg\alpha$.

Otherwise, Γ is **consistent**.

E.g. $\emptyset$ is consistent by soundness of $\mathcal{L}_0$, since for no α are both α and $\neg\alpha$ tautologies.

7.2. Lemma
If $\Gamma \nvdash \phi$ then $\Gamma \cup \{\neg\phi\}$ is consistent.

Proof: Suppose $\Gamma \cup \{\neg\phi\}$ is inconsistent, say $\Gamma \cup \{\neg\phi\} \vdash \alpha$ and $\Gamma \cup \{\neg\phi\} \vdash \neg\alpha$.

Then by the deduction theorem,
$\Gamma \vdash (\neg\phi \to \alpha)$ and $\Gamma \vdash (\neg\phi \to \neg\alpha)$.

By 6.12 and MP twice, $\Gamma \vdash \phi$.

□

7.3 Lemma

Suppose Γ *is consistent and* $\Gamma \vdash \phi$.
Then $\Gamma \cup \{\phi\}$ *is consistent.*

Proof: Suppose not. Then for some α

$$\left.\begin{array}{l}\Gamma \cup \{\phi\} \vdash \alpha \\ \Gamma \cup \{\phi\} \vdash \neg\alpha\end{array}\right\} \Rightarrow_{\mathrm{DT}} \begin{array}{l}\Gamma \vdash (\phi \to \alpha) \\ \Gamma \vdash (\phi \to \neg\alpha)\end{array}$$

$$\overset{\Gamma\vdash\phi}{\Rightarrow}_{\mathrm{MP}} \begin{array}{l}\Gamma \vdash \alpha \\ \Gamma \vdash \neg\alpha\end{array},$$

contradicting consistency of Γ.

$\square$

7.4 Definition

$\Gamma \subseteq \mathrm{Form}(\mathcal{L}_0)$ is **maximal consistent** if
(i) Γ is consistent, and
(ii) for *every* ϕ, either $\Gamma \vdash \phi$ or $\Gamma \vdash \neg\phi$.

7.5 Theorem

Suppose Γ *is consistent. Then there is a maximal consistent* $\Gamma' \supseteq \Gamma$.

Proof:

Form($\mathcal{L}_0$) is countable, say

$$\text{Form}(\mathcal{L}_0) = \{\phi_1, \phi_2, \phi_3, \ldots\}.$$

Construct consistent sets

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \ldots$$

as follows:

- $\Gamma_0 := \Gamma$.
- Given consistent Γ_n, let

  $$\Gamma_{n+1} := \begin{cases} \Gamma_n \cup \{\phi_{n+1}\} & \text{if } \Gamma_n \vdash \phi_{n+1} \\ \Gamma_n \cup \{\neg\phi_{n+1}\} & \text{if } \Gamma_n \nvdash \phi_{n+1} \end{cases}$$

  Then Γ_{n+1} is consistent by 7.3 and 7.2.

Now let $\Gamma' := \bigcup_{n=0}^{\infty} \Gamma_n$.

Then Γ' is consistent:

Any proof of $\Gamma' \vdash \alpha$ and $\Gamma' \vdash \neg\alpha$ would use only finitely many formulas from Γ', so for some n, $\Gamma_n \vdash \alpha$ and $\Gamma_n \vdash \neg\alpha$ – contradicting the consistency of Γ_n.

Finally, Γ' is maximal consistent: for all n, either $\phi_n \in \Gamma'$ or $\neg\phi_n \in \Gamma'$,
so in particular either $\Gamma' \vdash \phi_n$ or $\Gamma' \vdash \neg\phi_n$.

$\square$

(Note that this proof did not use Zorn's Lemma; countability of the language was crucial for this.)

7.6 Lemma
Suppose Γ is maximal consistent.
Then for every $\psi, \chi \in \mathrm{Form}(\mathcal{L}_0)$:
(a) $\Gamma \vdash \neg\psi$ iff $\Gamma \nvdash \psi$.
(b) $\Gamma \vdash (\psi \to \chi)$ iff either $\Gamma \nvdash \psi$ or $\Gamma \vdash \chi$.

Proof:

(a) **'$\Rightarrow$':** by consistency.
'$\Leftarrow$': by maximality.

(b) **'$\Rightarrow$':** Suppose $\Gamma \vdash (\psi \to \chi)$ but $\Gamma \vdash \psi$ and $\Gamma \nvdash \chi$.
By MP, $\Gamma \vdash \chi$, contradicting consistency.

'$\Leftarrow$': Suppose $\Gamma \nvdash \psi$. Then $\Gamma \vdash \neg\psi$ by (a).
$\Gamma \vdash (\neg\psi \to (\psi \to \chi))$ (Problem sheet 2 Q3)
$\Rightarrow_{\mathrm{MP}} \Gamma \vdash (\psi \to \chi)$.

Suppose $\Gamma \vdash \chi$.
$\Gamma \vdash (\chi \to (\psi \to \chi))$ (Axiom A1)
$\Rightarrow_{\mathrm{MP}} \Gamma \vdash (\psi \to \chi)$.

$\square$

7.7 Theorem

Suppose Γ *is maximal consistent.*
Then Γ *is satisfiable.*

Proof:

Define a valuation v by

$$v(p_i) = T \text{ iff } \Gamma \vdash p_i.$$

Claim: for all $\phi \in \text{Form}(\mathcal{L}_0)$:

$$\widetilde{v}(\phi) = T \text{ iff } \Gamma \vdash \phi.$$

Proof by induction on the length n of ϕ.

If $n = 1$, then $\phi = p_i$ for some i and we are done by the definition of v.

Suppose $n = \text{length}(\phi) > 1$.
IH: Claim true for all $n' < n$.

Case 1: $\phi = \neg\psi$

$$\begin{array}{llll} \tilde{v}(\phi) = T & \text{iff} & \tilde{v}(\psi) = F & \text{tt } \neg \\ & \text{iff} & \Gamma \nvdash \psi & \text{IH} \\ & \text{iff} & \Gamma \vdash \neg\psi & \text{7.6(a)} \\ & \text{iff} & \Gamma \vdash \phi & \end{array}$$

Case 2: $\phi = (\psi \to \chi)$

$$\begin{array}{llll} \tilde{v}(\phi) = T & \text{iff} & \tilde{v}(\psi) = F \text{ or } \tilde{v}(\chi) = T & \text{tt } \to \\ & \text{iff} & \Gamma \nvdash \psi \text{ or } \Gamma \vdash \chi & \text{IH} \\ & \text{iff} & \Gamma \vdash (\psi \to \chi) & \text{7.6(b)} \\ & \text{iff} & \Gamma \vdash \phi & \end{array}$$

So $\tilde{v}(\phi) = T$ for all $\phi \in \Gamma$, i.e. v satisfies Γ.

$\square$

7.8 Corollary
Let $\Gamma \subseteq \mathrm{Form}(\mathcal{L}_0)$. Then
Γ *is consistent if and only if* Γ *is satisfiable.*

Proof:

$\Rightarrow$: By 7.5 + 7.7:
If Γ is consistent,
then by 7.5 it extends to a maximal consistent set,
which by 7.7 is satisfiable,
hence also Γ is satisfiable.

$\Leftarrow$: By soundness:
Suppose Γ inconsistent,
say $\Gamma \vdash \alpha$ and $\Gamma \vdash \neg\alpha$.
Then $\Gamma \models \alpha$ and $\Gamma \models \neg\alpha$ by soundness,
so Γ is not satisfiable.

$\square$

7.9 The Completeness Theorem

If $\Gamma \models \phi$ *then* $\Gamma \vdash \phi$.

Proof:

Suppose $\Gamma \nvdash \phi$.

$\Rightarrow$ by 7.2, $\Gamma \cup \{\neg\phi\}$ is consistent
$\Rightarrow$ by 7.8, $\Gamma \cup \{\neg\phi\}$ is satisfiable
$\Rightarrow$ there is some valuation v such that
$\tilde{v}(\psi) = T$ for $\psi \in \Gamma$, but $\tilde{v}(\phi) = F$
$\Rightarrow \Gamma \not\models \phi$. $\square$

7.10 Corollary

(7.9 Completeness + 6.5 Soundness)

$$\Gamma \models \phi \text{ iff } \Gamma \vdash \phi$$

7.11 The Compactness Theorem for $\mathcal{L}_0$

$\Gamma \subseteq \mathrm{Form}(\mathcal{L}_0)$ *is satisfiable iff every finite subset of* Γ *is satisfiable.*

Proof: By 7.8, this is equivalent to:
$\Gamma \subseteq \mathrm{Form}(\mathcal{L}_0)$ *is consistent iff every finite subset of* Γ *is consistent.*

But indeed, by finiteness of proofs,
$\Gamma \vdash \alpha$ and $\Gamma \vdash \neg\alpha$ iff already
$\Gamma_0 \vdash \alpha$ and $\Gamma_0 \vdash \neg\alpha$ for some finite $\Gamma_0 \subseteq \Gamma$.

$\square$

PART II: PREDICATE CALCULUS

So far:

- *Logic of the connectives* $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \ldots$ (as used in mathematics).
- Logical validity in terms of truth tables.
- Found axioms and rule of inference yielding a sound and complete proof system. Deduced compactness.

Now:

- Look *more deeply into* the structure of propositions used in mathematics.
- Analyse grammatically correct use of *functions, relations, constants, variables* and *quantifiers*.
- Define *logical validity* in this refined language.
- Isolate *axioms* and *rules of inference* (beyond those of propositional calculus) used in mathematical arguments.
- Prove: soundness, completeness, compactness.

8. The language of (first-order) predicate calculus

A **countable first-order language** $\mathcal{L}$ consists of the following disjoint sets:

- for each $k \geq 1$, a countable set of k-ary *predicate* (or *relation*) *symbols*;
- for each $k \geq 1$, a countable set of k-ary *function symbols*;
- a countable set of constant symbols.

These symbols are called the **non-logical symbols** of $\mathcal{L}$.

The alphabet of $\mathcal{L}$ consists of its non-logical symbols along with the following disjoint set of **logical symbols**:

- *Connectives:* $\rightarrow, \neg$
- *Quantifier:* $\forall$ ('for all')
- *Variables:* $x_0, x_1, x_2, \ldots$
- *3 punctuation marks:* , ( )
- *Equality symbol:* $\doteq$

8.1 Definition

(a) The **terms** of $\mathcal{L}$ are defined recursively as follows:

 (i) Every variable is a term.

 (ii) Every constant symbol is a term.

 (iii) If f is a k-ary function symbol, and $t_1, \ldots, t_k$ are terms, then so is the string

$$f(t_1, \ldots, t_k).$$

(b) An **atomic formula** of $\mathcal{L}$ is any string of the form

$$P(t_1, \ldots, t_k) \text{ or } t_1 \doteq t_2$$

where $k \geq 1$, $P \in \mathcal{L}$ is a k-ary relation symbol, and all t_i are terms.

(c) The **formulas** of $\mathcal{L}$ are defined recursively as follows:

 (i) Any atomic formula is a formula.

 (ii) If ϕ, ψ are formulas, then so are $\neg\phi$ and $(\phi \to \psi)$.

 (iii) If ϕ is a formula, then for any variable x_i so is $\forall x_i \phi$.

8.2 Examples The most general countable language has a countably infinite set of symbols of each type:

$$\mathcal{L}_{\text{pred}} := \{(P_i^{(k)})_{i,k>0}, (f_i^{(k)})_{i,k>0}, (c_i)_{i>0}\},$$

where each $P_i^{(k)}$ is a k-ary predicate symbol, each $f_i^{(k)}$ is a k-ary function symbol, and each c_i is a constant symbol.

- The following are all $\mathcal{L}_{\text{pred}}$-terms:

  $$c_3 \quad x_5 \quad f_3^{(1)}(c_2) \quad f_1^{(2)}(x_1, f_1^{(1)}(c_{37}))$$

- $f_2^{(3)}(x_1, x_2)$ is *not* a term (wrong arity).
- $P_2^{(3)}(x_4, c_2, f_3^{(2)}(c_1, x_2))$ and $f_1^{(2)}(c_5, x_2) \doteq x_3$ are atomic formulas.
- $\forall x_1 f_2^{(2)}(x_1, c_7) \doteq x_2$ and $\forall x_2 P_1^{(1)}(x_3)$ are non-atomic formulas.

8.3 Exercise
We have **unique readability** for terms, for atomic formulas, and for formulas.

A more typical example of a language appearing in mathematics is

$$\mathcal{L}_{\text{o.ring}} := \{<, \cdot, +, -, \overline{0}, \overline{1}\},$$

where $<$ is a binary relation symbol, $\cdot$, $+$, and $-$ are binary function symbols, and $\overline{0}$ and $\overline{1}$ are constant symbols. We call this the *language of ordered rings*.

When dealing with binary symbols, we will allow ourselves to use infix notation as an abbreviation, so e.g.

$$\forall x_0\; x_0 < x_0 + \overline{1}$$

abbreviates the $\mathcal{L}_{\text{o.ring}}$-formula

$$\forall x_0 <\!(x_0, +(x_0, \overline{1})).$$

8.4 Interpretations and logical validity
(Informal discussion)

- Consider the following $\{f\}$-formula, with f a unary function symbol:

  $$\phi_1 : \ \forall x_1 \forall x_2 (x_1 \doteq x_2 \to f(x_1) \doteq f(x_2)).$$

  Interpreting $\doteq$ as equality, $\forall$ as 'for all', and f as some unary function, ϕ_1 *should always be true*. We write

  $$\models \phi_1$$

  and say 'ϕ_1 is **logically valid**'.

- Consider the following $\{g\}$-formula, with g a binary function symbol:

  $$\phi_2 : \ \forall x_1 \forall x_2 (g(x_1, x_2) \doteq g(x_2, x_1) \to x_1 \doteq x_2)$$

  Then ϕ_2 may be true or false, depending on the situation:

- If we interpret g as $+$ on $\mathbb{N}$, then ϕ_2 becomes false, since e.g. 1+2=2+1, but $1 \neq 2$.

  So in this *interpretation*, ϕ_2 is false and $\neg\phi_2$ is true. Write

$$\langle \mathbb{N}; + \rangle \models \neg\phi_2$$

- If we interpret g as subtraction on $\mathbb{R}$, then ϕ_2 becomes true: if $x_1 - x_2 = x_2 - x_1$, then $2x_1 = 2x_2$, and hence $x_1 = x_2$. So

$$\langle \mathbb{R}; - \rangle \models \phi_2$$

8.5 Free and bound variables
(Informal discussion)

There is a further complication: Consider the $\{P\}$-formula

$$\phi_3 : \ \forall x_0 P(x_1, x_0).$$

Specifying the interpretation is not enough to determine whether or not ϕ_3 holds.

For example, in $\langle \mathbb{N}; \leq \rangle$:
- If we put $x_1 = 0$ then ϕ_3 is true;
- if we put $x_1 = 2$ then ϕ_3 is false.

So it depends on the value we assign to x_1 (like in propositional calculus: the truth value of $(p_0 \wedge p_1)$ depends on the valuation).

In ϕ_3 we *can* assign a value to x_1 because x_1 occurs **free** in ϕ_3.

For x_0, however, it makes no sense to assign a particular value; because x_0 is **bound** in ϕ_3 by the quantifier $\forall x_0$.

9. Interpretations and Assignments

9.1 Definition

Let $\mathcal{L}$ be a language. An **interpretation** of $\mathcal{L}$ is an $\mathcal{L}$-**structure**

$$\mathcal{A} := \langle A; (f^{\mathcal{A}})_{f \in \mathsf{Fct}(\mathcal{L})}, (P^{\mathcal{A}})_{P \in \mathsf{Pred}(\mathcal{L})}, (c^{\mathcal{A}})_{c \in \mathsf{Const}(\mathcal{L})} \rangle,$$

where:

- A is a <u>non-empty</u> set, the **domain** of $\mathcal{A}$;
- For $f \in \mathcal{L}$ a k-ary function symbol, $f^{\mathcal{A}} : A^k \to A$ is a k-ary function;
- For $P \in \mathcal{L}$ a k-ary predicate symbol, $P^{\mathcal{A}}$ is a k-ary relation on A, i.e. $P^{\mathcal{A}} \subseteq A^k$;
- For $c \in \mathcal{L}$ a constant symbol, $c^{\mathcal{A}} \in A$.

9.2 Definition

Let $\mathcal{L}$ be a language and let $\mathcal{A} = \langle A; \ldots \rangle$ be an $\mathcal{L}$-structure.

(1) An **assignment** in $\mathcal{A}$ is a function

$$v : \{x_0, x_1, \ldots\} \to A$$

(2) v determines an assignment

$$\widetilde{v} = \widetilde{v}^{\mathcal{A}} : \text{Terms}(\mathcal{L}) \to A$$

defined recursively as follows:

(i) $\widetilde{v}(x_i) := v(x_i)$ for all $i = 0, 1, \ldots$;

(ii) $\widetilde{v}(c) := c^{\mathcal{A}}$ for each constant symbol $c \in \mathcal{L}$;

(iii) $\widetilde{v}(f(t_1, \ldots, t_k)) := f^{\mathcal{A}}(\widetilde{v}(t_1), \ldots, \widetilde{v}(t_k))$ for each k-ary function symbol $f \in \mathcal{L}$.

(3) v determines a **valuation**

$$\widetilde{v} = \widetilde{v}^{\mathcal{A}} : \text{Form}(\mathcal{L}) \to \{T, F\}$$

as follows:

Define $\widetilde{v}$ on formulas recursively:

- On atomic formulas:
  - For each k-ary predicate symbol $P \in \mathcal{L}$ and for all $t_i \in \text{Term}(\mathcal{L})$:

$$\widetilde{v}(P(t_1, \ldots, t_k)) = \begin{cases} T & \text{if } (\widetilde{v}(t_1), \ldots, \widetilde{v}(t_k)) \in P^{\mathcal{A}} \\ F & \text{otherwise.} \end{cases}$$

  - For all $t_1, t_2 \in \text{Term}(\mathcal{L})$:

$$\widetilde{v}(t_1 \doteq t_2) = \begin{cases} T & \text{if } \widetilde{v}(t_1) = \widetilde{v}(t_2) \\ F & \text{otherwise.} \end{cases}$$

- $\widetilde{v}(\neg\psi) = T$ iff $\widetilde{v}(\psi) = F$
- $\widetilde{v}(\psi \to \chi) = T$ iff $\widetilde{v}(\psi) = F$ or $\widetilde{v}(\chi) = T$
- $\widetilde{v}(\forall x_i \psi) = T$ iff $\widetilde{v}^{\star}(\psi) = T$ for all assignments $v^{\star}$ agreeing with v except possibly at x_i.

Notation: Write $\mathcal{A} \models \phi[v]$ for $\widetilde{v}^{\mathcal{A}}(\phi) = T$, read '$\phi$ *is true in* $\mathcal{A}$ *under the assignment* v'.

9.3 Example
Consider $\mathcal{A} = \langle \mathbb{Z}; \cdot \rangle$ as an $\{f\}$-structure (f a binary function symbol). Let v be the assignment $v(x_i) = i (\in \mathbb{Z})$ for $i = 0, 1, \ldots$, and let

$$\phi = \forall x_0 \forall x_1 (f(x_0, x_2) \doteq f(x_1, x_2) \to x_0 \doteq x_1)$$

Then $\mathcal{A} \models \phi[v]$; indeed:

$$\begin{array}{ll} & \mathcal{A} \models \phi[v] \\ \text{iff} & \text{for all } v^\star \text{ with } v^\star(x_i) = i \text{ for } i \neq 0 \\ & \mathcal{A} \models \forall x_1 (f(x_0, x_2) \doteq f(x_1, x_2) \to x_0 \doteq x_1)[v^\star] \\ \text{iff} & \text{for all } v^{\star\star} \text{ with } v^{\star\star}(x_i) = i \text{ for } i \neq 0, 1 \\ & \mathcal{A} \models (f(x_0, x_2) \doteq f(x_1, x_2) \to x_0 \doteq x_1)[v^{\star\star}] \\ \text{iff} & \text{for all } v^{\star\star} \text{ with } v^{\star\star}(x_i) = i \text{ for } i \neq 0, 1 \\ & v^{\star\star}(x_0) \cdot v^{\star\star}(x_2) = v^{\star\star}(x_1) \cdot v^{\star\star}(x_2) \\ & \text{implies } v^{\star\star}(x_0) = v^{\star\star}(x_1) \\ \text{iff} & \text{for all } a, b \in \mathbb{Z},\ a \cdot 2 = b \cdot 2 \text{ implies } a = b, \\ & \text{which is true.} \end{array}$$

However, with $v'(x_i) = 0$ for all i, we would have finished with
... iff for all $a, b \in \mathbb{Z}$, $a \cdot 0 = b \cdot 0$ implies $a = b$, which is false. So $\mathcal{A} \not\models \phi[v']$.

9.4 Example

Let P be a unary predicate symbol, $\mathcal{L} = \{P\}$, $\mathcal{A}$ an $\mathcal{L}$-structure,

$$\phi = (\forall x_0 P(x_0) \to P(x_1)),$$

and v any assignment in $\mathcal{A}$. Then $\mathcal{A} \models \phi[v]$.

Proof:
$\mathcal{A} \models \phi[v]$ iff
$\mathcal{A} \models \forall x_0 P(x_0)[v]$ implies $\mathcal{A} \models P(x_1)[v]$.

Now suppose $\mathcal{A} \models \forall x_0 P(x_0)[v]$. Then for all $v^\star$ which agree with v except possibly at x_0, $\mathcal{A} \models P(x_0)[v^\star]$.

In particular, for $v^\star(x_i) = \begin{cases} v(x_i) & \text{if } i \neq 0 \\ v(x_1) & \text{if } i = 0 \end{cases}$
we have $P^{\mathcal{A}}(v^\star(x_0))$, and hence $v(x_1) \in P^{\mathcal{A}}$, i.e. $\mathcal{A} \models P(x_1)[v]$. $\square$

9.5 Definition
Let $\mathcal{L}$ be a language.

- An $\mathcal{L}$-formula ϕ is **logically valid** ('$\models \phi$') if $\mathcal{A} \models \phi[v]$ for *all* $\mathcal{L}$-structures $\mathcal{A}$ and for *all* assignments v in $\mathcal{A}$.

- $\phi \in \text{Form}(\mathcal{L})$ is **satisfiable** if $\mathcal{A} \models \phi[v]$ for *some* $\mathcal{L}$-structure $\mathcal{A}$ and for *some* assignment v in $\mathcal{A}$.

- For $\Gamma \subseteq \text{Form}(\mathcal{L})$ and $\phi \in \text{Form}(\mathcal{L})$, ϕ is a **logical consequence** of Γ, written $\Gamma \models \phi$, if for *all* $\mathcal{L}$-structures $\mathcal{A}$ and for *all* assignments v in $\mathcal{A}$ with $\mathcal{A} \models \psi[v]$ for all $\psi \in \Gamma$, also $\mathcal{A} \models \phi[v]$.

- $\phi, \psi \in \text{Form}(\mathcal{L})$ are **logically equivalent** if $\{\phi\} \models \psi$ and $\{\psi\} \models \phi$.

Example: $\models \phi$ for ϕ from Example 9.4.

Note:
The symbol '$\models$' is now used in two ways:

- $\Gamma \models \phi$ means: ϕ is a logical consequence of Γ.

- $\mathcal{A} \models \phi[v]$ means: ϕ is satisfied in the $\mathcal{L}$-structure $\mathcal{A}$ under the assignment v.

This shouldn't give rise to confusion, since it will always be clear from the context whether there is a set Γ of $\mathcal{L}$-formulas or an $\mathcal{L}$-structure $\mathcal{A}$ in front of '$\models$'.

9.6 Some abbreviations

We use ...	as abbreviation for ...
$(\alpha \vee \beta)$	$((\alpha \to \beta) \to \beta)$
$(\alpha \wedge \beta)$	$\neg(\neg\alpha \vee \neg\beta)$
$(\alpha \leftrightarrow \beta)$	$((\alpha \to \beta) \wedge (\beta \to \alpha))$
$\exists x_i \phi$	$\neg\forall x_i \neg\phi$

9.7 Lemma

For any $\mathcal{L}$-structure $\mathcal{A}$ and any assignment v in $\mathcal{A}$ one has

$$\begin{array}{rll} \mathcal{A} \models (\alpha \vee \beta)[v] & \text{iff} & \mathcal{A} \models \alpha[v] \text{ or } \mathcal{A} \models \beta[v] \\ \mathcal{A} \models (\alpha \wedge \beta)[v] & \text{iff} & \mathcal{A} \models \alpha[v] \text{ and } \mathcal{A} \models \beta[v] \\ \mathcal{A} \models (\alpha \leftrightarrow \beta)[v] & \text{iff} & \widetilde{v}(\alpha) = \widetilde{v}(\beta) \\ \mathcal{A} \models \exists x_i \phi[v] & \text{iff} & \text{for some assignment} \\ & & v^\star \text{ agreeing with } v \\ & & \text{except possibly at } x_i \\ & & \mathcal{A} \models \phi[v^\star] \end{array}$$

Proof: Easy exercise.

10. Free and bound variables

Recall Example 9.3: The formula

$$\phi = \forall x_0 \forall x_1 (f(x_0, x_2) \doteq f(x_1, x_2) \rightarrow x_0 \doteq x_1)$$

- is true in $\langle \mathbb{Z}; \cdot \rangle$ under any assignment v with $v(x_2) = 2$,
- but false when $v(x_2) = 0$.

Whether or not $\mathcal{A} \models \phi[v]$ depends on $v(x_2)$ but not on $v(x_0)$ or $v(x_1)$.

This is because all occurrences of x_0 and x_1 in ϕ are subordinate to the corresponding quantifiers $\forall x_0$ and $\forall x_1$.
We say that these occurrences are **bound**, while the occurrence of x_2 is **free**.

10.1 Definition
Let $\mathcal{L}$ be a first-order language, ϕ an $\mathcal{L}$-formula, and $x \in \{x_0, x_1, \ldots\}$ a variable.

An occurrence of x in ϕ is **free**, if
(i) ϕ is atomic; or
(ii) $\phi = \neg\psi$ resp. $\phi = (\chi \to \rho)$, and the occurrence of x is free in ψ resp. in χ or in ρ; or
(iii) $\phi = \forall x_i \psi$, and $x \neq x_i$, and the occurrence of x is free in ψ.

The variables which occur free in ϕ are called the **free variables of** ϕ,
Free(ϕ) := $\{x_i : x_i$ occurs free in $\phi\}$.

An occurrence which is not free is **bound**.
In particular, if $\phi = \forall x_i \psi$, then any occurrence of x_i in ϕ is bound.

10.2 Example

$$(\exists x_0 P(\underbrace{x_0}_{bnd}, \underbrace{x_1}_{free}) \vee \forall x_1 (P(\underbrace{x_0}_{free}, \underbrace{x_1}_{bnd}) \to \exists x_0 P(\underbrace{x_0}_{bnd}, \underbrace{x_1}_{bnd})))$$

10.3 Lemma

Let $\mathcal{L}$ be a language, let $\mathcal{A}$ be an $\mathcal{L}$-structure, let v_1, v_2 be assignments in $\mathcal{A}$, and let ϕ be an $\mathcal{L}$-formula.

Suppose $v_1(x_i) = v_2(x_i)$ for every variable x_i with a free *occurrence in ϕ.*

Then

$$\mathcal{A} \models \phi[v_1] \text{ iff } \mathcal{A} \models \phi[v_2].$$

Proof:
For ϕ atomic: exercise.

Now use induction on the length of ϕ.
If $\phi = \neg\psi$ or $\phi = (\chi \to \rho)$, this is straightforward.

So say $\phi = \forall x_i \psi$.
IH: Assume the Lemma holds for ψ.

Suppose $\mathcal{A} \models \forall x_i \psi[v_1]$. $(\star)$
We want to show $\mathcal{A} \models \forall x_i \psi[v_2]$. So suppose $v_2^\star$ agrees with v_2 except possibly at x_i;
we want to show $\mathcal{A} \models \psi[v_2^\star]$.

Let $v_1^\star(x_j) := \begin{cases} v_1(x_j) & \text{if } j \neq i \\ v_2^\star(x_i) & \text{if } j = i \end{cases}$
Then $v_1^\star$ agrees with v_1 except possibly at x_i.
So by $(\star)$, $\mathcal{A} \models \psi[v_1^\star]$.

Now suppose x_j occurs free in ψ.
We show $v_2^\star(x_j) = v_1^\star(x_j)$.
If $j = i$, this is by definition of $v_1^\star$.
If $j \neq i$, then x_j occurs free in ϕ, so

$$v_2^\star(x_j) = v_2(x_j) = v_1(x_j) = v_1^\star(x_j).$$

So by IH, $\mathcal{A} \models \psi[v_2^\star]$, as required

$\square$

10.4 Corollary
Let $\mathcal{L}$ be a language, and let $\alpha, \beta \in \text{Form}(\mathcal{L})$. Assume the variable x_i has no free occurrence in α (i.e. $x_i \notin \text{Free}(\alpha)$). Then

$$\models (\forall x_i(\alpha \to \beta) \to (\alpha \to \forall x_i \beta)).$$

Proof:
Let $\mathcal{A}$ be an $\mathcal{L}$-structure and let v be an assignment in $\mathcal{A}$ such that
$\mathcal{A} \models \forall x_i(\alpha \to \beta)[v]$. $(\star)$

To show: $\mathcal{A} \models (\alpha \to \forall x_i \beta)[v]$.

So suppose $\mathcal{A} \models \alpha[v]$.
To show: $\mathcal{A} \models \forall x_i \beta[v]$.

So let $v^\star$ be an assignment agreeing with v except possibly at x_i.
To show: $\mathcal{A} \models \beta[v^\star]$.

x_i is *not* free in $\alpha \Rightarrow_{10.3} \mathcal{A} \models \alpha[v^\star]$
$(\star) \Rightarrow \mathcal{A} \models (\alpha \to \beta)[v^\star]$
$\Rightarrow \mathcal{A} \models \beta[v^\star]$. $\square$

10.5 Definition
A formula σ with no free (occurrences of) variables is called a **statement** or a **sentence**.

Then (by 10.3) for any $\mathcal{L}$-structure $\mathcal{A}$, whether or not $\mathcal{A} \models \sigma[v]$ does not depend on the choice of assignment v.

So we write

$$\mathcal{A} \models \sigma$$

if $\mathcal{A} \models \sigma[v]$ for some/all v.

Say: σ is **true** in $\mathcal{A}$, or $\mathcal{A}$ is a **model** of σ.

($\rightsquigarrow$ 'Model Theory')

10.6 Example
Let $\mathcal{L} = \{f, c\}$ be a language, where f is a binary function symbol, and c is a constant symbol.

Consider the sentences (writing x, y, z for x_0, x_1, x_2)

$$\begin{aligned}
\sigma_1 &: \ \forall x \forall y \forall z f(x, f(y, z)) \doteq f(f(x, y), z) \\
\sigma_2 &: \ \forall x \exists y (f(x, y) \doteq c \wedge f(y, x) \doteq c) \\
\sigma_3 &: \ \forall x (f(x, c) \doteq x \wedge f(c, x) \doteq x)
\end{aligned}$$

and let $\sigma = (\sigma_1 \wedge \sigma_2 \wedge \sigma_3)$

Let $\mathcal{A} = \langle A; \cdot, e \rangle$ be an $\mathcal{L}$-structure (i.e. $\cdot$ is an interpretation of f, and e is an interpretation of c).

Then $\mathcal{A} \models \sigma$ iff $\mathcal{A}$ is a group.

10.7 Example

Let $\mathcal{L} = \{E\}$ with E a binary relation symbol. Consider

$$\begin{aligned} \tau_1 &: \ \forall x E(x,x) \\ \tau_2 &: \ \forall x \forall y (E(x,y) \leftrightarrow E(y,x)) \\ \tau_3 &: \ \forall x \forall y \forall z (E(x,y) \to (E(y,z) \to E(x,z))) \end{aligned}$$

Then for any $\mathcal{L}$-structure $\langle A; R \rangle$:
$\langle A; R \rangle \models \bigwedge_i \tau_i$ iff R is an equivalence relation on A.

Note: Many mathematical concepts can be naturally expressed by first-order formulas.

10.8 Example
Let $<$ be a binary predicate symbol, $\mathcal{L} := \{<\}$. Consider the sentence

$$\begin{aligned}\sigma := \forall x \forall y \forall z\ (\neg x < x \\ &\wedge (x < y \vee x \doteq y \vee y < x) \\ &\wedge ((x < y \wedge y < z) \to x < z) \\ &\wedge (x < y \to \exists w\ (x < w \wedge w < y)) \\ &\wedge \exists w\ w < x \\ &\wedge \exists w\ x < w).\end{aligned}$$

This axiomatises a **dense linear order without endpoints**. In particular, $\langle \mathbb{Q}; < \rangle \models \sigma$ and $\langle \mathbb{R}; < \rangle \models \sigma$.

But: *'Completeness'* of $\langle \mathbb{R}; < \rangle$ is not captured by the first-order language $\mathcal{L}$, but rather in *second-order* terms, meaning that we also allow quantification over *subsets* of $\mathbb{R}$:

$$\forall A, B \subseteq \mathbb{R}(A < B \to \exists c \in \mathbb{R}(A \leq \{c\} \leq B)),$$

writing $A < B$ to mean that $a < b$ for every $a \in A$ and every $b \in B$, similarly for $A \leq B$.

11. Substitution

Discussion: Let $\mathcal{A}$ be an $\mathcal{L}$-structure, $\phi \in \text{Form}(\mathcal{L})$, and suppose $\mathcal{A} \models \forall x_i \phi$. If c is a constant symbol in $\mathcal{L}$, then $\mathcal{A} \models \phi[c/x_i]$ where $\phi[c/x_i]$ is the result of replacing each free instance of x_i in ϕ with c.

We would like to say more generally that

$$\models \forall x_i \phi \rightarrow \phi[t/x_i]$$

for a term t, but we have to be careful:

11.1 Example
Let $\mathcal{L}$ contain a constant symbol c, and let $\phi := \exists x_0 \neg x_0 \doteq x_1$.

Then $\mathcal{A} \models \forall x_1 \phi$ for any $\mathcal{L}$-structure $\mathcal{A}$ with at least two elements,
and then also $\mathcal{A} \models \phi[c/x_1] = \exists x_0 \neg x_0 \doteq c$.

However, if were to define $\phi[x_0/x_1]$ in the same way, we would obtain $\exists x_0 \neg x_0 \doteq x_0$, which does not hold in any $\mathcal{A}$.

Problem: the variable x_0 has become bound in the substitution.

11.2 Definition
For $\phi \in \text{Form}(\mathcal{L})$, a variable x_i, and a term $t \in \text{Term}(\mathcal{L})$, the result of **substituting t for x_i in ϕ** is the formula

$$(\phi)[t/x_i]$$

which is obtained by replacing each *free* occurrence of x_i in ϕ with the string t, *as long as* this does not lead to new bound occurrences of variables being introduced; if it does, we say that $(\phi)[t/x_i]$ is **undefined**.

We can restate this as a recursive definition:

(i) If ϕ is atomic, $(\phi)[t/x_i]$ is the result of replacing each instance of x_i in ϕ with t.

(ii) $(\neg\psi)[t/x_i] := \neg(\psi)[t/x_i]$ (undefined if $(\psi)[t/x_i]$ is).

(iii) $((\psi \to \chi))[t/x_i] := ((\psi)[t/x_i] \to (\chi)[t/x_i])$ (undefined if $(\psi)[t/x_i]$ or $(\chi)[t/x_i]$ is).

(iv) $(\forall x_i\psi)[t/x_i] := \forall x_i\psi$.

(v) If $j \neq i$, $(\forall x_j\psi)[t/x_i] := \forall x_j(\psi)[t/x_i]$ <u>unless</u> x_j occurs in t and x_i occurs free in ψ, in which case $(\forall x_j\psi)[t/x_i]$ is undefined.

Notation: When no ambiguity could result, we often write $\phi[t/x_i]$ for $(\phi)[t/x_i]$.

Let $\mathcal{L}$ be a first-order language, $\mathcal{A}$ an $\mathcal{L}$-structure.

11.3 Definition
For v an assignment in $\mathcal{A}$ and $t \in \text{Term}(\mathcal{L})$, define

$$v_{t/x_i}(x_j) := \begin{cases} v(x_j) & \text{if } j \neq i \\ \widetilde{v}(t) & \text{if } j = i \end{cases}$$

11.4 Substitution Lemma
Let v be an assignment in an $\mathcal{L}$-structure $\mathcal{A}$. Let $\phi \in \text{Form}(\mathcal{L})$, $t \in \text{Term}(\mathcal{L})$, and suppose $\phi[t/x_i]$ is defined.

Then $\mathcal{A} \models \phi[t/x_i][v]$ iff $\mathcal{A} \models \phi[v_{t/x_i}]$.

Proof:

<u>**Case 1** ϕ atomic:</u>

First, for $u \in \mathrm{Term}(\mathcal{L})$ define:

$u[t/x_i] :=$ the term obtained by replacing each occurrence of x_i in u by t.

Then $\widetilde{v_{t/x_i}}(u) = \widetilde{v}(u[t/x_i])$.
(Exercise)

Now if $\phi = P(t_1, \ldots, t_k)$ for a k-ary relation symbol P in $\mathcal{L}$, then:

$$\begin{array}{ll} & \mathcal{A} \models \phi[v_{t/x_i}] \\ \text{iff} & (\widetilde{v_{t/x_i}}(t_1), \ldots, \widetilde{v_{t/x_i}}(t_k)) \in P^{\mathcal{A}} \\ \text{iff} & (\widetilde{v}(t_1[t/x_i]), \ldots, \widetilde{v}(t_k[t/x_i])) \in P^{\mathcal{A}} \\ \text{iff} & \mathcal{A} \models P(t_1[t/x_i], \ldots, t_k[t/x_i])[v] \\ \text{iff} & \mathcal{A} \models \phi[t/x_i][v] \end{array}$$

If $\phi = t_1 \doteq t_2$, a similar argument applies.

IH: Lemma holds for shorter formulas.

Case 2 $\phi = \neg\psi$ or $\phi = (\xi \to \rho)$:
Follows directly from IH.

Case 3 $\phi = \forall x_i \psi$:
Then $\phi[t/x_i] = \phi$.

$x_i \notin \text{Free}(\phi)$,
so v and v_{t/x_i} agree on all $x \in \text{Free}(\phi)$,
so by Lemma 10.3,

$$\mathcal{A} \models \phi[v_{t/x_i}] \text{ iff } \mathcal{A} \models \phi[v] \text{ iff } \mathcal{A} \models \phi[t/x_i][v]$$

as required.

Case 4 $\phi = \forall x_j \psi$, $j \neq i$:
Then $\phi[t/x_i] = \forall x_j (\psi)[t/x_i]$.
If x_i does not occur free in ψ, then $\phi[t/x_i] = \phi$, and we conclude exactly as in the previous case.
So suppose x_i occurs free in ψ.
Then since $\phi[t/x_i]$ is defined, x_j does not occur in t. Hence:

Claim: *If v^* agrees with v except maybe at x_j, then $\widetilde{v^*}(t) = \widetilde{v}(t)$, so v^*_{t/x_i} agrees with v_{t/x_i} except maybe at x_j.*
Conversely, if v' agrees with v_{t/x_i} except maybe at x_j then $v' = v^*_{t/x_i}$ for some such v^*.

Now: $\mathcal{A} \models \phi[t/x_i][v]$
$\Leftrightarrow \mathcal{A} \models \forall x_j (\psi)[t/x_i][v]$
$\Leftrightarrow \mathcal{A} \models \psi[t/x_i][v^*]$ for all v^* agreeing with v except maybe at x_j,
$\Leftrightarrow \mathcal{A} \models \psi[v^*_{t/x_i}]$ for all v^* agreeing with v except maybe at x_j (by IH),
$\Leftrightarrow \mathcal{A} \models \psi[v']$ for all v' agreeing with v_{t/x_i} except maybe at x_j (by the Claim),
$\Leftrightarrow \mathcal{A} \models \phi[v_{t/x_i}]$.

11.5 Corollary
For any $\phi \in \text{Form}(\mathcal{L})$ *and* $t \in$ *Term*$(\mathcal{L})$ *such that* $\phi[t/x_i]$ *is defined,*

$$\models (\forall x_i \phi \to \phi[t/x_i]).$$

Proof: Let v be an assignment in an $\mathcal{L}$-structure $\mathcal{A}$.

Suppose $\mathcal{A} \models \forall x_i \phi[v]$.
Then $\mathcal{A} \models \phi[v_{t/x_i}]$, since v_{t/x_i} agrees with v except maybe at x_i.
Hence $\mathcal{A} \models \phi[t/x_i][v]$ by the Substitution Lemma (11.4).

□

12. A formal system for Predicate Calculus

12.1 Definition
Associate to each first-order language $\mathcal{L}$ the formal system $K(\mathcal{L})$ with the following axioms and rules:

Axioms
For any $\alpha, \beta, \gamma \in$ Form($\mathcal{L}$), $t \in$ Term($\mathcal{L}$), and $i, j \in \mathbb{N}$, the following are axioms:

A1 $(\alpha \to (\beta \to \alpha))$.
A2 $((\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)))$.
A3 $((\neg\beta \to \neg\alpha) \to (\alpha \to \beta))$.
A4 $(\forall x_i \alpha \to \alpha[t/x_i])$ <u>if</u> $\alpha[t/x_i]$ is defined.
A5 $(\forall x_i(\alpha \to \beta) \to (\alpha \to \forall x_i \beta))$ <u>if</u> $x_i \notin$ Free(α).
A6 $\forall x_i \, x_i \doteq x_i$.
A7 $(x_i \doteq x_j \to (\phi \to \phi'))$, where ϕ is <u>atomic</u> and ϕ' is obtained from ϕ by replacing <u>some</u> (i.e. one or more) occurrences of x_i in ϕ by x_j.

Rules

MP (Modus Ponens): From α and $(\alpha \to \beta)$ infer β.

Gen (Generalisation): For any variable x_i, from α infer $\forall x_i \alpha$.

Let Sent($\mathcal{L}$) be the set of $\mathcal{L}$-sentences.

If $\Sigma \subseteq \text{Sent}(\mathcal{L})$, a formula $\phi \in \text{Form}(\mathcal{L})$ is **provable** from hypotheses Σ, written

$$\Sigma \vdash \phi,$$

if there is a sequence of $\mathcal{L}$-formulas (a **derivation** or **proof**) $\phi_1, \ldots, \phi_n$ with $\phi_n = \phi$ such that for each $i \leq n$:

- (A1-A7) ϕ_i is an axiom, or
- (Hyp) $\phi_i \in \Sigma$, or
- (MP) $\phi_k = (\phi_j \to \phi_i)$ for some $j, k < i$, or
- (Gen) $\phi_i = \forall x_k \phi_j$ for some $j < i$ and some $k \in \mathbb{N}$.

$\vdash \phi$ abbreviates $\emptyset \vdash \phi$.

12.3 Example *Swapping variables*

Suppose Free(ϕ) $= \{x_i\}$.
Then $\{\forall x_i \phi\} \vdash \forall x_j \phi[x_j/x_i]$

1	$\forall x_i \phi$	[$\in \Sigma$]
2	$(\forall x_i \phi \to \phi[x_j/x_i])$	[A4]
3	$\phi[x_j/x_i]$	[MP 1,2]
4	$\forall x_j \phi[x_j/x_i]$	[(Gen)]

12.4 Soundness Theorem for Pred. Calc.

If $\Sigma \vdash \phi$ then $\Sigma \models \phi$.

Proof: By induction on length of a proof.

First we show that **A1**-**A7** are logically valid.
For **A1**, **A2**, and **A3**, this is immediate.
A4 and **A5**: Cor 11.5 resp. Cor 10.4.
A6: easy exercise.

A7: Suppose ϕ is atomic, and ϕ' results from replacing some instances of x_i with x_j.
Let $\mathcal{A}$ be an $\mathcal{L}$-structure and v an assignment in $\mathcal{A}$ such that

$$\mathcal{A} \models x_i \doteq x_j[v] \text{ and } \mathcal{A} \models \phi[v].$$

We want to show that $\mathcal{A} \models \phi'[v]$.

Now $v(x_i) = v(x_j)$,
so $\widetilde{v}(t') = \widetilde{v}(t)$ for any term t' obtained from t by replacing zero or more occurrences of x_i by x_j
(easy induction on terms).

If $\phi = P(t_1, \ldots, t_k)$ then say $\phi' = P(t'_1, \ldots, t'_k)$.

$$\begin{aligned}
\mathcal{A} \models \phi[v] \quad & \text{iff} \quad (\widetilde{v}(t_1), \ldots, \widetilde{v}(t_k)) \in P^{\mathcal{A}} \\
& \text{iff} \quad (\widetilde{v}(t'_1), \ldots, \widetilde{v}(t'_k)) \in P^{\mathcal{A}} \\
& \text{iff} \quad \mathcal{A} \models P(t'_1, \ldots, t'_k)[v] \\
& \text{iff} \quad \mathcal{A} \models \phi'[v] \text{ as required}
\end{aligned}$$

Similarly if ϕ is $t_1 \doteq t_2$.

MP: For any $\mathcal{A}$ and v:

if $\mathcal{A} \models \alpha[v]$ and $\mathcal{A} \models (\alpha \to \beta)[v]$ then $\mathcal{A} \models \beta[v]$;

so: if $\Sigma \models \alpha$ and $\Sigma \models (\alpha \to \beta)$ then $\Sigma \models \beta$.

Generalisation:
Suppose $\Sigma \models \psi$;
we want to show $\Sigma \models \forall x_i \psi$.

So let $\mathcal{A}$ be such that $\mathcal{A} \models \sigma$ for all $\sigma \in \Sigma$,
and let v be an arbitrary assignment on $\mathcal{A}$.
We must show $\mathcal{A} \models \forall x_i \psi[v]$.
So let $v^\star$ agree with v except maybe at x_i.
We must show $\mathcal{A} \models \psi[v^\star]$.
But since $\Sigma \models \psi$, we have $\mathcal{A} \models \psi[v']$ for *any* assignment v', in particular for v^*. $\square$

12.5 Deduction Theorem for Pred. Calc.
Let $\Sigma \subseteq \text{Sent}(\mathcal{L})$, and $\psi \in \text{Sent}(\mathcal{L})$, and $\phi \in \text{Form}(\mathcal{L})$.

$$\textit{If } \Sigma \cup \{\psi\} \vdash \phi \textit{ then } \Sigma \vdash (\psi \to \phi).$$

Proof: Same as for prop. calc. (Theorem 6.6); induction on the length of a proof, with one more case:

IH: $\Sigma \vdash (\psi \to \phi_j)$
to show: $\Sigma \vdash (\psi \to \forall x_i \phi_j)$,
where generalisation (**Gen**) has been used to infer $\forall x_i \phi_j$ from ϕ_j.

By IH and **Gen**: $\Sigma \vdash \forall x_i(\psi \to \phi_j)$
A5 $\vdash (\forall x_i(\psi \to \phi_j) \to (\psi \to \forall x_i \phi_j))$, since $x_i \notin \text{Free}(\psi) = \emptyset$.
So by **MP**, $\Sigma \vdash (\psi \to \forall x_i \phi_j)$ as required.

$\square$

12.6 Lemma
Let α *be a tautology of the* Propositional Calculus *with propositional variables among* $p_0, \ldots, p_n$*, let* $\psi_0, \ldots, \psi_n \in$ Form($\mathcal{L}$)*,*
and let α' *be the* $\mathcal{L}$*-formula obtained from* α *by replacing each occurrence of* p_i *by* ψ_i*.*
Then $\vdash \alpha'$*.*

Proof:
By completeness of L_0, there is a proof $\alpha_1, ..., \alpha_{n-1}, \alpha$ in L_0.

Since **A1**, **A2**, **A3** and **MP** are in $K(\mathcal{L})$, substituting ψ_i for p_i in each α_i yields a proof $\alpha'_1, ..., \alpha'_{n-1}, \alpha'$ in $K(\mathcal{L})$. $\square$

A formula α' as in Lemma 12.6 is called a **tautology** of $\mathcal{L}$. (Note that all tautologies are logical validities, but not vice versa.)

By the lemma, we may freely introduce tautologies in our proofs in $K(\mathcal{L})$.

12.7 Example Suppose $(\exists x_i \phi \to \psi) \in \mathrm{Sent}(\mathcal{L})$. Then

$$\{(\exists x_i \phi \to \psi)\} \vdash \forall x_i (\phi \to \psi)$$

Proof: Let $\Sigma = \{(\exists x_i \phi \to \psi), \neg\psi\}$

1	$(\neg\forall x_i \neg\phi \to \psi)$	[$\in \Sigma$]
2	$((\neg\forall x_i \neg\phi \to \psi) \to (\neg\psi \to \forall x_i \neg\phi))$	[taut.]
3	$(\neg\psi \to \forall x_i \neg\phi)$	[MP 1,2]
4	$\neg\psi$	[$\in \Sigma$]
5	$\forall x_i \neg\phi$	[MP 3,4]
6	$(\forall x_i \neg\phi \to \neg\phi)$	[A4]
7	$\neg\phi$	[MP 5,6]

(In line 6, we used that $(\neg\phi)[x_i/x_i] = \neg\phi$.)

Hence $\Sigma \vdash \neg\phi$. So

$$\begin{array}{ll}
(\exists x_i \phi \to \psi) \vdash (\neg\psi \to \neg\phi) & \text{[DT]} \\
(\exists x_i \phi \to \psi) \vdash (\phi \to \psi) & \text{[A3, MP]} \\
(\exists x_i \phi \to \psi) \vdash \forall x_i (\phi \to \psi) & \text{[Gen]}
\end{array}$$

$\square$

13. The Completeness Theorem for Predicate Calculus

Let $\mathcal{L}$ be a countable first-order language.

13.1 Theorem (Gödel)
Let $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *and* $\phi \in \mathrm{Form}(\mathcal{L})$.

If $\Sigma \models \phi$ *then* $\Sigma \vdash \phi$.

Here, $\Sigma \vdash \phi$ means that ϕ is provable from hypotheses Σ in the proof system $K(\mathcal{L})$.

In outline, our proof strategy is much as in the propositional case:

- Reduce to: consistent $\Rightarrow$ satisfiable.
- Show: any consistent Σ extends to "maximal consistent witnessing" Σ'.
- Show: maximal consistent witnessing $\Rightarrow$ satisfiable.

Call $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ **consistent** (in $K(\mathcal{L})$) if for no $\tau \in \mathrm{Sent}(\mathcal{L})$ do we have both $\Sigma \vdash \tau$ and $\Sigma \vdash \neg\tau$.

Remark

If Σ is inconsistent, then $\Sigma \vdash \chi$ for *any* $\chi \in \mathrm{Sent}(\mathcal{L})$, since $(\tau \to (\neg\tau \to \chi))$ is a tautology.

13.2 Lemma

Every consistent set of sentences has a model.

i.e. if $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is consistent then for some $\mathcal{L}$-structure $\mathcal{A}$,
$\mathcal{A} \models \sigma$ for every $\sigma \in \Sigma$.
c.f. Lemma 7.8.

Proof of Theorem 13.1 from Lemma 13.2
First we treat the case of a sentence $\sigma \in \text{Sent}(\mathcal{L})$.

$\Sigma \models \sigma \Rightarrow \Sigma \cup \{\neg\sigma\}$ has no model
$\Rightarrow_{(13.2)} \Sigma \cup \{\neg\sigma\}$ is not consistent
$\Rightarrow \Sigma \cup \{\neg\sigma\} \vdash \tau$ and $\Sigma \cup \{\neg\sigma\} \vdash \neg\tau$ for some τ
$\Rightarrow_{\text{DT}} \Sigma \vdash (\neg\sigma \to \tau)$ and $\Sigma \vdash (\neg\sigma \to \neg\tau)$.
But $\Sigma \vdash ((\neg\sigma \to \tau) \to ((\neg\sigma \to \neg\tau) \to \sigma))$ [taut]
$\Rightarrow \Sigma \vdash \sigma$ [MP twice]

Now let $\phi \in \text{Form}(\mathcal{L})$, and say $\text{Free}(\phi) = \{x_{i_1}, ..., x_{i_n}\}$.
Let $\sigma := \forall x_{i_1} ... \forall x_{i_n} \phi$.

If $\Sigma \models \phi$ then $\Sigma \models \sigma$, so $\Sigma \vdash \sigma$ by the above. But then by repeatedly applying (A4) and (MP), we obtain $\Sigma \vdash \phi$, as required.
$\square_{13.2 \Rightarrow 13.1}$

To prove Lemma 13.2, we want to introduce an additional assumption.

13.2' Lemma:
Suppose $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *is consistent and* $\mathcal{L}$ *contains infinitely many constant symbols not appearing in* Σ. *Then* Σ *has a model.*

We deduce Lemma 13.2 for arbitrary $\mathcal{L}$ and Σ from Lemma 13.2' as follows.

Let $C = \{c_0, c_1, ...\}$ be a set of distinct symbols disjoint from $\mathcal{L}$, and define the extended language $\mathcal{L}' := \mathcal{L} \cup C$ in which each c_i is a constant symbol.

13.3 Lemma
If $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *and* $\tau \in \mathrm{Sent}(\mathcal{L})$ *is provable from* Σ *in* $K(\mathcal{L}')$*, then* τ *is provable from* Σ *in* $K(\mathcal{L})$*.*

Proof
Exercise sheet 4, Question 3(b). $\square$

Proof of Lemma 13.2 from Lemma 13.2':
By Lemma 13.3, since $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is consistent in $K(\mathcal{L})$, it is also consistent in $K(\mathcal{L}')$;
indeed, otherwise (via the tautology $(\tau \to (\neg\tau \to \chi)))$ any $\chi \in \mathrm{Sent}(\mathcal{L})$ is provable from Σ in $K(\mathcal{L}')$ and hence in $K(\mathcal{L})$, contradicting consistency in $K(\mathcal{L})$.
By Lemma 13.2' applied with $\mathcal{L}'$ in place of $\mathcal{L}$, there is an $\mathcal{L}'$-structure $\mathcal{A}'$ satisfying Σ.
Let $\mathcal{A}$ be the $\mathcal{L}$-structure obtained from $\mathcal{A}'$ by "forgetting" the new constants C.
Then $\mathcal{A}$ satisfies Σ, as required. $\square_{13.2' \Rightarrow 13.2}$

13.4 Definition

- $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is called **maximal consistent** if Σ is consistent, and for any $\psi \in \mathrm{Sent}(\mathcal{L})$: $\Sigma \vdash \psi$ or $\Sigma \vdash \neg\psi$.

- $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is called **witnessing** if for all $\psi \in \mathrm{Form}(\mathcal{L})$ with $\mathrm{Free}(\psi) \subseteq \{x_i\}$ and such that $\Sigma \vdash \exists x_i \psi$, there is some constant symbol $c \in \mathcal{L}$ such that $\Sigma \vdash \psi[c/x_i]$

To prove Lemma 13.2', it suffices to prove the following two lemmas:

13.5 Lemma

Every maximal consistent witnessing set $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *has a model.*

13.6 Lemma

If $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *is consistent and* $\mathcal{L}$ *contains infinitely many constant symbols not appearing in* Σ*, then* Σ *extends to a maximal consistent witnessing set* $\Sigma' \subseteq \mathrm{Sent}(\mathcal{L})$.

For the proof of 13.6 we need two further lemmas.

13.7 Lemma

If $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *is consistent, then for any sentence* ψ*, either* $\Sigma \cup \{\psi\}$ *or* $\Sigma \cup \{\neg\psi\}$ *is consistent.*

Proof: Exercise – as in the proof of Theorem 7.5. $\square$.

13.8 Lemma

Assume $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *is consistent, and* $\Sigma \vdash \exists x_i \psi \in \mathrm{Sent}(\mathcal{L})$*, and* c *is a constant symbol of* $\mathcal{L}$ *which does* not *occur in* ψ *nor in any* $\sigma \in \Sigma$*.*
Then $\Sigma \cup \{\psi[c/x_i]\}$ *is consistent.*

Proof:

It suffices to show that if c does not occur in $\chi \in \mathrm{Sent}(\mathcal{L})$ and $\Sigma \cup \{\psi[c/x_i]\} \vdash \chi$,
then already $\Sigma \vdash \chi$. Indeed:
If $\Sigma \cup \{\psi[c/x_i]\}$ were inconsistent then (via the tautology $(\alpha \to (\neg\alpha \to \beta))$) we would have for *any* χ that $\Sigma \cup \{\psi[c/x_i]\} \vdash \chi$ and $\Sigma \cup \{\psi[c/x_i]\} \vdash \neg\chi$;
picking χ in which c does not occur, it would follow that $\Sigma \vdash \chi$ and $\Sigma \vdash \neg\chi$, contradicting consistency of Σ.

So suppose $\Sigma \cup \{\psi[c/x_i]\} \vdash \chi \in \mathsf{Sent}(\mathcal{L})$ and c does not occur in χ. Recall we also assumed that c does not occur in Σ or ψ.

By DT, $\Sigma \vdash (\psi[c/x_i] \to \chi)$
It follows that $\Sigma \vdash (\psi \to \chi)$
(Exercise Sheet 4 Question 3(a)).

By Gen, $\Sigma \vdash \forall x_i(\psi \to \chi)$.
It follows that $\Sigma \vdash (\exists x_i \psi \to \chi)$
(Exercise Sheet 4 Question 2).

But we assumed $\Sigma \vdash \exists x_i \psi$,
so by MP, $\Sigma \vdash \chi$, as required.

$\square_{13.8}$

Proof of 13.6:
Let $\Sigma \subseteq \text{Sent}(\mathcal{L})$ be consistent, and suppose $\mathcal{L}$ contains infinitely many constant symbols not appearing in Σ.

We show that Σ extends to a maximal consistent witnessing set.

$\text{Sent}(\mathcal{L})$ is countable; say $\text{Sent}(\mathcal{L}) = \{\tau_1, \tau_2, \tau_3, \ldots\}$.

Construct finite sets $\Delta_i \subseteq \text{Sent}(\mathcal{L})$

$$\Delta_0 \subseteq \Delta_1 \subseteq \Delta_2 \subseteq \ldots$$

such that $\Sigma \cup \Delta_n$ is consistent for each $n \geq 0$, as follows:

Let $\Delta_0 := \emptyset$. Then $\Sigma \cup \Delta_0 = \Sigma$ is consistent.

If Δ_n has been constructed let

$$\Delta'_n := \begin{cases} \Delta_n \cup \{\tau_{n+1}\} & \text{if } \Sigma \cup \Delta_n \cup \{\tau_{n+1}\} \\ & \text{ is consistent} \\ \Delta_n \cup \{\neg\tau_{n+1}\} & \text{otherwise.} \end{cases}$$

Then $\Sigma \cup \Delta'_n$ is consistent by Lemma 13.7.

If $\neg\tau_{n+1} \in \Delta'_n$ or if τ_{n+1} is not of the form $\exists x_i \psi$, let $\Delta_{n+1} := \Delta'_n$.

Otherwise, i.e. if $\tau_{n+1} = \exists x_i \psi \in \Delta'_n$:
Choose a constant symbol $c \in \mathcal{L}$ which occurs in no formula in $\Sigma \cup \Delta'_n \cup \{\psi\}$
(possible since $\Delta'_n \cup \{\psi\}$ is finite).
Let $\Delta_{n+1} := \Delta'_n \cup \{\psi[c/x_i]\}$.
By Lemma 13.8, $\Sigma \cup \Delta_{n+1}$ is consistent.

Let $\Sigma' := \Sigma \cup \bigcup_{n \geq 0} \Delta_n$.
Then Σ' is maximal consistent (as in 7.5), and Σ' is witnessing by construction.

$\square_{13.6}$

To finish the proof of completeness, it remains to prove:

13.5 Lemma
Every maximal consistent witnessing set $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *has a model.*

Proof:
A term is **closed** if no variable appears in it. Let T be the set of closed $\mathcal{L}$-terms.

Define an equivalence relation E on T by

$$t_1 E t_2 \text{ iff } \Sigma \vdash t_1 \doteq t_2$$

(This *is* an equivalence relation – see Sheet 4 Question 1(b).)

Let T/E be the set of equivalence classes t/E for $t \in T$.

Define an $\mathcal{L}$-structure $\mathcal{A}$ with domain T/E by

$$c^{\mathcal{A}} := c/E$$
$$f^{\mathcal{A}}(t_1/E, \ldots, t_k/E) := f(t_1, \ldots, t_k)/E$$
$$P^{\mathcal{A}} := \{(t_1/E, ..., t_k/E) \mid \Sigma \vdash P(t_1, \ldots, t_k)\}$$

(for c a constant symbol, f a k-ary function symbol, and P a k-ary predicate symbol).

Note: $t^{\mathcal{A}} = t/E$ for any $t \in T$.

Exercise: The definitions above do not depend on representatives, i.e. if $t_i/E = t'_i/E$ for $i = 1, \ldots k$ then:

- $f(t_1, \ldots, t_k)/E = f(t'_1, \ldots, t'_k)/E$
- $\Sigma \vdash P(t_1, \ldots, t_k) \Leftrightarrow \Sigma \vdash P(t'_1, \ldots, t'_k)$

This follows from **A7** and **A4**; see Sheet 4 Question 1(c).

We conclude by showing: $\mathcal{A} \models \Sigma$.

We show more generally that for any $\sigma \in \mathsf{Sent}(\mathcal{L})$,

$$\mathcal{A} \models \sigma \text{ iff } \Sigma \vdash \sigma.$$

We prove this by induction on the number of symbols among $\{\neg, \rightarrow, \forall\}$ in σ.

- $\sigma = P(t_1, ..., t_k)$. Then:

$$\begin{aligned} \mathcal{A} \models \sigma &\Leftrightarrow (t_1^{\mathcal{A}}, ..., t_k^{\mathcal{A}}) \in P^{\mathcal{A}} \\ &\Leftrightarrow (t_1/E, ..., t_k/E) \in P^{\mathcal{A}} \\ &\Leftrightarrow \Sigma \vdash \sigma. \end{aligned}$$

- $\sigma = t_1 \doteq t_2$. Then:

$$\begin{aligned} \mathcal{A} \models \sigma &\Leftrightarrow t_1^{\mathcal{A}} = t_2^{\mathcal{A}} \\ &\Leftrightarrow t_1/E = t_2/E \\ &\Leftrightarrow \Sigma \vdash \sigma. \end{aligned}$$

- $\sigma = \neg\tau$:

$$\begin{array}{lll} & \mathcal{A} \models \neg\tau & \\ \text{iff} & \mathcal{A} \not\models \tau & \text{[def. of `}\models\text{']} \\ \text{iff} & \Sigma \nvdash \tau & \text{[IH]} \\ \text{iff} & \Sigma \vdash \neg\tau & [\Sigma \text{ max. cons.]} \end{array}$$

- $\sigma = (\tau \to \rho)$:

$$\begin{array}{lll} & \mathcal{A} \models (\tau \to \rho) & \\ \text{iff} & \mathcal{A} \not\models \tau \text{ or } \mathcal{A} \models \rho & \text{[def. `}\models\text{']} \\ \text{iff} & \Sigma \nvdash \tau \text{ or } \Sigma \vdash \rho & \text{[IH]} \\ \text{iff} & \text{ not } (\Sigma \vdash \tau \text{ and } \Sigma \nvdash \rho) & \\ \text{iff} & \text{ not } (\Sigma \vdash \tau \text{ and } \Sigma \vdash \neg\rho) & [\Sigma \text{ max. cons.]} \\ \text{iff} & \Sigma \nvdash \neg(\tau \to \rho) & \text{[taut. (see below)]} \\ \text{iff} & \Sigma \vdash (\tau \to \rho) & [\Sigma \text{ max. cons.]} \end{array}$$

where the penultimate line uses the following tautologies:

$$(\tau \to (\neg\rho \to \neg(\tau \to \rho)))$$
$$(\neg(\tau \to \rho) \to \tau)$$
$$(\neg(\tau \to \rho) \to \neg\rho).$$

- $\sigma = \forall x_i \phi$:

  By the Substitution Lemma 11.4,
  $\mathcal{A} \models \phi[t/x_i] \Leftrightarrow \mathcal{A} \models \phi[v_t]$ where v_t is any assignment with $v_t(x_i) = t^{\mathcal{A}} = t/E$.

  So since the domain of $\mathcal{A}$ is T/E,
  $\mathcal{A} \models \forall x_i \phi$ iff for all $t \in T$, $\mathcal{A} \models \phi[t/x_i]$.

  Now for $t \in T$: $\phi[t/x_i] \in \text{Sent}(\mathcal{L})$, so by IH,
  $\mathcal{A} \models \phi[t/x_i]$ iff $\Sigma \vdash \phi[t/x_i]$.

  So to show $\Sigma \vdash \forall x_i \phi$ iff $\mathcal{A} \models \forall x_i \phi$, it suffices to show:
  $\Sigma \vdash \forall x_i \phi$ iff for all $t \in T$, $\Sigma \vdash \phi[t/x_i]$.

We prove:
$\Sigma \vdash \forall x_i \phi$ iff for all $t \in T$, $\Sigma \vdash \phi[t/x_i]$.

$\Rightarrow$: **A4** + **MP**.

For the converse, first note:

$$\{\forall x_i \neg\neg\phi\} \vdash \forall x_i \phi; \qquad (\star)$$

indeed, by **A4** we have $\{\forall x_i \neg\neg\phi\} \vdash \neg\neg\phi$; conclude using the tautology $(\neg\neg\phi \to \phi)$ and **Gen**.

Now suppose $\Sigma \nvdash \forall x_i \phi$.
Then $\Sigma \nvdash \forall x_i \neg\neg\phi$, by $(\star)$.
So by maximality, $\Sigma \vdash \neg\forall x_i \neg\neg\phi$,
i.e. $\Sigma \vdash \exists x_i \neg\phi$.
Since Σ is witnessing, $\Sigma \vdash (\neg\phi)[c/x_i]$ for some constant symbol c.
Then since Σ is consistent, $\Sigma \nvdash \phi[c/x_i]$.
But $c \in T$, so it is not the case that for all $t \in T$, $\Sigma \vdash \phi[t/x_i]$. $\square_{13.5}$

This concludes our proof of the Completeness Theorem 13.1.

In fact, our proof of completeness yields a stronger result.

13.9 Definition: A structure is **countable** if its domain is countable (i.e. finite or countably infinite).

The model constructed in Lemma 13.5 is countable, because the set T of closed terms is, so we have actually proven the following strengthening of Lemma 13.2:

13.10 Weak downwards Löwenheim-Skolem Theorem
Every consistent set of sentences has a countable model.

Exactly as in the propositional case, we deduce compactness from completeness and soundness.

13.11 Compactness Theorem:
A set of sentences $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ *has a model if and only if every finite subset* $\Sigma_0 \subseteq_{fin} \Sigma$ *has a model.*

14. Prenex normal form

A formula is in **prenex normal form (PNF)** if it is of the form

$$Q_1 x_{i_1} Q_2 x_{i_2} \cdots Q_k x_{i_k}\, \psi,$$

where each Q_i is a quantifier
(i.e. either $\forall$ or $\exists$), and where
ψ is a formula containing no quantifiers.

14.1 PNF-Theorem
Every $\phi \in \mathrm{Form}(\mathcal{L})$ *is logically equivalent to an* $\mathcal{L}$*-formula in PNF.*

Proof: Induction on ϕ
(working in the language with $\forall, \exists, \neg, \wedge$, recalling that $\{\neg, \wedge\}$ is adequate for propositional logic):

- ϕ atomic: ϕ is already in PNF.

- $\phi = \neg\chi$ with χ in PNF:
  say $\phi = \neg Q_1 x_{i_1} Q_2 x_{i_2} \cdots Q_k x_{i_k}\, \psi$.

  Then $\phi \models\!\!\!=\!\!\!\mid\ Q_1^- x_{i_1} \cdots Q_k^- x_{i_k}\, \neg\psi$,
  where $Q^- = \exists$ if $Q = \forall$,
  and $Q^- = \forall$ if $Q = \exists$.

- $\phi = (\chi \wedge \rho)$ with χ, ρ in PNF:

  Note that $\forall x_i \alpha \models\!\!\!=\!\!\!\mid\ \forall x_j \alpha[x_j/x_i]$
  if x_j does not occur in α.

  Swapping variables in this way, we may assume that the variables quantified over in χ do not occur in ρ, and vice versa.

  But then, e.g.
  $(\forall x_1 \alpha \wedge \exists x_2 \beta) \models\!\!\!=\!\!\!\mid\ \forall x_1 \exists x_2 (\alpha \wedge \beta)$. $\square$

B1.1 Logic
Lecture 15

Martin Bays

Oxford University, MT 23

15 Applications of the Completeness Theorem

Throughout, $\mathcal{L}$ denotes a countable first-order language.

15.1 Elementary equivalence

Definition 15.1.

- An **$\mathcal{L}$-theory** is a set of $\mathcal{L}$-sentences $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$.
- Let $\mathcal{A}$ be an $\mathcal{L}$-structure. Then the **(first-order) theory of** $\mathcal{A}$ is the $\mathcal{L}$-theory
$$\mathrm{Th}(\mathcal{A}) = \mathrm{Th}^{\mathcal{L}}(\mathcal{A}) := \{\sigma \in \mathrm{Sent}(\mathcal{L}) \mid \mathcal{A} \models \sigma\},$$
the set of all $\mathcal{L}$-sentences true in $\mathcal{A}$.
- $\mathcal{L}$-structures $\mathcal{A}$ and $\mathcal{B}$ are **elementarily equivalent**, written $\mathcal{A} \equiv \mathcal{B}$, if $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$.

Exercise 15.2. An $\mathcal{L}$-theory $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ is maximal consistent if and only if Σ has a model and $\mathcal{A} \equiv \mathcal{B}$ for any two models $\mathcal{A}$ and $\mathcal{B}$ of Σ.

15.2 Axiomatisations

Definition 15.3. An **axiomatisation** of the theory $\mathrm{Th}(\mathcal{A})$ of an $\mathcal{L}$-structure $\mathcal{A}$ is a maximal consistent subset of $\mathrm{Th}(\mathcal{A})$; i.e. a set of sentences which hold of $\mathcal{A}$ and which suffice to deduce any sentence which holds of $\mathcal{A}$.

Recall Hilbert's programme from Lecture 1. Now we have established the Completeness Theorem, the programme would call for us to find "finitary" (i.e. computable) axiomatisations of the structures in mathematics.

In general this is *impossible*: Gödel's first incompleteness theorem shows that already the theory of arithmetic $\mathrm{Th}(\langle \mathbb{N}; +, \cdot \rangle)$ has no computable axiomatisation. But for some interesting structures it is possible, as we will now begin to see.

15.3 A criterion for maximal consistency

Definition 15.4. Let $\mathcal{A} = \langle A; \ldots \rangle$ and $\mathcal{B} = \langle B; \ldots \rangle$ be $\mathcal{L}$-structures. An **isomorphism** of $\mathcal{A}$ with $\mathcal{B}$ is a bijection $\theta : A \to B$ such that

- $\theta(c^{\mathcal{A}}) = c^{\mathcal{B}}$ for c a constant symbol;
- $\theta(f^{\mathcal{A}}(a_1, \ldots, a_k)) = f^{\mathcal{B}}(\theta(a_1), \ldots, \theta(a_k))$ for f a k-ary function symbol and $a_i \in A$;
- $(a_1, \ldots, a_k) \in P^{\mathcal{A}} \Leftrightarrow (\theta(a_1), \ldots, \theta(a_k)) \in P^{\mathcal{B}}$ for P a k-ary relation symbol and $a_i \in A$.

We write $\mathcal{A} \cong \mathcal{B}$ to mean that there exists such an isomorphism.

Exercise 15.5. $\mathcal{A} \cong \mathcal{B}$ implies $\mathcal{A} \equiv \mathcal{B}$.
The converse fails (e.g. due to Löwenheim-Skolem).

Theorem 15.6. *Suppose $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$ has a unique countable model up to isomorphism, i.e. Σ is consistent and if $\mathcal{A}, \mathcal{B} \vDash \Sigma$ are countable then $\mathcal{A} \cong \mathcal{B}$.*
Then Σ is maximal consistent.

Proof. Let $\mathcal{A}, \mathcal{B} \vDash \Sigma$. We conclude by showing $\mathcal{A} \equiv \mathcal{B}$.
Both $\mathcal{A}$ and $\mathcal{B}$ are infinite. By Weak Downward Löwenheim-Skolem (Theorem 13.10), there are countable $\mathcal{A}' \equiv \mathcal{A}$ and $\mathcal{B}' \equiv \mathcal{B}$. Then $\mathcal{A}', \mathcal{B}' \vDash \Sigma$, so $\mathcal{A}' \cong \mathcal{B}'$, and so $\mathcal{A}' \equiv \mathcal{B}'$ by Exercise 15.5. Hence $\mathcal{A} \equiv \mathcal{A}' \equiv \mathcal{B}' \equiv \mathcal{B}$. ☐

Remark 15.7. The converse fails. We will see an example in the next lecture.

Example 15.8. Let $\mathcal{L}_= := \emptyset$, the language with no non-logical symbols. For $n \geq 2$, set $\tau_n := \exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} \neg x_i \doteq x_j$. Then the models of

$$\Sigma_\infty := \{\tau_n : n \geq 2\}$$

are precisely the infinite $\mathcal{L}_=$-structures (i.e. the infinite sets). By Theorem 15.6, Σ_∞ is maximal consistent.

15.4 Example: axiomatising $\mathrm{Th}(\langle \mathbb{Q}; < \rangle)$

Definition 15.9. Let $\mathcal{L}_< := \{<\}$ and let σ_{DLO} be the following $\mathcal{L}_<$-sentence, whose models are the dense linear orderings without endpoints:

$$\begin{aligned}\sigma_{\mathrm{DLO}} := \forall x\, \forall y\, \forall z\, (&\neg x < x \\ &\wedge (x < y \vee x = y \vee y < x) \\ &\wedge ((x < y \wedge y < z) \to x < z) \\ &\wedge (x < y \to \exists w\, (x < w \wedge w < y)) \\ &\wedge \exists w\, w < x \\ &\wedge \exists w\, x < w).\end{aligned}$$

Note that $\langle \mathbb{Q}; < \rangle \vDash \sigma_{\mathrm{DLO}}$, and also $\langle \mathbb{R}; < \rangle \vDash \sigma_{\mathrm{DLO}}$.

Theorem 15.10 (Cantor). *σ_{DLO} has a unique countable model up to isomorphism (so any countable model is isomorphic to $\langle \mathbb{Q}; < \rangle$).*

Proof. *("Back-and-forth argument")*
Let $\mathcal{M}, \mathcal{N} \vDash \sigma_{\text{DLO}}$ be countable. By the non-existence of endpoints, each is infinite.

A **partial isomorphism** $\theta : \mathcal{M} \dashrightarrow \mathcal{N}$ is a partially defined injective map such that for all $a, b \in \operatorname{dom}(\theta)$,

$$\mathcal{M} \vDash a < b \;\; \Leftrightarrow \;\; \mathcal{N} \vDash \theta(a) < \theta(b).$$

Enumerate the domains of $\mathcal{M}$ and $\mathcal{N}$ as $(m_i)_{i \in \mathbb{N}}$ and $(n_i)_{i \in \mathbb{N}}$ respectively. We recursively construct a chain of partial isomorphisms $\theta_i : \mathcal{M} \dashrightarrow \mathcal{N}$ such that

$$\operatorname{dom}(\theta_i) \text{ is finite, and for all } j < i, \text{ we have } m_j \in \operatorname{dom}\theta_i \text{ and } n_j \in \operatorname{im}\theta_i. \quad (*)$$

Let $\theta_0 := \emptyset$.

Given θ_i satisfying (*), we first extend θ_i by finding $n \in \mathcal{N}$ such that setting $\theta_i'(m_i) := n$ yields a partial isomorphism $\theta_i' : \mathcal{M} \dashrightarrow \mathcal{N}$ with $\operatorname{dom}\theta_i' = \operatorname{dom}\theta \cup \{m_i\}$.

Say $\operatorname{dom}(\theta_i) = \{a_1, \ldots, a_s\}$ with $\mathcal{M} \vDash a_k < a_l$ for $1 \leq k < l \leq s$, and similarly $\operatorname{im}(\theta_i) = \{b_1, \ldots, b_s\}$ with $\mathcal{N} \vDash b_k < b_l$ for $1 \leq k < l \leq s$. There are four cases:

(i) $m_i = a_k$ (some $k \in [1, s]$): set $n := b_k$.

(ii) $m_i < a_1$: let $n \in \mathcal{N}$ be such that $n < b_1$ (n exists, since $\mathcal{N}$ has no endpoint).

(iii) $m_i > a_s$: let $n \in \mathcal{N}$ be such that $n > b_s$ (n exists, since $\mathcal{N}$ has no endpoint).

(iv) $a_j < m_i < a_{j+1}$ (some $j \in [1, s-1]$): let $n \in \mathcal{N}$ be such that $a_i < n < a_{i+1}$ (n exists, since $\mathcal{N}$ is dense).

In all cases, θ_i' is a partial isomorphism.

Symmetrically, $(\theta_i')^{-1} : \mathcal{N} \dashrightarrow \mathcal{M}$ extends to $\theta_i'' : \mathcal{N} \dashrightarrow \mathcal{M}$ with $n_i \in \operatorname{dom}\theta_i{}''$;
then $\theta_{i+1} := (\theta_i'')^{-1} : \mathcal{M} \dashrightarrow \mathcal{N}$ is a partial isomorphism satisfying (*).

Then $\theta := \bigcup_i \theta_i : \mathcal{M} \xrightarrow{\cong} \mathcal{N}$ is an isomorphism. □

Applying Theorem 15.6, we obtain:

Corollary 15.11. $\{\sigma_{\text{DLO}}\}$ *is maximal consistent. Hence* $\{\sigma_{\text{DLO}}\}$ *axiomatises* $\operatorname{Th}(\langle \mathbb{Q}; < \rangle)$.

Corollary 15.12. *Completeness of a linear order is not a first-order property: there is no $\mathcal{L}_<$-theory Σ such that the models of Σ are precisely the complete linear orders.*

Proof. Suppose such a Σ exists. Then $\langle \mathbb{R}; < \rangle \vDash \Sigma$ since $\langle \mathbb{R}; < \rangle$ is a complete linear order. But $\langle \mathbb{R}; < \rangle \equiv \langle \mathbb{Q}; < \rangle$, since both satisfy the maximal complete theory $\{\sigma_{\text{DLO}}\}$, so then also $\langle \mathbb{Q}; < \rangle \vDash \Sigma$. But $\langle \mathbb{Q}; < \rangle$ is not a complete linear order, contradicting the desired property of Σ. □

B1.1 Logic
Lecture 16

Martin Bays

Oxford University, MT 23

16 An algebraic application (non-examinable)

16.1 ACF

Let $\mathcal{L}_{\text{ring}} := \{+, -, \cdot, \bar{0}, \bar{1}\}$. Let ACF be the $\mathcal{L}_{\text{ring}}$-theory whose models are precisely the algebraically closed fields:

$$\text{ACF} := \text{ [Field axioms] } \cup \{\forall z_0, \ldots, z_n \left(\neg z_n \doteq \bar{0} \to \exists x \sum_{i=0}^{n} z_i x^i \doteq \bar{0}\right) : n \geq 1\}.$$

Let

$$\text{ACF}_0 := \text{ACF} \cup \{\neg \bar{n} \doteq \bar{0} : n \in \mathbb{N}\},$$

where for $n \geq 1$, $\bar{n} := \bar{1} + \ldots + \bar{1}$ (n times). So the models of ACF_0 are precisely the algebraically closed fields of characteristic 0. In particular, $\langle \mathbb{C}; +, -, \cdot, 0, 1\rangle \vDash \text{ACF}_0$. We aim to show that ACF_0 is maximally consistent, i.e. axiomatises $\text{Th}(\langle \mathbb{C}; +, -, \cdot, 0, 1\rangle)$.

We can prove this analogously to the case of $\langle \mathbb{Q}; <\rangle$, but working with uncountable sets.

From now on, we assume the axiom of choice. We will explain this and the related notion of the **cardinality** ("size") $|A|$ of a set A in the Set Theory course; for now it suffices to know that $|A| = |B|$ if and only if there exists a bijection $A \to B$, and cardinalities are linearly ordered.

Fact 16.1. *Any characteristic 0 algebraically closed field* $\langle K; +, -, \cdot, 0, 1\rangle \vDash \text{ACF}_0$ *with the same cardinality as* $\mathbb{C}$ *is isomorphic to* $\langle \mathbb{C}; +, -, \cdot, 0, 1\rangle$.

Sketch proof. A subset $A \subseteq K$ is **algebraically independent** if there are no non-trivial polynomial relations between its elements, i.e. $f(a_1, \ldots, a_n) \neq 0$ for any $f \in \mathbb{Z}[X_1, \ldots, X_n] \setminus \{0\}$ and $\{a_1, \ldots, a_n\} \subseteq A$.

Then just as for linear independence in vector spaces, an algebraically closed field has a well-defined dimension ("transcendence degree") which is the cardinality of any maximal algebraically independent subset, this dimension determines an algebraically closed field of a given characteristic up to isomorphism, and the dimension of an uncountable ACF is equal to its cardinality. $\square$

Fact 16.2. *Let* $\mathcal{L}$ *be a possibly uncountable first-order language, i.e. with sets of constant, function, and relation symbols of arbitrary cardinality. Let* $|\mathcal{L}|$ *be the cardinality of the language, i.e. that of the alphabet.*

Let $\Sigma \subseteq \mathrm{Sent}(\mathcal{L})$, and suppose any finite subset of Σ has a model. Then Σ has a model of cardinality (i.e. with domain of cardinality) $\leq |\mathcal{L}|$.

Sketch proof. Our proof for countable $\mathcal{L}$ mostly goes through directly.

The only place we used the countability assumption was in extending a consistent set Σ to a maximal consistent witnessing set. We can use Zorn's lemma here in the uncountable case – the union of a chain of consistent witnessing sets containing Σ is still consistent and witnessing, so there exists a maximal such with respect to inclusion, which (as in the proof in the countable case) is maximal consistent witnessing. □

Corollary 16.3. ACF_0 *is maximal consistent, hence axiomatises* $\mathrm{Th}(\mathbb{C})$.

Proof. Let $\mathcal{A} \vDash \mathrm{ACF}_0$. Note that $\mathcal{A}$ is infinite, since it has characteristic 0.

Let $C = \{c_a : a \in \mathbb{C}\}$ be a set of constant symbols of cardinality $|\mathbb{C}|$, and let $\mathcal{L}' := \mathcal{L}_{\text{ring}} \cup C$. Let $\Sigma := \mathrm{Th}^{\mathcal{L}_{\text{ring}}}(\mathcal{A}) \cup \{\neg c_a \doteq c_b : a, b \in \mathbb{C},\ a \neq b\} \subseteq \mathrm{Sent}(\mathcal{L}')$. Then since $\mathcal{A}$ is infinite, any finite subset of Σ has as model $\mathcal{A}$ with the finitely many c_a which appear interpreted as distinct elements. So by Fact 16.2, Σ has a model $\mathcal{B}$ of cardinality $\leq |\mathcal{L}'| = |\mathbb{C}|$. Considering the interpretations of the c_a, we actually have $|\mathcal{B}| = |\mathbb{C}|$. Let $\mathcal{B}'$ be the $\mathcal{L}_{\text{ring}}$ structure obtained from $\mathcal{B}$ by ignoring the c_a. Then by Fact 16.1, $\mathcal{B}' \cong \mathbb{C}$. So $\mathcal{A} \equiv \mathcal{B}' \equiv \mathbb{C}$.

So we conclude that any two models of ACF_0 are elementary equivalent, so ACF_0 is maximal consistent. □

Theorem 16.4 (Ax-Grothendieck)**.** *Let $F : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map, i.e. $F(a_1, \ldots, a_n) = (F_1(a_1, \ldots, a_n), \ldots, F_n(a_1, \ldots, a_n))$, where $F_i \in \mathbb{C}[\overline{X}]$.*

If F is injective, then F is surjective.

Proof. Fact: The algebraic closure of the finite field $\mathbb{F}_p$ is the union of a chain of finite subfields, $\mathbb{F}_p^{\text{alg}} = \bigcup_k \mathbb{F}_{p^{k!}}$.

Claim 16.5. *Let p be prime. Any injective polynomial map $F : (\mathbb{F}_p^{\text{alg}})^n \to (\mathbb{F}_p^{\text{alg}})^n$ is surjective.*

Proof. Let k_0 be such that the coefficients of F are in $\mathbb{F}_{p^{k_0!}}$.

Let $k \geq k_0$. Then $F({\mathbb{F}_{p^{k!}}}^n) \subseteq {\mathbb{F}_{p^{k!}}}^n$, and so by injectivity, finiteness of ${\mathbb{F}_{p^{k!}}}^n$, and the pigeonhole principle, $F({\mathbb{F}_{p^{k!}}}^n) = {\mathbb{F}_{p^{k!}}}^n$.

Hence $F((\mathbb{F}_p^{\text{alg}})^n) = (\mathbb{F}_p^{\text{alg}})^n$. □

Let $n, d \in \mathbb{N}$. Let $\sigma_{n,d}$ be an $\mathcal{L}_{\text{ring}}$-sentence expressing that any injective polynomial map $F : K^n \to K^n$ consisting of polynomials of degree $\leq d$ is surjective:

$$\sigma_{n,d} := \forall z_{1,0}, \ldots, z_{n,d}\ (\forall \overline{x}, \overline{y}\ ((\bigwedge_i \sum_j z_{i,j} {x_i}^j \doteq \sum_j z_{i,j} {y_i}^j) \to \bigwedge_i x_i \doteq y_i)$$
$$\to \forall \overline{y}\ \exists \overline{x}\ \bigwedge_i \sum_j z_{i,j} {x_i}^j \doteq y_i).$$

Suppose $\mathbb{C} \nvDash \sigma_{n,d}$. Then by maximal consistency of ACF_0, $\mathrm{ACF}_0 \vDash \neg\sigma_{n,d}$. Then by compactness, for some $m \in \mathbb{N}$,

$$\mathrm{ACF} \cup \{\neg \bar{i} \doteq \bar{0} : 0 < i < m\} \vDash \neg\sigma_{n,d}.$$

So if $p > m$ is prime, $\mathbb{F}_p^{\text{alg}} \vDash \neg\sigma_{n,d}$. But this contradicts the Claim. □