Mathematical Logic, an Introduction

by Peter Koepke

Bonn, Winter 2019/20

Wann sollte die Mathematik je zu einem Anfang gelangen, wenn sie warten wollte, bis die Philosophie über unsere Grundbegriffe zur Klarheit und Einmüthigkeit gekommen ist? Unsere einzige Rettung ist der formalistische Standpunkt, undefinirte Begriffe (wie Zahl, Punkt, Ding, Menge) an die Spitze zu stellen, um deren actuelle oder psychologische oder anschauliche Bedeutung wir uns nicht kümmern, und ebenso unbewiesene Sätze (Axiome), deren actuelle Richtigkeit uns nichts angeht. Aus diesen primitiven Begriffen und Urtheilen gewinnen wir durch Definition und Deduction andere, und nur diese Ableitung ist unser Werk und Ziel. (Felix Hausdorff, 12. Januar 1918)

Table of contents

1 Introduction

Mathematical logic studies the general methods of mathematics:

- the mathematical language of sentences and texts
- mathematical structures
- truth of mathematical statements in structures
- proofs

Tne central theorem in general logic will be

- Gödel's completeness theorem

We shall also consider

- set theory as a foundation of mathematics
- automatic theorem proving

Formalizing set theory in logic and logic in set theory leads to the

- Gödel incompleteness theorems

Mathematical logic is a meta-mathematics. It is, amazingly, also part of mathematics itself, since mathematical language, structures and proofs satisfy mathematical laws themselves. This is another evidence for the remarkable power of mathematics to model variious fields: mathematics is able to *model itself*.

At the center of attention is the relation

$$\mathfrak{M} \vDash \varphi,$$

which expresses that the *formula* φ is true in the mathematical *structure* $\mathfrak{M}$. $\mathfrak{M}$ could, e.g., be a group $(G, *)$ and φ could be the associative law "for all x, y, z: $x + (y + z) = (x + y) + z$".

The mathematical enquiry into the mathematical method leads to deep insights into mathematics, applications to classical fields of mathematics, and to new mathematical theories. The study of mathematical language has also influenced the theory of formal and natural languages in computer science, linguistics and philosophy.

I First-order Logic and the Gödel Completeness Theorem

2 The Syntax of first-order logic: Symbols, words, and formulas

The art of free society consists first in the maintenance of the symbolic code.

A. N. Whitehead

2.1 Motivation: a mathematical statement

We quote a theorem by Tom Hales:

Theorem 1. (The Kepler Conjecture) *No packing of congruent balls in Euclidean three space has density greater than that of the face-centered cubic packing.*

Although we are not concerned with discrete geometry in this lecture, proof methods by Hales (and others) will be of relevance to this course.

This is a natural language statement. Mathematicians know how to interpret it in clearly determined, "formal" ways. Let us transform the statement in more formal form:

- Not exists a packing of congruent balls in Euclidean three space that has density greater than the density of the face-centered cubic packing.
- Not exists P such that (P is a packing of congruent balls in Euclidean three space and the density of P is greater than the density of the face-centered cubic packing).
- Not exists P (isAPackingOfCongruentBallsInEuclideanThreeSpace(P) and densityOf(P) is greater than densityOf(theFacecenteredCubicPacking))
- $\neg\exists P$(packing(P)$\wedge$greaterThan(density(P),density(faceenteredPacking)))
- $\neg\exists P(p(P) \wedge g(d(P), d(P_0)))$

Parsing natural language statements into understandable form is a process that humans perform constantly. Computer implementations of such parsings indicate the complexity of the process.

Formal mathematical statements consist of symbols, just like ordinary sentences are sequences of alphabetic letters. In our example, the symbols are

$$\neg, \exists, P, (,), p, \wedge, ...$$

and also

$$\text{isAPackingOfCongruentBallsInEuclideanThreeSpace, densityOf, ...}$$

Symbols stand for natural language words or even multi-word natural language phrases. Sentences formed of words and phrases correspond to words, i.e., sequences of symbols in the formal language.

We treat symbols and words as mathematical objects. The study of the formal properties of symbols, words, sentences,... is called *syntax*. Syntax will later be related to the "meaning" of symbolic material, its *semantics*. The interplay between syntax and semantics is at the core of logic. A strong logic is able to present interesting semantic properties, i.e., properties of interesting mathematical structure, already in its syntax.

2.2 Symbols

"Man muß jederzeit an Stelle von 'Punkte, Geraden, Ebenen', 'Tische, Stühle, Bierseidel' sagen können".
Quote ascribed to David Hilbert

Basic Notions. We introduce basic logical symbols:

- A *symbol* is a mathematical object;
- $\equiv, \neg, \rightarrow, \bot, \forall, (,)$ are symbols;
- v_n is a symbol for $n \in \mathbb{N}$;
- let $\mathrm{Var} = \{v_n | n \in \mathbb{N}\}$ be the class of *variables*;
- all symbols introduced so far are pairwise distinct.

Let S_0 be the class of basic symbols.

- A *relation symbol* is a symbol; a relation symbol R has an *arity* $\mathrm{ar}(R) \in \mathbb{N}$;
- a *propositional constant* is a relation symbol with arity 0;
- a *function symbol* is a symbol; a function symbol f has an *arity* $\mathrm{ar}(f) \in \mathbb{N}$;
- a *constant symbol* is a function symbol with arity 0.
- The classes of basic symbols, relation symbols and function symbols are pairwise disjoint.

A *language* is a class of relation symbols and function symbols.

Note that we do not specify the notion of *symbol* any further. This leaves room for freedom, so that we can treat “facecenteredPacking” as a symbol, as well as γ or $+, -, \ldots$. Some symbols have some convential functionalities: $\leqslant$ is usually taken as a *binary* relation symbol, i.e., $\mathrm{ar}(\leqslant) = 2$, and moreover is usually interpreted as some partial order.

We are now able to define specific languages:

Definition 2. *The* language of group theory *is the language*

$$S_{\mathrm{Gr}} = \{\circ, e\},$$

where $\circ$ *is a fixed binary function symbol and* e *is a fixed constant symbol.*

Definition 3. *The language of ordered fields is*

$$S_{\mathrm{OF}} = \{\leqslant, +, \cdot, 0, 1\}$$

where $\leqslant$ *is a binary relation symbol,* $+, \cdot$ *are binary function symbols, and* $0, 1$ *are constant symbols.*

Note 4. We are deliberately unspecific about the nature of mathematical objects and symbols. This allows to conduct logic within any theory that formalizes the notions introduced here. We shall use this later to obtain circular situations, where, e.g., the logic of set theory can be carried out *within* set theory. Such situations are the basis for the Gödel incompleteness theorems.

2.3 Words

Words:
A letter and a letter on a string
Will hold forever humanity spellbound
The Real Group

Definition 5. *Let S be a language. A* word over S *is a finite sequence $w = w_0 w_1 ... w_{n-1}$ of symbols $w_0, ..., w_{n-1} \in S_0 \cup S$. The natural number n is the* length *of w, we also write $|w| = n$.*

The empty word *is the unique sequence $\Box$ with $|\Box| = 0$. Let S^* be the class of all words over S.*

Definition 6. *Let $w = w_0 w_1 ... w_{m-1}$ and $w' = w'_0 w'_1 ... w'_{n-1}$ be words over S. Then the word*

$$w^\frown w' = w_0 w_1 ... w_{m-1} w'_0 w'_1 ... w'_{n-1}$$

is the concatenation *of w and w': $|w^\frown w'| = m + n$ and*

$$(w^\frown w')_i = \begin{cases} w_i\,,\ \text{if } i < m \\ w_{i-m}\ ,\ \text{if } m \leqslant i < m + n \end{cases}$$

We also write ww' instead of $w^\frown w'$.

If we consider words over $\{|\}$ of the form $||...|$ then their concatenation corresponds to addition of natural numbers. Numbers in decimal notation are words over $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$; a decimal addition $99 + 8 = 107$ is a *symbolic* operation of words, which corresponds to the addition operation in the natural numbers.

Exercise 1. The operation of concatenation satisfies some canonical laws:

a) $^\frown$ is associative: $(ww')w'' = w(w'w'')$.

b) $\emptyset$ is a neutral element for $^\frown$: $\emptyset w = w\emptyset = w$.

c) $^\frown$ satisfies cancelation: if $uw = u'w$ then $u = u'$; if $wu = wu'$ then $u = u'$.

2.4 Terms

Fix a language S.

Definition 7. *The class T^S of S-*terms *is the smallest subclass of S^* such that*

a) $x \in T^S$ for all variables x;

b) $ft_0...t_{n-1} \in T^S$ for all $n \in \mathbb{N}$, all n-ary function symbols $f \in S$, and all t_0, ..., $t_{n-1} \in T^S$.

Terms are written in *Polish* notation, meaning that function symbols come first and that no brackets are needed. Polish notation uses bracket-less *prefix* notations like $+v_0v_1$, whereas in algebra binary function symbols are usually written *infix*: $v_0 + v_1$.

Terms in T^S have *unique readings* according to the following

Lemma 8. *For every term $t \in T^S$ exactly one of the following holds:*

a) t is a variable;

b) there is a uniquely defined function symbol $f \in S$ and a uniquely defined sequence $t_0, ..., t_{n-1} \in T^S$ of terms, where f is n-ary, such that $t = ft_0...t_{n-1}$.

Proof. Exercise. □

Remark 9. Unique readability is essential for working with terms. Therefore if this Lemma would not hold one would have to alter the definition of terms or find workarounds.

Example 10. For the language $S_{\mathrm{Gr}} = \{\circ, e\}$ of group theory, terms in $T^{S_{\mathrm{Gr}}}$ look like

$$e, v_0, v_1, \ldots, \circ e e, \circ e v_m, \circ v_m e, \circ e e, \circ e \circ e e, \ldots, \circ v_i \circ v_j v_k, \circ \circ v_i v_j v_k, \ldots.$$

The standard infix notation $(t_0, t_1) \mapsto t_0 \circ t_1$ for terms does not have unique readability. The term $v_0 \circ v_1 \circ v_2$ can be read as

$$v_0 \circ v_1 \circ v_2 = (v_0 \circ v_1) \circ v_2 \quad \text{or} \quad v_0 \circ v_1 \circ v_2 = v_0 \circ (v_1 \circ v_2).$$

This corresponds to $\circ\circ v_0 v_1 v_2$ and $\circ v_0 \circ v_1 v_2$ in Polish notation. In contexts where the operation $\circ$ is associative, this might be fine and one may "leave out" some brackets.

Exercise 2. Show that every term $t \in T^{S_{\mathrm{Gr}}}$ has odd length $2n + 1$ where n is the number of $\circ$-symbols in t.

2.5 Formulas

Definition 11. *The class L^S of all S-*formulas *is the smallest subclass of S^* such that*

a) $\bot \in L^S$ *(the false formula);*

b) $t_0 \equiv t_1 \in L^S$ *for all S-terms $t_0, t_1 \in T^S$ (equality);*

c) $R t_0 \ldots t_{n-1} \in L^S$ *for all n-ary relation symbols $R \in S$ and all S-terms $t_0, \ldots, t_{n-1} \in T^S$ (relational formula);*

d) $\neg\varphi \in L^S$ *for all $\varphi \in L^S$ (negation);*

e) $(\varphi \to \psi) \in L^S$ *for all $\varphi, \psi \in L^S$ (implication);*

f) $\forall x \varphi \in L^S$ *for all $\varphi \in L^S$ and all variables x (universal quantification).*

L^S is also called the first-order language *over S. Formulas produced by conditions a) - c) only are called* atomic formulas *since they constitute the initial steps of the formula calculus.*

We restrict the language L^S to just the logical connectives $\bot$, $\neg$ and $\to$, and the quantifier $\forall$. The next definition introduces other connectives and quantifiers as convenient abbreviations for formulas in L^S. For theoretical considerations it is however advantageous to work with a "small" language.

Definition 12. *For S-formulas φ and ψ and a variable x write*

- $\top$ *("true") instead of* $\neg\bot$ *;*
- $(\varphi \vee \psi)$ *("φ or ψ") instead of* $(\neg\varphi \to \psi)$ *is the* disjunction *of φ, ψ ;*
- $(\varphi \wedge \psi)$ *("φ and ψ") instead of* $\neg(\varphi \to \neg\psi)$ *is the* conjunction *of φ, ψ ;*
- $(\varphi \leftrightarrow \psi)$ *("φ iff ψ") instead of* $((\varphi \to \psi) \wedge (\psi \to \varphi))$ *is the* equivalence *of φ, ψ ;*
- $\exists x \varphi$ *("for all x holds φ") instead of* $\neg\forall x \neg\varphi$ *is an* existential quantification.

For the sake of simplicity one often omits redundant brackets, in particular outer brackets. So we usually write $\varphi \vee \psi$ instead of $(\varphi \vee \psi)$.

Exercise 3. Formulate and prove the unique readability of formulas in L^S.

Exercise 4. Formulate the standard axioms of group theory in $L^{S_{\mathrm{Gr}}}$.

3 Semantics

We shall *interpret* formulas like $\forall y \exists x\, y = g(f(x))$ in adequate *structures*. The interaction between language and structures is also called *semantics*. Technically it will consist in "mapping" all syntactic material to semantic material centered around structures. We shall obtain a schema like:

$\forall$	domain A of a structure $\mathfrak{A}$
variable	element of A
function symbol	function on A
relation symbol	relation on A
term	element of A
formula	truth value
...	...

Fix a language S.

Definition 13. *An S*-structure *$\mathfrak{A}$ is determined by its "components":*

a) a nonempty set $|\mathfrak{A}|$; $|\mathfrak{A}|$ is called the underlying set *or the* domain *of $\mathfrak{A}$ and is often denoted by a corresponding plain letter, e.g., A;*

b) an n-ary relation $R^{\mathfrak{A}}$ on A for every n-ary relation symbol $R \in S$; i.e., $R^{\mathfrak{A}} \subseteq A^n$;

c) an n-ary function $f^{\mathfrak{A}}$ on A for every n-ary function symbol $f \in S$; i.e., $f^{\mathfrak{A}}: A^n \rightarrow A$.

Again we use customary and convenient notations for structures. In simple cases, one may simply list the components of the structure. If, e.g., when $S = \{R_0, R_1, f\}$ we may write

$$\mathfrak{A} = (A, R_0^{\mathfrak{A}}, R_1^{\mathfrak{A}}, f^{\mathfrak{A}})$$

or "$\mathfrak{A}$ has domain A with relations $R_0^{\mathfrak{A}}, R_1^{\mathfrak{A}}$ and an operation $f^{\mathfrak{A}}$".

A constant symbol $c \in S$ is interpreted by a 0-ary function $c^{\mathfrak{A}}$: $A^0 = \{0\} \rightarrow A$ which is defined for the single argument 0 and takes a single value $c^{\mathfrak{A}}(0)$ in A. It is natural to identify the function $c^{\mathfrak{A}}$ with ist constant value $c^{\mathfrak{A}}(0)$ and agree that $c^{\mathfrak{A}} \in A$.

One often uses the same notation for a structure and its underlying set like in

$$A = (A, R_0^{\mathfrak{A}}, R_1^{\mathfrak{A}}, f^{\mathfrak{A}}).$$

This "overloading" of notation is common in mathematics (and in natural language). Usually a reader is able to detect and "disambiguate" ambiguities introduced by multiple usage. There are techniques in computer science to deal with overloading, e.g., by *typing* of notions. Another common overloading is the naive identification of syntax and semantics, i.e., by writing

$$A = (A, R_0, R_1, f) \text{ instead of } A = (A, R_0^{\mathfrak{A}}, R_1^{\mathfrak{A}}, f^{\mathfrak{A}})$$

Since we are particularly interested in the interplay of syntax and semantics we shall try to avoid this kind of overloading.

Example 14. Define the language of *Boolean algebras* by

$$S_{\mathrm{BA}} = \{\wedge, \vee, -, 0, 1\}$$

where $\wedge$ and $\vee$ are binary function symbols for "and" and "or", $-$ is a unary function symbol for "not", and 0 and 1 are constant symbols. A Boolean algebra of particular importance in logic is the algebra $\mathbb{B}$ of *truth values*. Let $B = |\mathbb{B}| = \{\mathbb{F}, \mathbb{T}\}$ with $\mathbb{F} = 0^{\mathbb{B}}$(=false) and $\mathbb{T} = 1^{\mathbb{B}}$(=true). Define the operations `and` $= \wedge^{\mathbb{B}}$, `or` $= \vee^{\mathbb{B}}$, and `not` $= -^{\mathbb{B}}$ by *operation tables* in analogy with standard multiplication tables:

`and`	$\mathbb{F}$	$\mathbb{T}$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$
$\mathbb{T}$	$\mathbb{F}$	$\mathbb{T}$

,

`or`	$\mathbb{F}$	$\mathbb{T}$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{T}$
$\mathbb{T}$	$\mathbb{T}$	$\mathbb{T}$

, and

`not`	
$\mathbb{F}$	$\mathbb{T}$
$\mathbb{T}$	$\mathbb{F}$

.

Note that we use the non-exclusive "or" instead of the exclusive "either - or".

Exercise 5. Show that every *truth-function* $F\colon B^n \to B$ can be obtained as a composition of the functions `and` and `not`.

The notion of structure leads to derived definitions.

Definition 15. *Let $\mathfrak{A}$ be an S-structure and $\mathfrak{A}'$ be an S'-structure. Then $\mathfrak{A}$ is a* reduct *of $\mathfrak{A}'$, or $\mathfrak{A}'$ is an* expansion *of $\mathfrak{A}$, if*

- $S \subseteq S'$;
- $|\mathfrak{A}| = |\mathfrak{A}'|$;
- $R^{\mathfrak{A}} = R^{\mathfrak{A}'}$ *for every relation symbol* $R \in S$;
- $f^{\mathfrak{A}} = f^{\mathfrak{A}'}$ *for every function symbol* $f \in S$.

According to this definition, the additive group $(\mathbb{R}, +, 0)$ of reals is a reduct of the field $(\mathbb{R}, +, \cdot, 0, 1)$.

Definition 16. *Let $\mathfrak{A}, \mathfrak{B}$ be S-structures. Then $\mathfrak{A}$ is a* substructure *of $\mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{B}$, if $\mathfrak{B}$ is a pointwise extension of $\mathfrak{A}$, i.e.,*

a) $A = |\mathfrak{A}| \subseteq |\mathfrak{B}|$;

b) for every n-ary relation symbol $R \in S$ we have $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$;

c) for every n-ary function symbol $f \in S$ we have $f^{\mathfrak{A}} = f^{\mathfrak{B}} \upharpoonright A^n$.

Note that the substructure $\mathfrak{A}$ of $\mathfrak{B}$ is determined by its domain A. Also, A needs to be closed under the functions $f^{\mathfrak{B}}$ for f a function symbol in S.

Definition 17. *Let $\mathfrak{A}, \mathfrak{B}$ be S-structures and $h\colon |\mathfrak{A}| \to |\mathfrak{B}|$. Then h is a* homomorphism *from $\mathfrak{A}$ into $\mathfrak{B}$, $h\colon \mathfrak{A} \to \mathfrak{B}$, if*

a) for every n-ary relation symbol $R \in S$ and for every $a_0, \ldots, a_{n-1} \in A$

$$R^{\mathfrak{A}}(a_0, \ldots, a_{n-1}) \text{ implies } R^{\mathfrak{B}}(h(a_0), \ldots, h(a_{n-1}));$$

b) for every n-ary function symbol $f \in S$ and for every $a_0, \ldots, a_{n-1} \in A$

$$f^{\mathfrak{B}}(h(a_0), \ldots, h(a_{n-1})) = h(f^{\mathfrak{A}}(a_0, \ldots, a_{n-1})).$$

h is an embedding *of $\mathfrak{A}$ into $\mathfrak{B}$, $h\colon \mathfrak{A} \hookrightarrow \mathfrak{B}$, if moreover*

a) h is injective;

b) for every n-ary relation symbol $R \in S$ and for every $a_0, \ldots, a_{n-1} \in A$

$$R^{\mathfrak{A}}(a_0, \ldots, a_{n-1}) \text{ iff } R^{\mathfrak{B}}(h(a_0), \ldots, h(a_{n-1})).$$

If h is also bijective, it is called an isomorphism.

Exercise 6. A composition of homomorphisms is a homomorphism. What about products of structures? The embedding of $\mathfrak{A}$ into the diagonal of $\mathfrak{A} \times \mathfrak{A}$ is a homomorphism. Direct limits? Homomorphism into direct limit.

4 The satisfaction relation

> *"What is truth?" Pilate asked.*
> John 18:38

An S-structure interprets the symbols in S. To interpret a formula in a structure, one also has to interpret the (occuring) variables.

Definition 18. *Let S be a language. An S-*model $\mathfrak{M}$ *is an S-structure together with values $v_n^{\mathfrak{M}} \in M$ for every $n \in \mathbb{N}$. The function $n \mapsto v_n^{\mathfrak{M}}$ is an* assignment *of variables.*

We shall need to modify the values of a model $\mathfrak{M}$ at specific variables: For pairwise distinct variables $x_0, \ldots, x_{r-1} \in \mathrm{Var}$ and $a_0, \ldots, a_{r-1} \in M$ define

$$\mathfrak{M}' = \mathfrak{M}\frac{a_0 \ldots a_{r-1}}{x_0 \ldots x_{r-1}}$$

by letting $\mathfrak{M}' = \mathfrak{M}$ as S-structures and, for $n \in \mathbb{N}$,

$$v_n^{\mathfrak{M}'} = \begin{cases} a_i\,, \text{ if } v_n = x_i \text{ for some index } i < r \\ v_n^{\mathfrak{M}}\,, \text{ else} \end{cases}$$

We now define the *semantics* of first-order languages by interpreting terms and formulas in models.

Definition 19. *Let $\mathfrak{M}$ be an S-model. Define the* interpretation $t^{\mathfrak{M}} \in M$ *of a term $t \in T^S$ by recursion:*

a) for t a variable, $t^{\mathfrak{M}}$ is already defined;

b) for an n-ary function symbol and terms $t_0, \ldots, t_{n-1} \in T^S$, let

$$(f t_0 \ldots . t_{n-1})^{\mathfrak{M}} = f^{\mathfrak{M}}(t_0^{\mathfrak{M}}, \ldots, t_{n-1}^{\mathfrak{M}}).$$

This explains, e.g., the interpretation of a term like $v_3^2 + v_{200}^3$ in the reals under an assignment of variables.

Definition 20. *Let $\mathfrak{M}$ be an S-model. Define the* interpretation $\varphi^{\mathfrak{M}} \in \mathbb{B}$ *of a formula $\varphi \in L^S$, where $\mathbb{B} = \{\mathbb{F}, \mathbb{T}\}$ is the Boolean algebra of truth values, by recursion on the formula calculus:*

a) $\perp^{\mathfrak{M}} = \mathbb{F}$;

b) for terms $t_0, t_1 \in T^S$*:* $(t_0 \equiv t_1)^{\mathfrak{M}} = \mathbb{T}$ *iff* $t_0^{\mathfrak{M}} = t_1^{\mathfrak{M}}$*;*

c) for every n-ary relation symbol $R \in S$ *and terms* $t_0, ..., t_1 \in T^S$

$$(Rt_0...t_{n-1})^{\mathfrak{M}} = \mathbb{T} \text{ iff } R^{\mathfrak{M}}(t_0^{\mathfrak{M}}, ..., t_{n-1}^{\mathfrak{M}});$$

d) $(\neg\varphi)^{\mathfrak{M}} = \mathbb{T}$ *iff* $\varphi^{\mathfrak{M}} = \mathbb{F}$ *;*

e) $(\varphi \rightarrow \psi)^{\mathfrak{M}} = \mathbb{T}$ *iff* $\varphi^{\mathfrak{M}} = \mathbb{T}$ *implies* $\psi^{\mathfrak{M}} = \mathbb{T}$*;*

f) $(\forall v_n \varphi)^{\mathfrak{M}} = \mathbb{T}$ *iff for all* $a \in M$ *we have* $\varphi^{\mathfrak{M}\frac{a}{v_n}} = \mathbb{T}$.

We write $\mathfrak{M} \vDash \varphi$ *instead of* $\varphi^{\mathfrak{M}} = \mathbb{T}$. *We also say that* $\mathfrak{M}$ satisfies φ *or that* φ holds *in* $\mathfrak{M}$ *or that* φ *is* true *in* $\mathfrak{M}$. *For* $\Phi \subseteq L^S$ *write* $\mathfrak{M} \vDash \Phi$ *iff* $\mathfrak{M} \vDash \varphi$ *for every* $\varphi \in \Phi$.

Definition 21. *Let S be a language and* $\Phi \subseteq L^S$. Φ *is* universally valid *if* Φ *holds in every S-model.* Φ *is* satisfiable *if there is an S-model* $\mathfrak{M}$ *such that* $\mathfrak{M} \vDash \Phi$.

The language extension by the (abbreviating) symbols $\vee, \wedge, \leftrightarrow, \exists$ is consistent with the expected meanings of the additional symbols:

Exercise 7. Prove:

a) $\mathfrak{M} \vDash (\varphi \vee \psi)$ iff $\mathfrak{M} \vDash \varphi$ *or* $\mathfrak{M} \vDash \psi$;

b) $\mathfrak{M} \vDash (\varphi \wedge \psi)$ iff $\mathfrak{M} \vDash \varphi$ *and* $\mathfrak{M} \vDash \psi$;

c) $\mathfrak{M} \vDash (\varphi \leftrightarrow \psi)$ iff $\mathfrak{M} \vDash \varphi$ *is equivalent to* $\mathfrak{M} \vDash \psi$;

d) $\mathfrak{M} \vDash \exists v_n \varphi$ iff *there exists* $a \in |\mathfrak{M}|$ such that $\mathfrak{M}\frac{a}{v_n} \vDash \varphi$.

With the notion of $\vDash$ we can now formally define what it means for a structure to be a group or for a function to be differentiable. Before considering examples we make some auxiliary definitions and simplifications.

It is intuitively obvious that the interpretation of a term only depends on the occuring variables, and that satisfaction for a formula only depends on its free, non-bound variables.

Definition 22. *For* $t \in T^S$ *let* $\mathrm{var}(t)$ *be the finite set of variables occuring in t.*

Theorem 23. *Let t be an S-term and let* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *be S-models which agree as S-structures. Assume* $x^{\mathfrak{M}} = x^{\mathfrak{M}'}$ *for all* $x \in \mathrm{var}(t)$. *Then* $t^{\mathfrak{M}} = t^{\mathfrak{M}'}$.

Definition 24. *Für* $\varphi \in L^S$ *define the set of* free variables $\mathrm{free}(\varphi) \subseteq \{v_n | n \in \mathbb{N}\}$ *by recursion on (the lengths of) formulas:*

- $\mathrm{free}(\bot) = \emptyset$
- $\mathrm{free}(t_0 \equiv t_1) = \mathrm{var}(t_0) \cup \mathrm{var}(t_1)$*;*
- $\mathrm{free}(Rt_0...t_{n-1}) = \mathrm{var}(t_0) \cup ... \cup \mathrm{var}(t_{n-1})$*;*
- $\mathrm{free}(\neg\varphi) = \mathrm{free}(\varphi)$*;*
- $\mathrm{free}(\varphi \rightarrow \psi) = \mathrm{free}(\varphi) \cup \mathrm{free}(\psi)$.
- $\mathrm{free}(\forall x \varphi) = \mathrm{free}(\varphi) \setminus \{x\}$.

For $\Phi \subseteq L^S$ *define the class* free(Φ) *of* free variables *as*

$$\mathrm{free}(\Phi) = \bigcup_{\varphi \in \Phi} \mathrm{free}(\varphi) .$$

Example 25.

$$\begin{array}{rcl}\mathrm{free}(Ryx \rightarrow \forall y \neg y = z) & = & \mathrm{free}(Ryx) \cup \mathrm{free}(\forall y \neg y = z)\\ & = & \mathrm{free}(Ryx) \cup (\mathrm{free}(\neg y = z) \setminus \{y\})\\ & = & \mathrm{free}(Ryx) \cup (\mathrm{free}(y = z) \setminus \{y\})\\ & = & \{y, x\} \cup (\{y, z\} \setminus \{y\})\\ & = & \{y, x\} \cup \{z\}\\ & = & \{x, y, z\}.\end{array}$$

Definition 26.

a) For $n \in \mathbb{N}$ let $L_n^S = \{\varphi \in L^S \mid \mathrm{free}(\varphi) \subseteq \{v_0, \ldots, v_{n-1}\}\}$.

*b) $\varphi \in L^S$ is an S-*sentence *if* free$(\varphi) = \emptyset$*; L_0^S is the class of S-sentences.*

Theorem 27. *Let t be an S-term and let $\mathfrak{M}$ and $\mathfrak{M}'$ be S-models which agree as S-structures. Assume $x^{\mathfrak{M}} = x^{\mathfrak{M}'}$ for all $x \in$* free(t)*. Then*

$$\mathfrak{M} \vDash \varphi \quad \textit{iff} \quad \mathfrak{M}' \vDash \varphi.$$

Proof. By induction on φ.
$\varphi = t_0 \equiv t_1$: Then $\mathrm{var}(t_0) \cup \mathrm{var}(t_1) = \mathrm{free}(\varphi)$ and

$$\begin{array}{rl}\mathfrak{M} \vDash \varphi & \text{iff } t_0^{\mathfrak{M}} = t_1^{\mathfrak{M}}\\ & \text{iff } t_0^{\mathfrak{M}'} = t_1^{\mathfrak{M}'} \text{ by the previous Theorem,}\\ & \text{iff } \mathfrak{M}' \vDash \varphi.\end{array}$$

$\varphi = \psi \rightarrow \chi$ and assume the claim to be true for ψ and χ. Then

$$\begin{array}{rl}\mathfrak{M} \vDash \varphi & \text{iff } \mathfrak{M} \vDash \psi \text{ implies } \mathfrak{M} \vDash \chi\\ & \text{iff } \mathfrak{M}' \vDash \psi \text{ implies } \mathfrak{M}' \vDash \chi \text{ by the inductive assumption,}\\ & \text{iff } \mathfrak{M}' \vDash \varphi.\end{array}$$

$\varphi = \forall v_n \psi$ and assume the claim to be true for ψ. Then $\mathrm{free}(\psi) \subseteq \mathrm{free}(\varphi) \cup \{v_n\}$. For all $a \in |\mathfrak{M}|$: $\mathfrak{M}\frac{a}{v_n} \restriction \mathrm{free}(\psi) = \mathfrak{M}'\frac{a}{v_n} \restriction \mathrm{free}(\psi)$, i.e., the structures agree on the free variables of ψ,

$$\begin{array}{rl}\mathfrak{M} \vDash \varphi & \text{iff for all } a \in M \text{ holds } \mathfrak{M}\dfrac{a}{v_n} \vDash \psi\\ & \text{iff for all } a \in M \text{ holds } \mathfrak{M}'\dfrac{a}{v_n} \vDash \psi \text{ by the inductive assumption,}\\ & \text{iff } \mathfrak{M}' \vDash \varphi.\end{array}$$

□

This allows further simplifications in notations for $\vDash$:

Definition 28. *Let $\mathfrak{A}$ be an S-structure and let $(a_0, \ldots, a_{n-1})$ be a sequence of elements of A. Let t be an S-term with* var$(t) \subseteq \{v_0, \ldots, v_{n-1}\}$*. Then define*

$$t^{\mathfrak{A}}[a_0, \ldots, a_{n-1}] = t^{\mathfrak{M}},$$

where the model $\mathfrak{M}$ *is the structure* $\mathfrak{A}$ *together with some (or any) assignment such that* $v_0^{\mathfrak{M}} = a_0, \ldots, v_{n-1}^{\mathfrak{M}} = a_{n-1}$.
Let φ *be an S-formula with* $\operatorname{free}(\varphi) \subseteq \{v_0, \ldots, v_{n-1}\}$. *Then define*

$$\mathfrak{A} \vDash \varphi[a_0, \ldots, a_{n-1}] \quad \textit{iff} \quad \mathfrak{M} \vDash \varphi,$$

where the model $\mathfrak{M}$ *is the structure* $\mathfrak{A}$ *together with some (or any) assignment such that* $v_0^{\mathfrak{M}} = a_0, \ldots, v_{n-1}^{\mathfrak{M}} = a_{n-1}$.

In case $n = 0$ *we also write* $t^{\mathfrak{A}}$ *instead of* $t^{\mathfrak{A}}[a_0, \ldots, a_{n-1}]$, *and* $\mathfrak{A} \vDash \varphi$ *instead of* $\mathfrak{A} \vDash \varphi[a_0, \ldots, a_{n-1}]$. *In the latter case we also say:* $\mathfrak{A}$ *is a* model *of* φ, $\mathfrak{A}$ satisfies φ *or* φ is true *in* $\mathfrak{A}$.

For $\Phi \subseteq L_0^S$ *a class of sentences also write*

$$\mathfrak{A} \vDash \Phi \quad \textit{iff for all} \quad \varphi \in \Phi \ \textit{holds}\colon \mathfrak{A} \vDash \varphi.$$

Example 29. *Groups.* S_{Gr}: $=\{\circ, \ e\}$ with a binary function symbol $\circ$ and a constant symbol e is the *language of groups theory*. The group axioms are

a) $\forall v_0 \forall v_1 \forall v_2 \circ v_0 \circ v_1 v_2 \equiv \circ\circ v_0 v_1 v_2$;

b) $\forall v_0 \circ v_0 e \equiv v_0$;

c) $\forall v_0 \exists v_1 \circ v_0 v_1 \equiv e$.

This defines the axiom set

$$\Phi_{\mathrm{Gr}} = \{\forall v_0 \forall v_1 \forall v_2 \circ v_0 \circ v_1 v_2 \equiv \circ\circ v_0 v_1 v_2, \forall v_0 \circ v_0 e \equiv v_0 t_0^{\mathfrak{M}} \ldots t_{r-1}^{\mathfrak{M}}, \forall v_0 \exists v_1 \circ v_0 v_1 \equiv e\}.$$

An S-structure $\mathfrak{G} = (G, *, k) = (G, \circ^{\mathfrak{G}}, e^{\mathfrak{G}})$ satisfies Φ_{Gr} iff it is a group in the ordinary sense.

Definition 30. *Let S be a language and let* $\Phi \subseteq L_0^S$ *be a class of S-sentences. Then*

$$\mathrm{Mod}^S \Phi = \{\mathfrak{A} \mid \mathfrak{A} \textit{ is an S-structure and } \mathfrak{A} \vDash \Phi\}$$

is the model class *of* Φ. *In case* $\Phi = \{\varphi\}$ *we also write* $\mathrm{Mod}^S \varphi$ *instead of* $\mathrm{Mod}^S \Phi$. *We also say that* Φ *is an* axiom system *for* $\mathrm{Mod}^S \Phi$, *or that* Φ axiomatizes *the class* $\mathrm{Mod}^S \Phi$.

Thus $\mathrm{Mod}^{S_{\mathrm{Gr}}} \Phi_{\mathrm{Gr}}$ is the model class of all groups. Model classes are studied in generality within *model theory* which is a branch of mathematical logic. For specific axiom systems Φ the model class $\mathrm{Mod}^S \Phi$ is examined in subfields of mathematics: group theory, ring theory, graph theory, etc. Some typical questions questions are: is $\mathrm{Mod}^S \Phi \neq \emptyset$, i.e., is Φ satisfiable? What are the elements of $\mathrm{Mod}^S \Phi$? Can one classify the isomorphism classes of models? What are the cardinalities of models?

Exercise 8. One may consider $\mathrm{Mod}^S \Phi$ with appropriate morphisms as a category. In certain cases this category has closure properties like closure under products. One can give the categorial definition of cartesian product and show their existence under certain assumptions on Φ.

5 Logical implication and propositional connectives

> *The design of the following treatise is to investigate the fundamental laws of those operations of the mind by which reasoning is performed; to give expression to them in the symbolical language of a Calculus, and upon this foundation to establish the science of Logic and construct its method.*
> George Boole, The Laws of Thought

Definition 31. *For a symbol class S and $\Phi \subseteq L^S$ and $\varphi \in L^S$ define that Φ* (logically) implies *φ ($\Phi \vDash \varphi$) iff every S-model $\mathfrak{I} \vDash \Phi$ is also a model of φ.*

Note that logical implication $\vDash$ is a relation between *syntactical* entities which is defined via the *semantic* notion of interpretation. The relation $\Phi \vDash ?$ can be viewed as the central relation in modern axiomatic mathematics: given the assumptions Φ what do they imply? The $\vDash$-relation is usually verified by mathematical *proofs*. These proofs seem to refer to the exploration of some domain of mathematical objects and, in practice, require particular mathematical skills and ingenuity.

We will however show that the logical implication $\vDash$ satisfies certain simple syntactical laws. These laws correspond to ordinary proof methods but are purely formal. Amazingly a finite list of methods will (in principle) suffice for all mathematical proofs. This is Gödel's completeness theorem that we shall prove later.

Theorem 32. *Let S be a language, $t \in T^S$, $\varphi, \psi \in L^S$, and $\Gamma, \Phi \subseteq L^S$. Then*

a) (Monotonicity) If $\Gamma \subseteq \Phi$ and $\Gamma \vDash \varphi$ then $\Phi \vDash \varphi$.

b) (Assumption property) If $\varphi \in \Gamma$ then $\Gamma \vDash \varphi$.

c) ($\rightarrow$-Introduction) If $\Gamma \cup \varphi \vDash \psi$ then $\Gamma \vDash (\varphi \rightarrow \psi)$.

d) ($\rightarrow$-Elimination) If $\Gamma \vDash \varphi$ and $\Gamma \vDash (\varphi \rightarrow \psi)$ then $\Gamma \vDash \psi$.

e) ($\bot$-Introduction) If $\Gamma \vDash \varphi$ and $\Gamma \vDash \neg\varphi$ then $\Gamma \vDash \bot$.

f) ($\bot$-Elimination) If $\Gamma \cup \{\neg\varphi\} \vDash \bot$ then $\Gamma \vDash \varphi$.

g) ($\equiv$-Introduction) $\Gamma \vDash t \equiv t$.

Proof. f) Assume $\Gamma \cup \{\neg\varphi\} \vDash \bot$. Consider an S-model with $\mathfrak{M} \vDash \Gamma$. Assume that $\mathfrak{M} \nvDash \varphi$. Then $\mathfrak{M} \vDash \neg\varphi$. $\mathfrak{M} \vDash \Gamma \cup \{\neg\varphi\}$, and by assumption, $\mathfrak{M} \vDash \bot$. But by the definition of the satisfaction relation, this is false. Thus $\mathfrak{M} \vDash \varphi$. Thus $\Gamma \vDash \varphi$. □

Exercise 9. There are similar rules for the introduction and elimination of junctors like $\wedge$ and $\vee$ that we have introduced as abbreviations:

a) ($\wedge$-Introduction) If $\Gamma \vDash \varphi$ and $\Gamma \vDash \psi$ then $\Gamma \vDash \varphi \wedge \psi$.

b) ($\wedge$-Elimination) If $\Gamma \vDash \varphi \wedge \psi$ then $\Gamma \vDash \varphi$ and $\Gamma \vDash \psi$.

c) ($\vee$-Introduction) If $\Gamma \vDash \varphi$ then $\Gamma \vDash \varphi \vee \psi$ and $\Gamma \vDash \psi \vee \varphi$.

d) ($\vee$-Elimination) If $\Gamma \vDash \varphi \vee \psi$ and $\Gamma \vdash \neg\varphi$ then $\Gamma \vDash \psi$.

6 Substitution and term rules

To prove further rules for equality and quantification, we first have to consider the *substitution* of terms in formulas.

Definition 33. *For a term $s \in T^S$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$ define the* (simultaneous) substitution

$$s\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$$

of $t_0, \ldots, t_{r-1}$ for $x_0, \ldots, x_{r-1}$ by recursion:

a) $x\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = \begin{cases} x, \text{if } x \neq x_0, \ldots, x \neq x_{r-1} \\ t_i\,, \text{ if } x = x_i \end{cases}$ for all variables x;

b) $(fs_0...s_{n-1})\frac{t_0....t_{r-1}}{x_0...x_{r-1}} = fs_0\frac{t_0....t_{r-1}}{x_0...x_{r-1}}...s_{n-1}\frac{t_0....t_{r-1}}{x_0...x_{r-1}}$ *for all n-ary function symbols $f\in S$.*

Note that the *simultaneous* substitution

$$s\frac{t_0....t_{r-1}}{x_0...x_{r-1}}$$

is in general different from a *successive* substitution

$$s\frac{t_0}{x_0}\frac{t_1}{x_1}...\frac{t_{r-1}}{x_{r-1}}$$

which depends on the order of substitution. E.g., $x\frac{yx}{xy} = y$, $x\frac{y}{x}\frac{x}{y} = y\frac{x}{y} = x$ and $x\frac{x}{y}\frac{y}{x} = x\frac{y}{x} = y$.

The following *substitution theorem* shows that syntactic substitution corresponds semantically to a (simultaneous) modification of assignments by interpreted terms.

Theorem 34. *Consider an S-model $\mathfrak{M}$, pairwise distinct variables $x_0, ..., x_{r-1}$ and terms $t_0, ..., t_{r-1}\in T^S$. Then for any S-term s:*

$$\mathfrak{M}(s\frac{t_0...t_{r-1}}{x_0...x_{r-1}}) = \mathfrak{M}\frac{t_0^{\mathfrak{M}}...t_{r-1}^{\mathfrak{M}}}{x_0...x_{r-1}}(s).$$

Proof. By induction on the complexity of s.
Case 1: $s = x$.
Case 1.1: $x\notin\{x_0, ..., x_{r-1}\}$. Then

$$\mathfrak{M}(x\frac{t_0...t_{r-1}}{x_0...x_{r-1}}) = \mathfrak{M}(x) = \mathfrak{M}\frac{t_0^{\mathfrak{M}}...t_{r-1}^{\mathfrak{M}}}{x_0...x_{r-1}}(x).$$

Case 1.2: $x = x_i$. Then

$$\mathfrak{M}(x\frac{t_0...t_{r-1}}{x_0...x_{r-1}}) = \mathfrak{M}(t_i) = \mathfrak{M}\frac{t_0^{\mathfrak{M}}...t_{r-1}^{\mathfrak{M}}}{x_0...x_{r-1}}(x_i) = \mathfrak{M}\frac{t_0^{\mathfrak{M}}...t_{r-1}^{\mathfrak{M}}}{x_0...x_{r-1}}(x).$$

Case 2: $s = fs_0...s_{n-1}$ where $f\in S$ is an n-ary function symbol and the terms s_0, ..., $s_{n-1}\in T^S$ satisfy the theorem. Then

$$\begin{aligned}\mathfrak{M}((fs_0...s_{n-1})\frac{t_0...t_{r-1}}{x_0...x_{r-1}}) &= \mathfrak{M}(fs_0\frac{t_0...t_{r-1}}{x_0...x_{r-1}}...s_{n-1}\frac{t_0...t_{r-1}}{x_0...x_{r-1}})\\ &= f^{\mathfrak{M}}(\mathfrak{M}(s_0\frac{t_0...t_{r-1}}{x_0...x_{r-1}}), ..., \mathfrak{M}(s_{n-1}\frac{t_0...t_{r-1}}{x_0...x_{r-1}}))\\ &= \mathfrak{M}(f)(\mathfrak{M}\frac{t_0^{\mathfrak{M}}...t_{r-1}^{\mathfrak{M}}}{x_0...x_{r-1}}(s_0),\\ &\qquad ..., \mathfrak{M}\frac{t_0^{\mathfrak{M}}...t_{r-1}^{\mathfrak{M}}}{x_0...x_{r-1}}(s_{n-1}))\\ &= \mathfrak{M}\frac{t_0^{\mathfrak{M}}...t_{r-1}^{\mathfrak{M}}}{x_0...x_{r-1}}(fs_0...s_{n-1}).\end{aligned}$$

□

Definition 35. *For a formula $\varphi\in L^S$, pairwise distinct variables $x_0, ..., x_{r-1}$ and terms $t_0, ..., t_{r-1}\in T^S$ define the* (simultaneous) substitution

$$\varphi\frac{t_0....t_{r-1}}{x_0...x_{r-1}}$$

of $t_0, \ldots, t_{r-1}$ *for* $x_0, \ldots, x_{r-1}$ *by recursion:*

a) $(s_0 \equiv s_1)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = s_0\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} \equiv s_1\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *for all terms* $s_0, s_1 \in T^S$*;*

b) $(R s_0\ldots s_{n-1})\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = R s_0\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}\ldots s_{n-1}\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *for all* n*-ary relation symbols* $R \in s$ *and terms* $s_0, \ldots, s_{n-1} \in T^S$*;*

c) $(\neg\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = \neg(\varphi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}})$*;*

d) $(\varphi \to \psi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = (\varphi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} \to \psi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}})$*;*

e) for $(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *we proceed in two steps: let* $x_{i_0}, \ldots, x_{i_{s-1}}$ *with* $i_0 < \ldots < i_{s-1}$ *be exactly those* x_i *which are "relevant" for the substitution, i.e.,* $x_i \in \mathrm{free}(\forall x\varphi)$ *and* $x_i \neq t_i$*.*

- *if* x *does not occur in* $t_{i_0}, \ldots, t_{i_{s-1}}$*, then set*

$$(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = \forall x\,(\varphi\frac{t_{i_0}\ldots t_{i_{s-1}}}{x_{i_0}\ldots x_{i_{s-1}}}).$$

- *if* x *does occur in* $t_{i_0}, \ldots, t_{i_{s-1}}$*, then let* $k \in \mathbb{N}$ *minimal such that* v_k *does not occur in* φ*,* $t_{i_0}, \ldots, t_{i_{s-1}}$ *and set*

$$(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = \forall v_k\,(\varphi\frac{t_{i_0}\ldots t_{i_{s-1}} v_k}{x_{i_0}\ldots x_{i_{s-1}} x}).$$

The *substitution theorem* for formulas again shows that syntactic substitutions and a modifications of assignments correspond. The definition of substitution is designed to make the substitution theorem true. There are variants of the syntactical substitution which would also satisfy the substitution theorem.

Theorem 36. *Consider an* S*-model* $\mathfrak{M}$*, pairwise distinct variables* $x_0, \ldots, x_{r-1}$ *and terms* $t_0, \ldots, t_{r-1} \in T^S$*. If* $\varphi \in L^S$ *is a formula,*

$$\mathfrak{M} \vDash \varphi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} \text{ iff } \mathfrak{M}\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}}{x_0\ldots x_{r-1}} \vDash \varphi.$$

Proof. By induction on the complexity of φ. There is nothing to show for $\varphi = \bot$.
Case 1: $\varphi = R s_0\ldots s_{n-1}$. Then

$$\begin{aligned}
\mathfrak{M} \vDash (R s_0\ldots s_{n-1})\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} \quad & \text{iff } \mathfrak{M} \vDash R s_0\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}\ldots s_{n-1}\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} \\
& \text{iff } R^{\mathfrak{M}}\left(\mathfrak{M}(s_0\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}), \ldots, \mathfrak{M}(s_1\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}})\right) \\
& \text{iff } R^{\mathfrak{M}}\left(\mathfrak{M}\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}}{x_0\ldots x_{r-1}}(s_0),\right. \\
& \qquad\qquad \left.\ldots, \mathfrak{M}\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}}{x_0\ldots x_{r-1}}(s_{n-1})\right) \\
& \text{iff } \mathfrak{M}\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}}{x_0\ldots x_{r-1}} \vDash R s_0\ldots s_{n-1}
\end{aligned}$$

Equations $s_0 \equiv s_1$ can be treated as a special case of the relational case. Propositional combinations of formulas by $\bot$, $\neg$ and $\rightarrow$ behave similar to terms; indeed formulas can be viewed as terms whose values are truth values. So we are left with universal quantification.
Case 2: $\varphi = (\forall x \psi)\frac{t_0 \ldots . t_{r-1}}{x_0 \ldots x_{r-1}}$, assuming that the theorem holds for ψ.

We proceed according to our definition of syntactic substitution. Let $x_{i_0}, \ldots, x_{i_{s-1}}$ with $i_0 < \ldots < i_{s-1}$ be exactly those x_i such that $x_i \in \operatorname{free}(\forall x \psi)$ and $x_i \neq t_i$. Since

$$\mathfrak{M}\frac{t_0^{\mathfrak{M}} \ldots t_{r-1}^{\mathfrak{M}}}{x_0 \ldots x_{r-1}} \vDash \varphi \text{ iff } \mathfrak{M}\frac{t_{i_0}^{\mathfrak{M}} \ldots t_{i_{r-1}}^{\mathfrak{M}}}{x_{i_0} \ldots x_{i_{s-1}}} \vDash \varphi,$$

we can assume that $(x_0, \ldots, x_{r-1}) = (x_{i_0}, \ldots, x_{i_{s-1}})$, i.e., every x_i is free in $\forall x \psi$, $x_i \neq x$, and $x_i \neq t_i$. Now follow the two cases in the definition of the substitution:

Case 2.1: The variable x does not occur in $t_0, \ldots., t_{r-1}$ and

$$(\forall x \psi)\frac{t_0 \ldots . t_{r-1}}{x_0 \ldots x_{r-1}} = \forall x \, (\psi \frac{t_0 \ldots . t_{r-1}}{x_0 \ldots x_{r-1}}).$$

$$\begin{aligned}
\mathfrak{M} \vDash (\forall x \psi)\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \quad & \text{iff} \quad \mathfrak{M} \vDash \forall x \, (\psi \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}) \\
& \text{iff} \quad \text{for all } a \in M \text{ holds } \mathfrak{M}\frac{a}{x} \vDash \psi \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \\
& \qquad \text{(definition of } \vDash) \\
& \text{iff} \quad \text{for all } a \in M \text{ holds} \\
& \qquad (\mathfrak{M}\frac{a}{x})\frac{t_0^{\mathfrak{M}\frac{a}{x}} \ldots t_{r-1}^{\mathfrak{M}\frac{a}{x}}}{x_0 \ldots x_{r-1}} \vDash \psi \\
& \qquad \text{(by the inductive hypothesis for } \psi) \\
& \text{iff} \quad \text{for all } a \in M \text{ holds} \\
& \qquad (\mathfrak{M}\frac{a}{x})\frac{t_0^{\mathfrak{M}} \ldots t_{r-1}^{\mathfrak{M}}}{x_0 \ldots x_{r-1}} \vDash \psi \\
& \qquad \text{(since } x \text{ does not occur in } t_i) \\
& \text{iff} \quad \text{for all } a \in M \text{ holds} \\
& \qquad \mathfrak{M}\frac{t_0^{\mathfrak{M}} \ldots t_{r-1}^{\mathfrak{M}} \, a}{x_0 \ldots x_{r-1} \, x} \vDash \psi \\
& \qquad \text{(since } x \text{ does not occur in } x_0, \ldots, x_{r-1}) \\
& \text{iff} \quad \text{for all } a \in M \text{ holds} \\
& \qquad (\mathfrak{M}\frac{t_0^{\mathfrak{M}} \ldots t_{r-1}^{\mathfrak{M}}}{x_0 \ldots x_{r-1}})\frac{a}{x} \vDash \psi \\
& \qquad \text{(by simple properties of assignments)} \\
& \text{iff} \quad \mathfrak{M}\frac{t_0^{\mathfrak{M}} \ldots t_{r-1}^{\mathfrak{M}}}{x_0 \ldots x_{r-1}} \vDash \forall x \psi
\end{aligned}$$

Case 2.2: The variable x occurs in $t_0, \ldots., t_{r-1}$. Then

$$(\forall x \psi)\frac{t_0 \ldots . t_{r-1}}{x_0 \ldots x_{r-1}} = \forall v_k \, (\psi \frac{t_0 \ldots . t_{r-1} v_k}{x_0 \ldots x_{r-1} x}),$$

where $k\in\mathbb{N}$ is minimal such that v_k does not occur in φ, $t_{i_0}, \ldots., t_{i_{s-1}}$.

$$\begin{aligned}
\mathfrak{M}\vDash(\forall x\psi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} \quad &\text{iff}\quad \mathfrak{M}\vDash\forall v_k\,(\psi\frac{t_0\ldots.t_{r-1}v_k}{x_0\ldots x_{r-1}x})\\
&\text{iff}\quad \text{for all } a\in M \text{ holds } \mathfrak{M}\frac{a}{v_k}\vDash\psi\frac{t_0\ldots t_{r-1}v_k}{x_0\ldots x_{r-1}x}\\
&\text{iff}\quad \text{for all } a\in M \text{ holds}\\
&\qquad (\mathfrak{M}\frac{a}{v_k})\frac{t_0^{\mathfrak{M}\frac{a}{v_k}}\ldots t_{r-1}^{\mathfrak{M}\frac{a}{v_k}}\, v_k^{\mathfrak{M}\frac{a}{v_k}}}{x_0\ldots x_{r-1}\,x}\vDash\psi\\
&\qquad \text{(inductive hypothesis for } \psi)\\
&\text{iff}\quad \text{for all } a\in M \text{ holds}\\
&\qquad (\mathfrak{M}\frac{a}{x})\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}\,a}{x_0\ldots x_{r-1}x}\vDash\psi\\
&\qquad \text{(since } v_k \text{ does not occur in } t_i)\\
&\text{iff}\quad \text{for all } a\in M \text{ holds}\\
&\qquad \mathfrak{M}\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}\,a}{x_0\ldots x_{r-1}\,x}\vDash\psi\\
&\qquad \text{(since } x \text{ is anyway sent to } a)\\
&\text{iff}\quad \text{for all } a\in M \text{ holds}\\
&\qquad (\,\mathfrak{M}\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}}{x_0\ldots x_{r-1}})\,\frac{a}{x}\vDash\psi\\
&\qquad \text{(by simple properties of assignments)}\\
&\text{iff}\quad \mathfrak{M}\frac{t_0^{\mathfrak{M}}\ldots t_{r-1}^{\mathfrak{M}}}{x_0\ldots x_{r-1}}\vDash\forall x\psi
\end{aligned}$$

□

We can now formulate properties of the $\vDash$ relation in connection with the treatment of variables.

Theorem 37. *Let S be a language. Let x, y be variables, $t, t'\in T^S$, $\varphi\in L^S$, and $\Gamma\subseteq L^S$. Then:*

a) ($\forall$-Introduction) If $\Gamma\vDash\varphi\frac{y}{x}$ and $y\notin\mathrm{free}(\Gamma\cup\{\forall x\varphi\})$ then $\Gamma\vDash\forall x\varphi$.

b) ($\forall$-elimination) If $\Gamma\vDash\forall x\varphi$ then $\Gamma\vDash\varphi\frac{t}{x}$.

c) ($\equiv$-Elimination or substitution) If $\Gamma\vDash\varphi\frac{t}{x}$ and $\Gamma\vDash t\equiv t'$ then $\Gamma\vDash\varphi\frac{t'}{x}$.

Proof. a) Assume $\Gamma\vDash\varphi\frac{y}{x}$ and $y\notin\mathrm{free}(\Gamma\cup\{\forall x\varphi\})$. Consider an S-model $\mathfrak{M}$ with $\mathfrak{M}\vDash\Gamma$. Let $a\in M=|\mathfrak{M}|$. Since $y\notin\mathrm{free}(\Gamma)$, $\mathfrak{M}\frac{a}{y}\vDash\Gamma$. By assumption, $\mathfrak{M}\frac{a}{y}\vDash\varphi\frac{y}{x}$. By the substitution theorem,

$$(\mathfrak{M}\frac{a}{y})\,\frac{y^{\mathfrak{M}\frac{a}{y}}}{x}\vDash\varphi \text{ and so } (\mathfrak{M}\frac{a}{y})\,\frac{a}{x}\vDash\varphi$$

Case 1: $x=y$. Then $\mathfrak{M}\frac{a}{x}\vDash\varphi$.
Case 2: $x\neq y$. Then $\mathfrak{M}\frac{a\,a}{y\,x}\vDash\varphi$, and since $y\notin\mathrm{free}(\varphi)$ we have $\mathfrak{M}\frac{a}{x}\vDash\varphi$.

Since $a\in M$ is arbitrary, $\mathfrak{M}\vDash\forall x\varphi$. Thus $\Gamma\vDash\forall x\varphi$.
b) Let $\Gamma\vDash\forall x\varphi$. Consider an S-model $\mathfrak{M}$ with $\mathfrak{M}\vDash\Gamma$. For all $a\in M=|\mathfrak{M}|$ holds $\mathfrak{M}\frac{a}{x}\vDash\varphi$. In particular $\mathfrak{M}\frac{t^{\mathfrak{M}}}{x}\vDash\varphi$. By the substitution theorem, $\mathfrak{M}\vDash\varphi\frac{t}{x}$. Thus $\Gamma\vDash\varphi\frac{t}{x}$.
c) Let $\Gamma\vDash\varphi\frac{t}{x}$ and $\Gamma\vDash t\equiv t'$. Consider an S-model $\mathfrak{M}$ mit $\mathfrak{M}\vDash\Gamma$. By assumption $\mathfrak{M}\vDash\varphi\frac{t}{x}$ and $\mathfrak{M}\vDash t\equiv t'$. By the substitution theorem

$$\mathfrak{M}\frac{t^{\mathfrak{M}}}{x}\vDash\varphi.$$

Since $t^{\mathfrak{M}}=t'^{\mathfrak{M}}$,

$$\mathfrak{M}\frac{t'^{\mathfrak{M}}}{x}\vDash\varphi$$

and again by the substitution theorem

$$\mathfrak{M}\vDash\varphi\frac{t'}{x}.$$

Thus $\Gamma\vDash\varphi\frac{t'}{x}$. □

Note that in proving these proof rules we have used corresponding forms of arguments in the language of our discourse. This "circularity" was noted before and is a general feature in formalizations of logic. A particularly important method of proof is the $\forall$-introduction: to prove a universal statement $\forall x\varphi$ it suffices to consider an "arbitrary but fixed" y and prove the claim for y. Formally this corresponds to using a "new" variable $y\notin\operatorname{free}(\Gamma\cup\{\forall x\varphi\})$.

7 A sequent calculus

> *The only way to rectify our reasonings is to make them as tangible as those of the Mathematicians, so that we can find our error at a glance, and when there are disputes among persons, we can simply say: Let us calculate [calculemus], without further ado, to see who is right.* G.W. Leibniz

We can put the rules of implication established in the previous two sections together as a *calculus* which leads from correct implications $\Phi\vDash\varphi$ to further correct implications $\Phi'\vDash\varphi'$. Our *sequent calculus* will work on *sequents* (Γ,φ) of formulas, whose intuitive meaning is that Γ implies φ. The Gödel completeness theorem shows that the rules from the last section actually generate the implication relation $\vDash$. Fix a language S.

Definition 38. *A pair* (Γ,φ) *where* Γ *is a finite set of* S*-formulas and* φ *is an* S*-formula is called a* sequent. $\Gamma=\{\varphi_0,\ldots,\varphi_{n-1}\}$ *is the* antecedent *and* φ *is the* succedent *of the sequent. We also write* $\Gamma\varphi$, *or* $\varphi_0\ldots\varphi_{n-1}\,\varphi$ *instead of* (Γ,φ). *Moreover we may denote an antecedent of the form* $\Gamma\cup\{\psi\}$ *also by* $\Gamma\psi$.

A sequent $\Gamma\varphi$ *is* correct *if* $\Gamma\vDash\varphi$.

Exercise 10. One could also define a sequent to be the concatenation of finitely many formulas

Definition 39. *The* sequent calculus *consists of the following (sequent-)rules, which transform given sequents, the* premisses, *into another sequent, the* conclusion. *We write the premisses on top of a bar, and the conclusions underneath.*

- *monotonicity* (MR) $\dfrac{\Gamma\quad\varphi}{\Gamma'\quad\varphi}$, *if* $\Gamma\subseteq\Gamma'$

- *assumption* (AR) $\begin{array}{l} \\ \hline \Gamma\ \ \varphi \end{array}$, *if* $\varphi\in\Gamma$

- $\rightarrow$*-introduction* $(\rightarrow I)$ $\begin{array}{ll} \Gamma\cup\{\varphi\} & \psi \\ \hline \Gamma & \varphi\rightarrow\psi \end{array}$

- $\rightarrow$*-elimination* $(\rightarrow E)$ $\begin{array}{l} \Gamma\ \ \varphi \\ \Gamma\ \ \varphi\rightarrow\psi \\ \hline \Gamma\ \ \psi \end{array}$

- $\perp$*-introduction* $(\perp I)$ $\begin{array}{l} \Gamma\ \ \varphi \\ \Gamma\ \ \neg\varphi \\ \hline \Gamma\ \ \perp \end{array}$

- $\perp$*-elimination* $(\perp E)$ $\begin{array}{ll} \Gamma\cup\{\neg\varphi\} & \perp \\ \hline \Gamma & \varphi \end{array}$

- $\forall$*-introduction* $(\forall I)$ $\begin{array}{l} \Gamma\ \ \varphi\frac{y}{x} \\ \hline \Gamma\ \ \forall x\varphi \end{array}$, *if* $y\notin\operatorname{free}(\Gamma\cup\{\forall x\varphi\})$

- $\forall$*-elimination* $(\forall E)$ $\begin{array}{l} \Gamma\ \ \forall x\varphi \\ \hline \Gamma\ \ \varphi\frac{t}{x} \end{array}$, *if* $t\in T^S$

- $\equiv$*-introduction* $(\equiv I)$ $\begin{array}{l} \\ \hline \Gamma\ \ t\equiv t \end{array}$, *if* $t\in T^S$

- $\equiv$*-elimination* $(\equiv E)$ $\begin{array}{l} \Gamma\ \ \varphi\frac{t}{x} \\ \Gamma\ \ t\equiv t' \\ \hline \Gamma\ \ \varphi\frac{t'}{x} \end{array}$

One can view these rules as functions on sequents.

Definition 40. *A formula* $\varphi\in L^S$ *is derivable from* $\Gamma\subseteq L^S$, $\Gamma\vdash\varphi$, *iff there is a* derivation *or a* formal proof

$$(\Gamma_0\varphi_0,\Gamma_1\varphi_1,\ldots,\Gamma_{k-1}\varphi_{k-1})$$

in which every sequent $\Gamma_i\varphi_i$ *is generated by a sequent rule from sequents* $\Gamma_{i_0}\varphi_{i_0},\ldots,\Gamma_{i_{n-1}}\varphi_{i_{n-1}}$ *with* $i_0,\ldots,i_{n-1}<i$, *and where* $\Gamma_{k-1}\subseteq\Gamma$ *and* $\varphi_{k-1}=\varphi$.

For Φ *an arbitrary class of formulas define* $\Phi\vdash\varphi$ *iff there is a finite* $\Gamma\subseteq\Phi$ *such that* $\Gamma\vdash\varphi$. *We say that* φ *can be* deduced *or* derived *from* Γ *or* Φ, *resp. We also write* $\vdash\varphi$ *instead of* $\emptyset\vdash\varphi$ *and say that* φ *is a* tautology.

We usually write the derivation $(\Gamma_0\varphi_0,\Gamma_1\varphi_1,\ldots,\Gamma_{k-1}\varphi_{k-1})$ as a vertical scheme

$$\begin{array}{ll} \Gamma_0 & \varphi_0 \\ \Gamma_1 & \varphi_1 \\ \vdots & \\ \Gamma_{k-1} & \varphi_{k-1} \end{array}$$

where we may also put rules and other remarks along the course of the derivation.

In our theorems on the laws of implication we have already shown:

Theorem 41. *The sequent calculus is* correct*, i.e., every rule of the sequent calculus leads from correct sequents to correct sequents. Thus every derivable sequent is correct. In terms of the relations of derivability and logical implication this means that*

$$\vdash \subseteq \vDash .$$

The converse inclusion corresponds to

Definition 42. *The sequent calculus is* complete *iff* $\vDash \subseteq \vdash$.

The GÖDEL completeness theorem will prove the completeness of the sequent calculus, and thus $\vDash = \vdash$.

Note that the relation $\vDash$ is defined semantically by ranging over all S-models, which is a proper class, possibly including models of high cardinalities, and models which cannot be constructed in any obvious sense.

The relation $\vdash$ is syntactical and defined by "concrete" finitary proofs: finite sequences of sequents, which obey simple syntactical rules. The rules can be implemented straightforwardly on computers working with sequences of symbols.

It is surprising that these relations agree. Once one has established that $\vDash = \vdash$, simple properties of $\vdash$ carry over to $\vDash$ and vice versa.

8 Derivable sequent rules

The composition of rules of the sequent calculus yields *derived sequent rules* which are again correct. First note:

Lemma 43. *Assume that*

$$\begin{array}{ll} \Gamma & \varphi_0 \\ \vdots & \\ \Gamma & \varphi_{k-1} \\ \hline \Gamma & \varphi_k \end{array}$$

is a derived rule of the sequent calculus. Then

$$\begin{array}{ll} \Gamma_0 & \varphi_0 \\ \vdots & \\ \Gamma_{k-1} & \varphi_{k-1} \\ \hline \Gamma & \varphi_k \end{array} \text{, where } \Gamma_0, \ldots, \Gamma_{k-1} \subseteq \Gamma$$

is also a derived rule of the sequent calculus.

Proof. This follows immediately from applications of the monotonicity rule. □

8.1 Auxiliary derived rules

We write the derivation of rules as proofs in the sequent calculus where the premisses of the derivation are written above the upper horizontal line and the conclusion as last row.

ex falso quodlibet $\dfrac{\Gamma \ \ \bot}{\Gamma \ \ \varphi}$:

$$\begin{array}{llll} 1. & \Gamma & & \bot \\ \hline 2. & \Gamma & \neg\varphi & \bot \\ \hline 3. & \Gamma & & \varphi \end{array}$$

$\neg$-*Introduction* $\dfrac{\Gamma\ \ \varphi\ \ \bot}{\Gamma\qquad \neg\varphi}$:

$$\begin{array}{llllll}
1. & \Gamma & \varphi & & \bot \\ \hline
2. & \Gamma & & & \varphi \to \bot \\
3. & \Gamma & \neg\neg\varphi & & \neg\neg\varphi \\
4. & \Gamma & \neg\neg\varphi & \neg\varphi & \neg\varphi \\
5. & \Gamma & \neg\neg\varphi & \neg\varphi & \bot \\
6. & \Gamma & \neg\neg\varphi & & \varphi \\
7. & \Gamma & \neg\neg\varphi & & \bot \\ \hline
8. & \Gamma & & & \neg\varphi
\end{array}$$

$$\begin{array}{ll}
\Gamma & \neg\varphi \\ \hline
\Gamma & \varphi \to \psi
\end{array}$$

$$\begin{array}{ll}
\Gamma & \psi \\ \hline
\Gamma & \varphi \to \psi
\end{array}$$

Cut rule

$$\begin{array}{lll}
\Gamma & & \varphi \\
\Gamma & \varphi & \psi \\ \hline
\Gamma & & \psi
\end{array}$$

Contraposition

$$\begin{array}{lll}
\Gamma & \varphi & \psi \\ \hline
\Gamma & \neg\psi & \neg\varphi
\end{array}$$

8.2 Introduction and elimination of $\vee, \wedge, \ldots$

The (abbreviating) logical symbols $\vee$, $\wedge$, and $\exists$ also possess (derived) introduction and elimination rules. We list the rules and leave their derivations as exercises.

$\vee$-*Introduction*

$$\begin{array}{ll}
\Gamma & \varphi \\ \hline
\Gamma & \varphi \vee \psi
\end{array}$$

$\vee$-*Introduction*

$$\begin{array}{ll}
\Gamma & \psi \\ \hline
\Gamma & \varphi \vee \psi
\end{array}$$

$\vee$-*Elimination*

$$\begin{array}{ll}
\Gamma & \varphi \vee \psi \\
\Gamma & \varphi \to \chi \\
\Gamma & \psi \to \chi \\ \hline
\Gamma & \chi
\end{array}$$

$\wedge$-*Introduction*

$$\begin{array}{ll}
\Gamma & \varphi \\
\Gamma & \psi \\ \hline
\Gamma & \varphi \wedge \psi
\end{array}$$

$\wedge$-*Elimination*

$$\begin{array}{ll}\Gamma & \varphi\wedge\psi\\ \hline \Gamma & \varphi\end{array}$$

$\wedge$-*Elimination*

$$\begin{array}{ll}\Gamma & \varphi\wedge\psi\\ \hline \Gamma & \psi\end{array}$$

$\exists$-*Introduction*

$$\begin{array}{ll}\Gamma & \varphi\frac{t}{x}\\ \hline \Gamma & \exists x\varphi\end{array}$$

$\exists$-*Elimination*

$$\begin{array}{lll}\Gamma & & \exists x\varphi\\ \Gamma & \varphi\frac{y}{x} & \psi\\ \hline \Gamma & & \psi\end{array}\quad \text{where } y\notin \mathrm{free}(\Gamma\cup\{\exists x\varphi,\psi\})$$

8.3 Formal proofs about $\equiv$

We give some examples of formal proofs which show that within the proof calculus $\equiv$ is an equivalence relation.

Lemma 44. *We prove the following tautologies:*

a) *Reflexivity:* $\vdash\forall x\, x\equiv x$

b) *Symmetry:* $\vdash\forall x\forall y(x\equiv y\rightarrow y\equiv x)$

c) *Transitivity:* $\vdash\forall x\forall y\forall z(x\equiv y\wedge y\equiv z\rightarrow x\equiv z)$

Proof. a)

$$\begin{array}{l} x\equiv x\\ \hline \forall x\, x\equiv x\end{array}$$

b)

$$\begin{array}{ll} x\equiv y & x\equiv y\\ x\equiv y & x\equiv x\\ x\equiv y & (z\equiv x)\frac{x}{z}\\ x\equiv y & (z\equiv x)\frac{y}{x}\\ x\equiv y & y\equiv x\\ & x\equiv y\rightarrow y\equiv x\\ & \forall y(x\equiv y\rightarrow y\equiv x)\\ \hline & \forall x\forall y(x\equiv y\rightarrow y\equiv x)\end{array}$$

c)

$$\begin{array}{ll} x\equiv y\wedge y\equiv z & x\equiv y\wedge y\equiv z\\ x\equiv y\wedge y\equiv z & x\equiv y\\ x\equiv y\wedge y\equiv z & (x\equiv w)\frac{y}{w}\\ x\equiv y\wedge y\equiv z & y\equiv z\\ x\equiv y\wedge y\equiv z & (x\equiv w)\frac{z}{w}\\ x\equiv y\wedge y\equiv z & x\equiv z\\ & x\equiv y\wedge y\equiv z\rightarrow x\equiv z\\ & \forall z(x\equiv y\wedge y\equiv z\rightarrow x\equiv z)\\ & \forall y\forall z(x\equiv y\wedge y\equiv z\rightarrow x\equiv z)\\ \hline & \forall x\forall y\forall z(x\equiv y\wedge y\equiv z\rightarrow x\equiv z)\end{array}$$

□

We show moreover that $\equiv$ is a *congruence relation* from the perspective of $\vdash$.

Theorem 45. *Let* $\varphi \in L^S$ *and* $t_0, \ldots, t_{n-1}, t_0', \ldots, t_{n-1}' \in T^S$. *Then*

$$\vdash t_0 \equiv t_0' \wedge \ldots \wedge t_{n-1} \equiv t_{n-1}' \rightarrow (\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} \leftrightarrow \varphi \frac{t_0' \ldots t_{n-1}'}{v_0 \ldots v_{n-1}}).$$

Proof. Choose pairwise distinct "new" variables $u_0, \ldots, u_{n-1}$. Then

$$\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} = \varphi \frac{u_0}{v_0} \frac{u_1}{v_1} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \frac{t_1}{u_1} \ldots \frac{t_{n-1}}{u_{n-1}}$$

and

$$\varphi \frac{t_0' \ldots t_{n-1}'}{v_0 \ldots v_{n-1}} = \varphi \frac{u_0}{v_0} \frac{u_1}{v_1} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0'}{u_0} \frac{t_1'}{u_1} \ldots \frac{t_{n-1}'}{u_{n-1}}.$$

Thus the simultaneous substitutions can be seen as successive substitutions, and the order of the substitutions $\frac{t_i}{u_i}$ may be permuted without affecting the final outcome. We may use the substitution rule repeatedly:

$$\begin{array}{ll}
\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} & \varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} & \varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} \; t_{n-1} \equiv t_{n-1}' & \varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}'}{u_{n-1}} \\
\vdots & \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} \; t_{n-1} \equiv t_{n-1}' \ldots t_0 \equiv t_0' & \varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0'}{u_0} \ldots \frac{t_{n-1}'}{u_{n-1}} \\
\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} \; t_0 \equiv t_0' \; \ldots \; t_{n-1} \equiv t_{n-1}' & \varphi \frac{t_0' \ldots t_{n-1}'}{v_0 \ldots v_{n-1}}.
\end{array}$$

□

9 Consistency

> *Vor Allem aber möchte ich unter den zahlreichen Fragen, welche hinsichtlich der Axiome gestellt werden können, dies als das wichtigste Problem bezeichnen, zu beweisen, daß dieselben untereinander widerspruchslos sind, d.h. daß man auf Grund derselben mittelst einer endlichen Anzahl von logischen Schlüssen niemals zu Resultaten gelangen kann, die miteinander in Widerspruch stehen.*
> David Hilbert

The notion of *consistency* will be central in proving the Gödel completeness theorem. We have to show: if $\Phi \nvdash \varphi$ then $\Phi \nvDash \varphi$. $\Phi \nvdash \varphi$ will mean that $\Phi \cup \{\neg\varphi\}$ is *consistent*. The *model existence theorem* shows the existence of models for consistent sets of formulas. So there is $\mathfrak{M} \vDash \Phi \cup \{\neg\varphi\}$ and so $\Phi \nvDash \varphi$.

Fix a language S.

Definition 46. *A set* $\Phi \subseteq L^S$ *is* consistent *if* $\Phi \nvdash \bot$. Φ *is* inconsistent *if* $\Phi \vdash \bot$.

We prove some laws of consistency.

Lemma 47. *Let* $\Phi \subseteq L^S$ *and* $\varphi \in L^S$. *Then*

a) Φ *is inconsistent iff there is* $\psi \in L^S$ *such that* $\Phi \vdash \psi$ *and* $\Phi \vdash \neg\psi$.

b) $\Phi \vdash \varphi$ *iff* $\Phi \cup \{\neg\varphi\}$ *is inconsistent.*

c) If Φ *is consistent, then* $\Phi \cup \{\varphi\}$ *is consistent or* $\Phi \cup \{\neg\varphi\}$ *is consistent (or both).*

d) Let $\mathcal{F}$ *be a family of consistent sets which is linearly ordered by inclusion, i.e., for all* $\Phi, \Psi \in \mathcal{F}$ *holds* $\Phi \subseteq \Psi$ *or* $\Psi \subseteq \Phi$. *Then*

$$\Phi^* = \bigcup_{\Phi \in \mathcal{F}} \Phi$$

is consistent.

Proof. a) Assume $\Phi \vdash \bot$. Then by the *ex falso* rule, $\Phi \vdash \psi$ and $\Phi \vdash \neg\psi$.

Conversely assume that $\Phi \vdash \psi$ and $\Phi \vdash \neg\psi$ for some $\psi \in L^S$. Then $\Phi \vdash \bot$ by $\bot$-introduction.

b) Assume $\Phi \vdash \varphi$. Take $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ such that $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$. Then we can extend a derivation of $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$ as follows

$$\begin{array}{lllll}
\varphi_0 & \cdots & \varphi_{n-1} & & \varphi \\
\varphi_0 & \cdots & \varphi_{n-1} & \neg\varphi & \neg\varphi \\
\varphi_0 & \cdots & \varphi_{n-1} & \neg\varphi & \bot
\end{array}$$

and $\Phi \cup \{\neg\varphi\}$ is inconsistent.

Conversely assume that $\Phi \cup \{\neg\varphi\} \vdash \bot$ and take $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ such that $\varphi_0 \ldots \varphi_{n-1} \neg \varphi \vdash \bot$. Then $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$ and $\Phi \vdash \varphi$.

c) Assume that $\Phi \cup \{\varphi\}$ and $\Phi \cup \{\neg\varphi\}$ are inconsistent. Then there are $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ such that $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$ and $\varphi_0 \ldots \varphi_{n-1} \vdash \neg\varphi$. By the introduction rule for $\bot$, $\varphi_0 \ldots \varphi_{n-1} \vdash \bot$. Thus Φ is inconsistent.

d) Assume that Φ^* is inconsistent. Take $\varphi_0, \ldots, \varphi_{n-1} \in \Phi^*$ such that $\varphi_0 \ldots \varphi_{n-1} \vdash \bot$. Take $\Phi_0, \ldots \Phi_{n-1} \in \mathcal{F}$ such that $\varphi_0 \in \Phi_0, \ldots, \varphi_{n-1} \in \Phi_{n-1}$. Since $\mathcal{F}$ is linearly ordered by inclusion there is $\Phi \in \{\Phi_0, \ldots \Phi_{n-1}\}$ such that $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$. Then Φ is inconsistent, contradiction. □

The proof of the completeness theorem will be based on the relation between consistency and satisfiability.

Lemma 48. *Assume that* $\Phi \subseteq L^S$ *is satisfiable. Then* Φ *is consistent.*

Proof. Assume that $\Phi \vdash \bot$. By the correctness of the sequent calculus, $\Phi \vDash \bot$. Assume that Φ is satisfiable and let $\mathfrak{M} \vDash \Phi$. Then $\mathfrak{M} \vDash \bot$. This contradicts the definition of the satisfaction relation. Thus Φ is not satisfiable. □

We shall later show the converse of this Lemma, since:

Theorem 49. *The sequent calculus is complete iff every consistent* $\Phi \subseteq L^S$ *is satisfiable.*

Proof. Assume that the sequent calculus is complete. Let $\Phi \subseteq L^S$ be consistent, i.e., $\Phi \nvdash \bot$. By completeness, $\Phi \nvDash \bot$, and we can take an S-model $\mathfrak{M} \vDash \Phi$ such that $\mathfrak{M} \nvDash \bot$. Thus Φ is satisfiable.

Conversely, assume that every consistent $\Phi \subseteq L^S$ is satisfiable. Assume $\Psi \vDash \psi$. Assume for a contradiction that $\Psi \nvdash \psi$. Then $\Psi \cup \{\neg\psi\}$ is consistent. By assumption there is an S-model $\mathfrak{M} \vDash \Psi \cup \{\neg\psi\}$. $\mathfrak{M} \vDash \Psi$ and $\mathfrak{M} \nvDash \psi$, which contradicts $\Psi \vDash \psi$. Thus $\Psi \vdash \psi$. □

10 Term models and Henkin sets

The following constructions will assume that the class of all terms of some language is a set. In view of the previous lemma, we strive to construct interpretations for given sets $\Phi \subseteq L^S$ of S-formulas. Since we are working in great generality and abstractness, the only material available for the construction of structures is the language L^S itself. We shall build a model out of S-terms.

Definition 50. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. The* term model $\mathfrak{T}^\Phi$ *of Φ is the following S-model:*

a) Define a relation $\sim$ on T^S,

$$t_0 \sim t_1 \text{ iff } \Phi \vdash t_0 \equiv t_1 .$$

$\sim$ is an equivalence relation on T^S.

b) For $t \in T^S$ let $\bar{t} = \{s \in T^S \,|\, s \sim t\}$ be the equivalence class of t.

c) The underlying set $|\mathfrak{T}^\Phi|$ of the term model is the set of $\sim$-equivalence classes

$$|\mathfrak{T}^\Phi| = \{\bar{t} \,|\, t \in T^S\}.$$

d) For an n-ary relation symbol $R \in S$ let $R^{\mathfrak{T}^\Phi}$ on T^Φ be defined by

$$(\bar{t}_0, \ldots, \bar{t}_{n-1}) \in R^{\mathfrak{T}^\Phi} \text{ iff } \Phi \vdash R t_0 \ldots t_{n-1} .$$

e) For an n-ary function symbol $f \in S$ let $f^{\mathfrak{T}^\Phi}$ on T^Φ be defined by

$$f^{\mathfrak{T}^\Phi}(\bar{t}_0, \ldots, \bar{t}_{n-1}) = \overline{f t_0 \ldots t_{n-1}} .$$

f) For $n \in \mathbb{N}$ define the variable interpretation $v_n^{\mathfrak{T}^\Phi} = \bar{v_n}$.

The term model is well-defined.

Lemma 51. *In the previous construction the following holds:*

a) $\sim$ is an equivalence relation on T^S.

b) The definition of $R^{\mathfrak{T}^\Phi}$ is independent of representatives.

c) The definition of $f^{\mathfrak{T}^\Phi}$is independent of representatives.

Proof. a) We derived the axioms of equivalence relations for $\equiv$:

- $\vdash \forall x \, x \equiv x$
- $\vdash \forall x \forall y \, (x \equiv y \rightarrow y \equiv x)$
- $\vdash \forall x \forall y \forall z \, (x \equiv y \wedge y \equiv z \rightarrow x \equiv z)$

Consider $t \in T^S$. Then $\vdash t \equiv t$. Thus for all $t \in T^S$ holds $t \sim t$.

Consider $t_0, t_1 \in T^S$ with $t_0 \sim t_1$. Then $\vdash t_0 \equiv t_1$. Also $\vdash t_0 \equiv t_1 \rightarrow t_1 \equiv t_0$, $\vdash t_1 \equiv t_0$, and $t_1 \sim t_0$. Thus for all $t_0, t_1 \in T^S$ with $t_0 \sim t_1$ holds $t_1 \sim t_0$.

The transitivity of $\sim$ follows similarly.

b) Let $\bar{t}_0, \ldots, \bar{t}_{n-1} \in T^\Phi$, $\bar{t}_0 = \bar{s}_0, \ldots, \bar{t}_{n-1} = \bar{s}_{n-1}$ and $\Phi \vdash Rt_0 \ldots t_{n-1}$. Then $\vdash t_0 \equiv s_0$, ..., $\vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule yield $\Phi \vdash Rs_0 \ldots s_{n-1}$. Hence $\Phi \vdash Rt_0 \ldots t_{n-1}$ implies $\Phi \vdash Rs_0 \ldots s_{n-1}$. By the symmetry of the argument, $\Phi \vdash Rt_0 \ldots t_{n-1}$ iff $\Phi \vdash Rs_0 \ldots s_{n-1}$.

c) Let $\bar{t}_0, \ldots, \bar{t}_{n-1} \in T^\Phi$ and $\bar{t}_0 = \bar{s}_0, \ldots, \bar{t}_{n-1} = \bar{s}_{n-1}$. Then $\vdash t_0 \equiv s_0$, ..., $\vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule to $\vdash ft_0 \ldots t_{n-1} \equiv ft_0 \ldots t_{n-1}$ yield

$$\vdash ft_0 \ldots t_{n-1} \equiv fs_0 \ldots s_{n-1}$$

and $\overline{ft_0 \ldots t_{n-1}} = \overline{fs_0 \ldots s_{n-1}}$. □

We aim to obtain $\mathfrak{T}^\Phi \vDash \Phi$. The initial cases of an induction over the complexity of formulas is given by

Theorem 52.

a) For terms $t \in T^S$ *holds* $\mathfrak{T}^\Phi(t) = \bar{t}$.

b) For atomic formulas $\varphi \in L^S$ *holds*

$$\mathfrak{T}^\Phi \vDash \varphi \text{ iff } \Phi \vdash \varphi.$$

Proof. a) By induction on the term calculus. The initial case $t = v_n$ is obvious by the definition of the term model. Now consider a term $t = ft_0 \ldots t_{n-1}$ with an n-ary function symbol $f \in S$, and assume that the claim is true for $t_0, \ldots, t_{n-1}$. Then

$$\begin{aligned} (ft_0 \ldots t_{n-1})^{\mathfrak{T}^\Phi} &= f^{\mathfrak{T}^\Phi}(\mathfrak{T}^\Phi(t_0), \ldots, \mathfrak{T}^\Phi(t_{n-1})) \\ &= f^{\mathfrak{T}^\Phi}(\bar{t_0}, \ldots, \overline{t_{n-1}}) \\ &= \overline{ft_0 \ldots t_{n-1}}. \end{aligned}$$

b) Let $\varphi = Rt_0 \ldots t_{n-1}$ with an n-ary relation symbol $R \in S$ and $t_0, \ldots, t_{n-1} \in T^S$. Then

$$\begin{aligned} \mathfrak{T}^\Phi \vDash Rt_0 \ldots t_{n-1} \text{ iff } & R^{\mathfrak{T}^\Phi}(\mathfrak{T}^\Phi(t_0), \ldots, \mathfrak{T}^\Phi(t_{n-1})) \\ \text{iff } & R^{\mathfrak{T}^\Phi}(\bar{t_0}, \ldots, \overline{t_{n-1}}) \\ \text{iff } & \Phi \vdash Rt_0 \ldots t_{n-1}. \end{aligned}$$

Let $\varphi = t_0 \equiv t_1$ with $t_0, t_1 \in T^S$. Then

$$\begin{aligned} \mathfrak{T}^\Phi \vDash t_0 \equiv t_1 \text{ iff } & \mathfrak{T}^\Phi(t_0) = \mathfrak{T}^\Phi(t_1) \\ \text{iff } & \bar{t_0} = \bar{t_1} \\ \text{iff } & t_0 \sim t_1 \\ \text{iff } & \Phi \vdash t_0 \equiv t_1. \end{aligned}$$

□

To extend the lemma to complex S-formulas, Φ has to satisfy some recursive properties.

Definition 53. *A set* $\Phi \subseteq L^S$ *of* S*-formulas is a* HENKIN set *if it satisfies the following properties:*

a) Φ *is consistent;*

b) Φ *is* (derivation) complete*, i.e., for all* $\varphi \in L^S$

$$\Phi \vdash \varphi \text{ or } \Phi \vdash \neg\varphi;$$

c) Φ contains witnesses*, i.e., for all* $\forall x\varphi \in L^S$ *there is a term* $t \in T^S$ *such that*

$$\Phi \vdash \neg\forall x\varphi \rightarrow \neg\varphi\frac{t}{x}.$$

Lemma 54. *Let* $\Phi \subseteq L^S$ *be a* Henkin *set. Then for all* $\chi, \psi \in L^S$ *and variables x:*

a) $\Phi \nvdash \chi$ *iff* $\Phi \vdash \neg\chi$.

b) $\Phi \vdash \chi$ *implies* $\Phi \vdash \psi$*, iff* $\Phi \vdash \chi \rightarrow \psi$.

c) For all $t \in T^S$ *holds* $\Phi \vdash \chi\frac{t}{u}$ *iff* $\Phi \vdash \forall x\chi$.

Proof. a) Assume $\Phi \nvdash \chi$. By derivation completeness, $\Phi \vdash \neg\chi$. Conversely assume $\Phi \vdash \neg\chi$. Assume for a contradiction that $\Phi \vdash \chi$. Then Φ is inconsistent. Contradiction. Thus $\Phi \nvdash \chi$.
b) Assume $\Phi \vdash \chi$ implies $\Phi \vdash \psi$.
Case 1. $\Phi \vdash \chi$. Then $\Phi \vdash \psi$ and by an easy derivation $\Phi \vdash \chi \rightarrow \psi$.
Case 2. $\Phi \nvdash \chi$. By the derivation completeness of Φ holds $\Phi \vdash \neg\chi$. And by an easy derivation $\Phi \vdash \chi \rightarrow \psi$.

Conversely assume that $\Phi \vdash \chi \rightarrow \psi$. Assume that $\Phi \vdash \chi$. By →-elimination, $\Phi \vdash \psi$. Thus $\Phi \vdash \chi$ implies $\Phi \vdash \psi$.
c) Assume that for all $t \in T^S$ holds $\Phi \vdash \chi\frac{t}{u}$. Assume that $\Phi \nvdash \forall x\chi$. By a), $\Phi \vdash \neg\forall x\chi$. Since Φ contains witnesses there is a term $t \in T^S$ such that $\Phi \vdash \neg\forall x\chi \rightarrow \neg\chi\frac{t}{u}$. By →-elimination, $\Phi \vdash \neg\chi\frac{t}{u}$. Contradiction. Thus $\Phi \vdash \forall x\chi$. The converse follows from the rule of ∀-elimination. □

Theorem 55. *Let* $\Phi \subseteq L^S$ *be a* Henkin *set. Then*

a) For all formulas $\chi \in L^S$*, pairwise distinct variables* $\vec{x}$ *and terms* $\vec{t} \in T^S$

$$\mathfrak{T}^\Phi \vDash \chi\frac{\vec{t}}{\vec{x}} \text{ iff } \Phi \vdash \chi\frac{\vec{t}}{\vec{x}}.$$

b) $\mathfrak{T}^\Phi \vDash \Phi$.

Proof. b) follows immediately from a). a) is proved by induction on the number of logical symbols $\bot, \neg, \rightarrow, \forall$ occuring in the formula χ. The atomic case, where that number is 0, has already been proven. Consider the non-atomic cases:
i) $\chi = \bot$. Then $\bot\frac{\vec{t}}{\vec{x}} = \bot$. $\mathfrak{T}^\Phi \vDash \bot$ is false by definition of $\vDash$, and $\Phi \vdash \bot$ is false since Φ is consistent. Thus $\mathfrak{T}^\Phi \vDash \bot\frac{\vec{t}}{\vec{x}}$ iff $\Phi \vdash \bot\frac{\vec{t}}{\vec{x}}$.
ii.) $\chi = \neg\varphi\frac{\vec{t}}{\vec{x}}$ and assume that the claim holds for φ. Then

$$\begin{aligned} \mathfrak{T}^\Phi \vDash \neg\varphi\frac{\vec{t}}{\vec{x}} &\text{ iff not } \mathfrak{T}^\Phi \vDash \varphi\frac{\vec{t}}{\vec{x}} \\ &\text{ iff not } \Phi \vdash \varphi\frac{\vec{t}}{\vec{x}} \text{ by the inductive assumption} \\ &\text{ iff } \Phi \vdash \neg\varphi\frac{\vec{t}}{\vec{x}} \text{ by a) of the previous lemma.} \end{aligned}$$

iii.) $\chi = (\varphi \to \psi) \frac{\vec{t}}{\vec{x}}$ and assume that the claim holds for φ and ψ. Then

$$\begin{aligned}
\mathfrak{T}^{\Phi} \vDash (\varphi \to \psi) \frac{\vec{t}}{\vec{x}} \quad & \text{iff} \quad \mathfrak{T}^{\Phi} \vDash \varphi \frac{\vec{t}}{\vec{x}} \text{ implies } \mathfrak{T}^{\Phi} \vDash \psi \frac{\vec{t}}{\vec{x}} \\
& \text{iff} \quad \Phi \vdash \varphi \frac{\vec{t}}{\vec{x}} \text{ implies } \Phi \vdash \psi \frac{\vec{t}}{\vec{x}} \ \text{ by the inductive assumption} \\
& \text{iff} \quad \Phi \vdash \left(\varphi \frac{\vec{t}}{\vec{x}} \to \psi \frac{\vec{t}}{\vec{x}} \right) \ \text{ by a) of the previous lemma} \\
& \text{iff} \quad \Phi \vdash (\varphi \to \psi) \frac{\vec{t}}{\vec{x}} \ \text{ by the definition of substitution.}
\end{aligned}$$

iv.) $\chi = (\forall x \varphi) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ and assume that the claim holds for φ. By definition of the substitution χ is of the form

$$\forall x \, (\varphi \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}) \ \text{ or } \ \forall u \, (\varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x})$$

with a suitable variable u. Without loss of generality assume that χ is of the second form. Then

$$\begin{aligned}
\mathfrak{T}^{\Phi} \vDash (\forall x \varphi) \frac{\vec{t}}{\vec{x}} \quad & \text{iff} \quad \mathfrak{T}^{\Phi} \vDash \exists u \, (\varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x}) \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^{\Phi} \frac{\bar{t}}{u} \vDash \varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^{\Phi} \frac{\mathfrak{I}^{\Phi}(t)}{u} \vDash \varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x} \ \text{ by a previous lemma} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^{\Phi} \vDash (\varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x}) \frac{t}{u} \ \text{ by the substitution lemma} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^{\Phi} \vDash \varphi \frac{t_0 \ldots t_{r-1} \, t}{x_0 \ldots x_{r-1} \, x} \ \text{ by successive substitutions} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \Phi \vdash \varphi \frac{t_0 \ldots t_{r-1} \, t}{x_0 \ldots x_{r-1} \, x} \ \text{ by the inductive assumption} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \Phi \vdash (\varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x}) \frac{t}{u} \ \text{ by successive substitutions} \\
& \text{iff} \quad \Phi \vdash \forall u \, (\varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x}) \ \text{ by c) of the previous lemma} \\
& \text{iff} \quad \Phi \vdash (\forall x \varphi) \frac{\vec{t}}{\vec{x}} .
\end{aligned}$$

□

11 “Constructing” Henkin sets

We shall show that every consistent set of formulas can be extended to a henkin set by first “adding witnesses” and then ensuring derivation completeness.

Theorem 56. *Let $\Phi \subseteq L^S$ be consistent. Let $\varphi \in L^S$ and let z be a variable which does not occur in $\Phi \cup \{\varphi\}$. Then the set*

$$\Phi \cup \{\neg \forall x \varphi \to \neg \varphi \frac{z}{x}\}$$

is consistent.

Proof. Assume not. Take $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ such that

$$\varphi_0 \ldots \varphi_{n-1} \ \neg \forall x \varphi \to \neg \varphi \frac{z}{x} \vdash \bot .$$

Set $\Gamma = \varphi_0 \ldots \varphi_{n-1}$. Then extend the derivation as follows:

$$
\begin{array}{lll}
1. & \Gamma \ \neg\forall x\,\varphi \rightarrow \neg\varphi\frac{z}{x} & \bot \\
\hline
2. & \Gamma \ \neg\neg\forall x\,\varphi & \neg\neg\forall x\,\varphi \\
3. & \Gamma \ \neg\neg\forall x\,\varphi & \neg\forall x\,\varphi \rightarrow \neg\varphi\frac{z}{x} \\
4. & \Gamma \ \neg\neg\forall x\,\varphi & \bot \\
5. & \Gamma & \neg\forall x\,\varphi \\
6. & \Gamma \ \neg\varphi\frac{z}{x} & \neg\varphi\frac{z}{x} \\
7. & \Gamma \ \neg\varphi\frac{z}{x} & \neg\forall x\,\varphi \rightarrow \neg\varphi\frac{z}{x} \\
8. & \Gamma \ \neg\varphi\frac{z}{x} & \bot \\
9. & \Gamma & \varphi\frac{z}{x} \\
10. & \Gamma & \forall x\,\varphi \\
\hline
11. & \Gamma & \bot
\end{array}
$$

Hence Φ is inconsistent, contradiction. □

This means that "new" variables may be used as HENKIN witnesses. Since "new" constant symbols behave much like new variables, we get:

Theorem 57. *Let $\Phi \subseteq L^S$ be consistent. Let $\varphi \in L^S$ and let $c \in S$ be a constant symbol which does not occur in $\Phi \cup \{\varphi\}$. Then the set*

$$\Phi \cup \{\neg\forall x\,\varphi \rightarrow \neg\varphi\frac{c}{x}\}$$

is consistent.

Proof. Assume that $\Phi \cup \{(\neg\exists x\,\varphi \vee \varphi\frac{c}{x})\}$ is inconsistent. Take a derivation

$$
\begin{array}{c}
\Gamma_0\varphi_0 \\
\Gamma_1\varphi_1 \\
\vdots \\
\Gamma_{n-1}\,\varphi_{n-1} \\
\Gamma_n\ (\neg\forall x\,\varphi \rightarrow \neg\varphi\frac{c}{x})\ \bot
\end{array}
\tag{1}
$$

with $\Gamma_n \subseteq \Phi$. Choose a variable z, which does not occur in the derivation. For a formula ψ define ψ' by replacing each occurence of c by z, and for a sequence $\Gamma = \psi_0 \ldots \psi_{k-1}$ of formulas let $\Gamma' = \psi_0' \ldots \psi_{k-1}'$. Replacing each occurence of c by z in (1) we get

$$
\begin{array}{c}
\Gamma_0'\varphi_0' \\
\Gamma_1'\varphi_1' \\
\vdots \\
\Gamma_{n-1}'\,\varphi_{n-1}' \\
\Gamma_n\ (\neg\forall x\,\varphi \rightarrow \neg\varphi\frac{z}{x})\ \bot
\end{array}
\tag{2}
$$

The particular form of the final sequence is due to the fact that c does not occur in $\Phi \cup \{\varphi\}$. To show that (2) is again a derivation in the sequent calculus we show that the replacement $c \mapsto z$ transforms every instance of a sequent rule in (1) into an instance of a (derivable) rule in (2). This is obvious for all rules except possibly the quantifyer rules.

So let

$$\frac{\Gamma \ \ \psi\frac{y}{x}}{\Gamma \ \ \forall x\psi}\ , \text{ with } y \notin \text{free}(\Gamma \cup \{\forall x\psi\})$$

be an $\forall$-introduction in (1). Then $(\psi\frac{y}{x})' = \psi'\frac{y}{x}$, $(\forall x\psi)' = \forall x\psi'$, and $y \notin \mathrm{free}(\Gamma' \cup \{(\forall x\psi)'\})$. Hence

$$\frac{\Gamma' \ \ (\psi\frac{y}{x})'}{\Gamma' \ \ (\forall x\psi)'}$$

is a justified $\forall$-introduction.

Now consider an $\forall$-elimination in (1):

$$\frac{\Gamma \ \ \forall x\psi}{\Gamma \ \ \psi\frac{t}{x}}$$

Then $(\forall x\psi)' = \forall x\psi'$ and $(\psi\frac{t}{x})' = \psi'\frac{t'}{x}$ where t' is obtained from t by replacing all occurences of c by z. Hence

$$\frac{\Gamma' \ \ (\forall x\psi)'}{\Gamma' \ \ (\psi\frac{t}{x})'}$$

is a justified $\forall$-elimination.

The derivation (2) proves that

$$\Phi \cup \left\{\left(\neg\forall x\,\varphi \to \neg\varphi\frac{z}{x}\right)\right\} \vdash \bot,$$

which contradicts the preceding lemma. □

We shall now show that any consistent set of formulas can be consistently expanded to a set of formulas which contains witnesses.

Theorem 58. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. Then there is a language S^ω and $\Phi^\omega \subseteq L^{S^\omega}$ such that*

- *a) S^ω extends S by constant symbols, i.e., $S \subseteq S^\omega$ and if $s \in S^\omega \setminus S$ then s is a constant symbol;*
- *b) $\Phi^\omega \supseteq \Phi$;*
- *c) Φ^ω is consistent;*
- *d) Φ^ω contains witnesses;*
- *e) if L^S is countable then so are L^{S^ω} and Φ^ω.*

Proof. For every a define a "new" distinct constant symbol c_a, which does not occur in S. Extend S by constant symbols c_ψ for $\psi \in L^S$:

$$S^+ = S \cup \{c_\psi | \psi \in L^S\}.$$

Then set

$$\Phi^+ = \Phi \cup \{\neg\forall x\varphi \to \neg\varphi\frac{c_{\forall x\varphi}}{x} | \forall x\,\varphi \in L^S\}.$$

Φ^+ contains witnesses for all universal formulas of S.

(1) $\Phi^+ \subseteq L^{S^+}$ is consistent.

Proof: Assume instead that Φ^+ is inconsistent. Choose a finite sequence $\forall x_0\varphi_0$, ..., $\forall x_{n-1}\varphi_{n-1} \in L^S$ of pairwise distinct universal formulas such that

$$\Phi \cup \{\neg\forall x_0\varphi_0 \to \neg\varphi_0\frac{c_{\forall x_0\varphi_0}}{x_0}, \ldots, \neg\forall x_{n-1}\varphi_{n-1} \to \neg\varphi_{n-1}\frac{c_{\forall x_{n-1}\varphi_{n-1}}}{x_{n-1}}\}$$

is inconsistent. By the previous theorem one can inductively show that for all $i < n$ the set

$$\Phi \cup \{\neg\forall x_0\varphi_0 \to \neg\varphi_0\frac{c_{\forall x_0\varphi_0}}{x_0}, \ldots, \neg\forall x_{i-1}\varphi_{i-1} \to \neg\varphi_{i-1}\frac{c_{\forall x_{i-1}\varphi_{i-1}}}{x_{i-1}}\}$$

is consistent. Contradiction. *qed*(1)

We iterate the +-operation through the integers. Define recursively

$$\begin{aligned}\Phi^0 &= \Phi\\ S^0 &= S\\ S^{n+1} &= (S^n)^+\\ \Phi^{n+1} &= (\Phi^n)^+\\ S^\omega &= \bigcup_{n\in\mathbb{N}} S^n\\ \Phi^\omega &= \bigcup_{n\in\mathbb{N}} \Phi^n.\end{aligned}$$

S^ω is an extension of S by constant symbols. For $n\in\mathbb{N}$, Φ^n is consistent by induction. Φ^ω is consistent by the lemma on unions of consistent sets.

(2) Φ^ω contains witnesses.

Proof. Let $\forall x\varphi\in L^{S^\omega}$. Let $n\in\mathbb{N}$ such that $\forall x\varphi\in L^{S^n}$. Then $\neg\forall x\varphi\rightarrow\neg\varphi\frac{c_{\forall x\varphi}}{x}\in\Phi^{n+1}\subseteq\Phi^\omega$. *qed*(2)

(3) Let L^S be countable. Then L^{S^ω} and Φ^ω are countable.

Proof. Since L^S is countable, there can only be countably many symbols in the alphabet of $S^0=S$. The alphabet of S^1 is obtained by adding the countable set $\{c_\psi|\psi\in L^S\}$; the alphabet of S^1 is countable as the union of two countable sets. The set of words over a countable alphabet is countable, hence L^{S^1} and $\Phi^1\subseteq L^{S^1}$ are countable.

Inductive application of this argument show that for any $n\in\mathbb{N}$, the sets L^{S^n} and Φ^n are countable. Since countable unions of countable sets are countable, $L^{S^\omega}=\bigcup_{n\in\mathbb{N}}L^{S^n}$ and also $\Phi^\omega\subseteq L^{S^\omega}$ are countable. □

Exercise 11. Let S be a countable language, let $\Phi\subseteq L^S$ be consistent, and let $\mathrm{Var}\setminus\mathrm{Var}(\Phi)$ be infinite. Then there exists $\Phi^\omega\subseteq L^S$ such that

a) $\Phi^\omega\supseteq\Phi$;

b) Φ^ω is consistent;

c) Φ^ω contains witnesses.

To get Henkin sets we have to ensure derivation completeness.

Theorem 59. *Let S be a language and let $\Phi\subseteq L^S$ be consistent. Then there is a consistent $\Phi^*\subseteq L^S$, $\Phi^*\supseteq\Phi$ which is derivation complete.*

Proof. Define the partial order $(P,\subseteq)$ by

$$P=\{\Psi\subseteq L^S\,|\,\Psi\supseteq\Phi \text{ and } \Psi \text{ is consistent}\}.$$

$P\neq\emptyset$ since $\Phi\in P$. P is *inductively ordered* by a previous lemma: if $\mathcal{F}\subseteq P$ is linearly ordered by inclusion, i.e., for all $\Psi,\Psi'\in\mathcal{F}$ holds $\Psi\subseteq\Psi'$ or $\Psi'\subseteq\Psi$ then

$$\bigcup_{\Psi\in\mathcal{F}}\Psi\in P.$$

Hence $(P,\subseteq)$ satisfies the conditions of Zorn's lemma. Let Φ^* be a maximal element of $(P,\subseteq)$. By the definition of P, $\Phi^*\subseteq L^S$, $\Phi^*\supseteq\Phi$, and Φ^* is consistent. Derivation completeness follows from the following claim.

(1) For all $\varphi\in L^S$ holds $\varphi\in\Phi^*$ or $\neg\varphi\in\Phi^*$.

Proof. Φ^* is consistent. By a previous lemma, $\Phi^*\cup\{\varphi\}$ or $\Phi^*\cup\{\neg\varphi\}$ are consistent.

Case 1. $\Phi^*\cup\{\varphi\}$ is consistent. By the $\subseteq$-maximality of Φ^*, $\Phi^*\cup\{\varphi\}=\Phi^*$ and $\varphi\in\Phi^*$.

Case 2. $\Phi^*\cup\{\neg\varphi\}$ is consistent. By the $\subseteq$-maximality of Φ^*, $\Phi^*\cup\{\neg\varphi\}=\Phi^*$ and $\neg\varphi\in\Phi^*$. □

The proof uses ZORN's lemma. In case L^S is countable one can work without ZORN's lemma.

Proof. (For countable L^S) Let $L^S = \{\varphi_n | n \in \mathbb{N}\}$ be an enumeration of L^S. Define a sequence $(\Phi_n | n \in \mathbb{N})$ by recursion on n such that

i. $\Phi \subseteq \Phi_n \subseteq \Phi_{n+1} \subseteq L^S$;

ii. Φ_n is consistent.

For $n = 0$ set $\Phi_0 = \Phi$. Assume that Φ_n is defined according to i. and ii.
Case 1. $\Phi_n \cup \{\varphi_n\}$ is consistent. Then set $\Phi_{n+1} = \Phi_n \cup \{\varphi_n\}$.
Case 2. $\Phi_n \cup \{\varphi_n\}$ is inconsistent. Then $\Phi_n \cup \{\neg\varphi_n\}$ is consistent by a previous lemma, and we define $\Phi_{n+1} = \Phi_n \cup \{\neg\varphi_n\}$.

Let

$$\Phi^* = \bigcup_{n \in \mathbb{N}} \Phi_n .$$

Then Φ^* is a consistent superset of Φ. By construction, $\varphi \in \Phi^*$ or $\neg\varphi \in \Phi^*$, for all $\varphi \in L^S$. Hence Φ^* is derivation complete. □

According to Theorem 58 a given consistent set Φ can be extended to $\Phi^\omega \subseteq L^{S^\omega}$ containing witnesses. By Theorem 59 Φ^ω can be extended to a derivation complete $\Phi^* \subseteq L^{S^\omega}$. Since the latter step does not extend the language, Φ^* contains witnesses and is thus a HENKIN set:

Theorem 60. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. Then there is a language S^* and $\Phi^* \subseteq L^{S^*}$ such that*

a) $S^* \supseteq S$ is an extension of S by constant symbols;

b) $\Phi^* \supseteq \Phi$ is a HENKIN *set;*

c) if L^S is countable then so are L^{S^*} and Φ^*.

12 The completeness theorem

> *The development of mathematics towards greater precision has led, as is well known, to the formalization of large tracts of it, so that one can prove any theorem using nothing but a few mechanical rules.* Kurt Gödel, 1941

We can now combine our technical preparations to show the fundamental theorems of first-order logic. Combining Theorems 60 and 55, we obtain a general and a countable model existence theorem:

Theorem 61. (HENKIN model existence theorem) *Let $\Phi \subseteq L^S$. Then Φ is consistent iff Φ is satisfiable.*

By Lemma 49, Theorem 61 the model existence theorems imply the main theorem.

Theorem 62. (GÖDEL completeness theorem) *The sequent calculus is complete, i.e., $\models = \vdash$.*

The Gödel completeness theorem is the *fundamental theorem of mathematical logic*. It connects syntax and semantics of formal languages in an optimal way. Before we continue the mathematical study of its consequences we make some general remarks about the wider impact of the theorem:

- The completeness theorem gives an *ultimate correctness criterion* for mathematical proofs. A proof is correct if it can (in principle) be reformulated as a formal derivation. Although mathematicians prefer semi-formal or informal arguments, this criterion could be applied in case of doubt.
- Checking the correctness of a formal proof in the above sequent calculus is a syntactic task that can be carried out by computer. We shall later consider a prototypical *proof checker* `Naproche` which uses a formal language which is a subset of natural english.
- By systematically running through all possible formal proofs, *automatic theorem proving* is in principle possible. In this generality, however, algorithms immediately run into very high algorithmic complexities and become practically infeasable.
- Practical automatic theorem proving has become possible in restricted situations, either by looking at particular kinds of axioms and associated intended domains, or by restricting the syntactical complexity of axioms and theorems.
- Automatic theorem proving is an important component of *artificial intelligence* (AI) where a system has to obtain logical consequences from conditions formulated in first-order logic. Although there are many difficulties with artificial intelligence this approach is still being followed with some success.
- Another special case of automatic theorem proving is given by *logic programming* where programs consist of logical statements of some restricted complexity and a run of a program is a systematic search for a solution of the given statements. The original and most prominent logic programming language is `Prolog` which is still widely used in linguistics and AI.
- There are other areas which can be described formally and where syntax/semantics constellations similar to first-order logic may occur. In the theory of algorithms there is the syntax of programming languages versus the (mathematical) meaning of a program. Since programs crucially involve time alternative logics with time have to be introduced. Now in all such generalizations, the Gödel completeness theorem serves as a pattern onto which to model the syntax/semantics relation.
- The success of the formal method in mathematics makes mathematics a leading *formal science*. Several other sciences also strive to present and justify results formally, like computer science and parts of philosophy.
- The completeness theorem must not be confused with the famous Gödel *incompleteness theorems*: they say that certain axiom systems like Peano arithmetic are incomplete in the sense that they do not imply some formulas which hold in the standard model of the axiom system.

13 The compactness theorem

By the definition of $\vdash$, $\Phi \vdash \varphi$ iff there is a finite subset $\Phi_0 \subseteq \Phi$ such that $\Phi_0 \vdash \varphi$.The equality of $\vDash$ and $\vdash$ implies:

Theorem 63. (Compactness theorem) *Let* $\Phi \subseteq L^S$ *and* $\varphi \in \Phi$. *Then*

a) $\Phi \vDash \varphi$ *iff there is a finite subset* $\Phi_0 \subseteq \Phi$ *such that* $\Phi_0 \vDash \varphi$.

b) Φ *is satisfiable iff every finite subset* $\Phi_0 \subseteq \Phi$ *is satisfiable.*

This theorem is often to construct (unusual) models of first-order theories. It is the basis of a field of logic called *Model Theory*.

We present a number theoretic application of the compactness theorem. The language of arithmetic can be naturally interpreted in the structure $\mathbb{N} = (\mathbb{N}, +, \cdot, 0, 1)$. This structure obviously satisfies the following axioms:

Definition 64. *The axiom system* PA $\subseteq L^{S_{\mathrm{AR}}}$ *of* PEANO arithmetic *consists of the following sentences*

- $\forall x\, x + 1 \neq 0$
- $\forall x \forall y\ x + 1 = y + 1 \rightarrow x = y$
- $\forall x\, x + 0 = x$
- $\forall x \forall y\, x + (y + 1) = (x + y) + 1$
- $\forall x\, x \cdot 0 = 0$
- $\forall x \forall y\, x \cdot (y + 1) = x \cdot y + x$
- *Schema of induction: for every formula* $\varphi(x_0, \ldots, x_{n-1}, x_n) \in L^{S_{\mathrm{AR}}}$*:*

$$\forall x_0 \ldots \forall x_{n-1} (\varphi(x_0, \ldots, x_{n-1}, 0) \wedge \forall x_n (\varphi \rightarrow \varphi(x_0, \ldots, x_{n-1}, x_n + 1)) \rightarrow \forall x_n\, \varphi)$$

The theory PA allows to prove a lot of number theoretic properties, e.g., about divisibility and prime numbers. On the other hand the first *incompleteness theorem* of GÖDEL shows that there are arithmetic sentences φ which are not decided by PA although they are true in the standard model $\mathbb{N}$ of PA. Therefore PA is *not* complete.

If φ and $\neg\varphi$ are both not derivable from PA then PA $+ \neg\varphi$ and PA $+ \varphi$ are consistent. By the model existence theorem, there are models $\mathfrak{M}^-$ and $\mathfrak{M}^+$ such that $\mathfrak{M}^- \vDash \mathrm{PA} + \neg\varphi$ and $\mathfrak{M}^+ \vDash \mathrm{PA} + \varphi$. $\mathfrak{M}^-$ and $\mathfrak{M}^+$ are not isomorphic. So there exist models of PA which are not isomorphic to the standard model $\mathbb{N}$.

We can also use the compactness theorem to obtain nonstandard models of theories. Define the S_{AR}-terms $\bar{n}$ for $n \in \mathbb{N}$ recursively by

$$\begin{aligned} \bar{0} &= 0, \\ \overline{n+1} &= (\bar{n} + 1). \end{aligned}$$

Note that this definition is taking place in the "meta theory" which studies the "object theory" PA: give me a standard natural number n and I return the term $\bar{n}$.

Define divisibility by the S_{AR}-formula $\delta = \exists v_2\ v_0 \cdot v_2 \equiv v_1$.

Theorem 65. *There is a model* $\mathfrak{M} \vDash$ PA *which contains an element* $\infty \in M$, $\infty \neq 0^{\mathfrak{M}}$ *such that* $\mathfrak{M} \vDash n \mid \infty$ *for every* $n \in \mathbb{N} \setminus \{0\}$, *where* $\mathfrak{M} \vDash n \mid \infty$ *is an intuitive abbreviation for* $\mathfrak{M}\frac{\infty}{v_1} \vDash \delta\frac{\bar{n}}{v_0}$ *or equivalently* $\mathfrak{M} \vDash \delta[\bar{n}^{\mathfrak{M}}, \infty]$.

So "from the outside", ∞ is divisible by every positive natural number. This implies $\mathfrak{M} \not\cong \mathbb{N}$, and so $\mathfrak{M}$ is a *nonstandard* model of PA.

Proof. Consider the theory

$$\Phi = \mathrm{PA} \cup \{\delta(\bar{n}, v_0) \mid n \in \mathbb{N} \setminus \{0\}\} \cup \{\neg v_0 \equiv \bar{0}\}$$

(1) Φ is satisfiable.
Proof. We use the compactness theorem 63(b). Let $\Phi_0\subseteq\Phi$ be finite. It suffices to show that Φ_0 is satisfiable. Take a finite number $n_0\in\mathbb{N}$ such that

$$\Phi_0\subseteq\mathrm{PA}\cup\{\delta(\bar{n},v_0)\,|\,n\in\mathbb{N},1\leqslant n\leqslant n_0\}.$$

Let $N=n!$. Then

$$\mathbb{N}\vDash\mathrm{PA}\text{ and }\mathbb{N}\vDash\delta(\bar{n},N)\text{ for }1\leqslant n\leqslant n_0.$$

So $\mathbb{N}\frac{N}{v_0}\vDash\Phi_0$. *qed*(1)

By (1), let $\mathfrak{M}'\vDash\Phi$. Let $\infty=\mathfrak{M}'(v_0)\in|\mathfrak{M}'|$. Let $\mathfrak{M}$ be underlying S_{AR}-structure of the model $\mathfrak{M}'$. Then $\mathfrak{M}$ is as required. □

This indicates that the model class of PA is rather complicated and rich. Indeed there is a subfield of model theory which studies models of Peano arithmetic.

We define notions which allow to examine the axiomatizability of classes of structures.

Definition 66. *Let S be a language and $\mathcal{K}$ be a class of S-structures.*

a) *$\mathcal{K}$ ist* elementary *or* finitely axiomatizable *if there is an S-sentence φ with $\mathcal{K}=\mathrm{Mod}^S\varphi$.*

b) *$\mathfrak{K}$ is* Δ-elementary *or* axiomatizable*, if there is a set Φ of S-sentences with $\mathcal{K}=\mathrm{Mod}^S\Phi$.*

We state simple properties of the Mod-operator:

Theorem 67. *Let S be a language.Then*

a) *For $\Phi\subseteq\Psi\subseteq L_0^S$ holds $\mathrm{Mod}^S\Phi\supseteq\mathrm{Mod}^S\Psi$.*

b) *For $\Phi,\Psi\subseteq L_0^S$ holds $\mathrm{Mod}^S(\Phi\cup\Psi)=\mathrm{Mod}^S\Phi\cap\mathrm{Mod}^S\Psi$.*

c) *For $\Phi\subseteq L_0^S$ holds $\mathrm{Mod}^S\Phi=\bigcap_{\varphi\in\Phi}\mathrm{Mod}^S\varphi$.*

d) *For $\varphi_0,\ldots,\varphi_{n-1}\in L_0^S$ holds $\mathrm{Mod}^S\{\varphi_0,\ldots,\varphi_{n-1}\}=\mathrm{Mod}^S(\varphi_0\wedge\ldots\wedge\varphi_{n-1})$.*

e) *For $\varphi\in L_0^S$ holds $\mathrm{Mod}^S(\neg\varphi)=\mathrm{Mod}^S(\emptyset)\setminus\mathrm{Mod}^S(\varphi)$.*

c) explains the denotation "Δ-elementary", since $\mathrm{Mod}^S\Phi$ is the intersection ("**D**urchschnitt") of all single $\mathrm{Mod}^S\varphi$.

Theorem 68. *Let S be a language and $\mathcal{K},\mathcal{L}$ be classes of S-structures with*

$$\mathcal{L}=\mathrm{Mod}^S\emptyset\setminus\mathcal{K}.$$

Then if $\mathcal{K}$ and $\mathcal{L}$ are axiomatizable, they are finitely axiomatizable.

Proof. Take axiom systems Φ_K and Φ_L such that $\mathfrak{K}=\mathrm{Mod}^S\Phi_K$ and $\mathfrak{L}=\mathrm{Mod}^S\Phi_L$. Assume that $\mathfrak{K}$ is not finitely axiomatizable.
(1) Let $\Phi_0\subseteq\Phi_K$ be finite. Then $\Phi_0\cup\Phi_L$ is satisfiable.
Proof: $\mathrm{Mod}^S\Phi_0\supseteq\mathrm{Mod}^S\Phi_K$. Since $\mathfrak{K}$ is not finitely axiomatizable, $\mathrm{Mod}^S\Phi_0\neq\mathrm{Mod}^S\Phi_K$. Then $\mathrm{Mod}^S\Phi_0\cap\mathfrak{L}\neq\emptyset$. Take a model $\mathfrak{A}\in\mathfrak{L}$, $\mathfrak{A}\in\mathrm{Mod}^S\Phi_0$. Then $\mathfrak{A}\vDash\Phi_0\cup\Phi_L$. *qed*(1)
(2) $\Phi_K\cup\Phi_L$ is satisfiable.
Proof: By the compactness theorem 63 it suffices to show that every finite $\Psi\subseteq\Phi_K\cup\Phi_L$ is satisfiable. By (1), $(\Psi\cap\Phi_K)\cup\Phi_L$ is satisfiable. Thus $\Psi\subseteq(\Psi\cap\Phi_K)\cup\Phi_L$ is satisfiable. *qed*(2)

By (2), $\mathrm{Mod}^S\Phi_K\cap\mathrm{Mod}^S\Phi_L\neq\emptyset$. But the classes $\mathfrak{K}$ and $\mathfrak{L}$ are complements, contradiction. Thus $\mathfrak{K}$ is finitely axiomatizable. □

II Herbrand's Theorem and Automatic Theorem Proving

> *When a man Reasoneth, hee does nothing else but conceive a summe totall, from Addition of parcels. For as Arithmeticians teach to adde and substract in numbers; so the Geometricians teach the same in lines, figures (solid and superficiall,) angles, proportions, times, degrees of swiftnesse, force, power, and the like; The Logicians teach the same in Consequences of words; adding together two Names, to make an Affirmation; and two Affirmations, to make a Syllogisme; and many Syllogismes to make a Demonstration; and from the summe, or Conclusion of a Syllogisme, they substract one Proposition, to finde the other. For REASON, in this sense, is nothing but Reckoning (that is, Adding and Substracting) of the Consequences of generall names agreed upon, for the marking and signifying of our thoughts.*
>
> Thomas Hobbes (1588–1679), *Leviathan, or The Matter, Forme, & Power of a Common-Wealth Ecclesiasticall and Civill*

This quote introduces the standard reference for implementing logic on computers: the *Handbook of Practical Logic and Automated Reasoning* by John Harrison. Syntactical "calculations" can be carried out by hand and by computers. We shall first consider some transformations to normal forms.

14 Normal forms

Normal forms are important in all fields of mathematics. Linear algebra, e.g., knows several normal forms for matrices which are equivalent to given matrices with respect to certain transformations, and polynomials are normal forms of terms in the theory of commutative rings.

Here we shall study normal forms of formulas, where equivalence is logical equivalence. Our motivation is the importance for *automated theorem proving*. We work in some fixed language S.

Definition 69.

a) An S-formula is a literal *if it is atomic or the negation of an atomic formula.*

b) Define the dual *of the literal L as*

$$\bar{L}=\begin{cases}\neg L, \text{ if } L \text{ is an atomic formula;}\\ K, \text{ if } L \text{ is of the form } \neg K.\end{cases}$$

14.1 Negation normal form

Most proving algorithms are based on the cancellation of positive and negative literals. It is important to shift negations down to the atoms:

Definition 70. $\varphi \in L^S$ *is in* negation normal form (NNF) *if* φ *does not contain the symbols* $\rightarrow$ *and* $\leftrightarrow$ *and if every subformula of* φ *of the form* $\neg\psi$ *is a literal.*

Note the we eliminate the junctors $\rightarrow$ and $\leftrightarrow$ as they contain implicit negations.

Lemma 71. *Every* $\varphi \in L^S$ *is logically equivalent to a formula in* NNF*.*

Proof. An obvious proof can be conducted by induction on the structure of φ. Standard equivalences of formulas like

$$\begin{array}{rcl} (\varphi \leftrightarrow \psi) & \leftrightarrow & (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi) \\ (\varphi \rightarrow \psi) & \leftrightarrow & (\neg\varphi \vee \psi) \\ \neg\forall x\varphi & \leftrightarrow & \exists x\neg\varphi \\ \neg(\varphi \wedge \psi) & \leftrightarrow & (\neg\varphi) \vee (\neg\psi) \end{array}$$

serve to eliminate $\rightarrow$ and $\leftrightarrow$ and to push negation symbols to the inside of a formula. □

14.2 Conjunctive and disjunctive normal form

$\wedge$, $\vee$ (and $\neg$) satisfy associative, commutative and distributive laws (up to logical equivalence). Therefore quantifier-free formulas can be transformed in certain kinds of "polynomials":

Definition 72.

a) *A formula* φ *is in* disjunctive normal form (DNF) *if it is of the form*

$$\varphi = \bigvee_{i<m} \, (\bigwedge_{j<n_i} L_{ij})$$

where each L_{ij} *is a literal.*

b) *A formula* φ *is in* conjunctive normal form (CNF) *if it is of the form*

$$\varphi = \bigwedge_{i<m} \, (\bigvee_{j<n_i} L_{ij})$$

where each L_{ij} *is a literal.*

Theorem 73. *Let* φ *be a formula without quantifiers. Then* φ *is equivalent to some* φ' *in disjunctive normal form and to some* φ'' *in conjunctive normal form.*

Proof. By induction on the complexity of φ. Clear for φ atomic. The $\neg$ step follows from the de Morgan laws:

$$\begin{array}{rcl} \neg\bigvee_{i<m} \, (\bigwedge_{j<n_i} L_{ij}) & \leftrightarrow & \bigwedge_{i<m} \neg(\bigwedge_{j<n_i} L_{ij}) \\ & \leftrightarrow & \bigwedge_{i<m} \, (\bigvee_{j<n_i} \neg L_{ij}). \end{array}$$

The $\wedge$-step is clear for conjunctive normal forms. For disjunctive normal forms the associativity rules yield

$$\bigvee_{i<m} \, (\bigwedge_{j<n_i} L_{ij}) \wedge \bigvee_{i<m'} \, (\bigwedge_{j<n_i'} L'_{ij}) \;\leftrightarrow\; \bigvee_{i<m, i'<m'} \, (\bigwedge_{j<n_i} L_{ij} \wedge \bigwedge_{j<n_i'} L'_{ij})$$

which is also in conjunctive normal form. □

Often the conjunctive normal form

$$\varphi = \bigwedge_{i<m} (\bigvee_{j<n_i} L_{ij})$$

is also written in set notion as

$$\varphi = \{\{L_{00}, ..., L_{0n_0-1}\}, ..., \{L_{m-1,0}, ..., L_{m-1,n_{m-1}}\}\},$$

using that sets are independent of the order of elements and eliminate multiple entries just like finite conjunctions and disjunctions. Furthermore we can distinguish positive and negative literals L_{ij} and partition the corresponding atomic formulas into a positive set p_i and a negative set n_i. So we can represent φ as a set of *pairs* of sets of atomic formulas:

$$\varphi = \{(p_0, n_0), ..., (p_{m-1}, n_{m-1})\}.$$

Details of such presentations are of course dependent on the intended use.

14.3 Prenex normal form

Definition 74. *A formula φ is in* prenex normal form *if it is of the form*

$$\varphi = Q_0\, x_0\, Q_1\, x_1 ... Q_{m-1}\, x_{m-1}\, \psi$$

where each Q_i is either the quantifier $\forall$ or $\exists$ and ψ is quantifier-free. Then the quantifier string $Q_0\, x_0\, Q_1\, x_1 ... Q_{m-1}\, x_{m-1}$ is called the prefix *of φ and the formula ψ is the* matrix *of φ.*

Theorem 75. *Let φ be a formula. Then φ is equivalent to a formula φ' in prenex normal form.*

Proof. By induction on the complexity of φ. Clear for atomic formulas. If

$$\varphi \leftrightarrow Q_0\, x_0\, Q_1\, x_1 ... Q_{m-1}\, x_{m-1}\, \psi$$

with quantifier-free ψ then by the de Morgan laws for quantifiers

$$\neg\varphi \leftrightarrow \bar{Q}_0\, x_0\, \bar{Q}_1\, x_1 ...\, \bar{Q}_{m-1} x_{m-1}\, \neg\psi$$

where the dual quantifier $\bar{Q}$ is defined by $\bar{\exists} = \forall$ and $\bar{\forall} = \exists$.

For the $\wedge$-operation consider another formula

$$\varphi' \leftrightarrow Q_0'\, x_0'\, Q_1'\, x_1' ... Q_{m'-1}'\, x_{m'-1}'\, \psi'$$

with quantifier-free ψ'. We may assume that the bound variables of φ are disjoint from all variables occuring in φ' and that the bound variables of φ' are disjoint from all variables occuring in φ. Then a semantic argument shows that

$$\varphi \wedge \varphi' \leftrightarrow Q_0\, x_0\, Q_1\, x_1 ... Q_{m-1}\, x_{m-1} Q_0'\, x_0'\, Q_1'\, x_1' ... Q_{m'-1}'\, x_{m'-1}'\, (\psi \wedge \psi').$$ □

The quantifier structure of prenex formulas is a measure of the complexity of formulas. In particular:

Definition 76. *A formula φ is* universal *if it is of the form*

$$\varphi = \forall x_0\, \forall x_1 ... \forall x_{m-1}\, \psi$$

where ψ is quantifier-free. A formula φ is existential *if it is of the form*

$$\varphi = \exists x_0\, \exists x_1 ... \exists x_{m-1}\, \psi$$

where ψ is quantifier-free.

14.4 Skolem normal form

Theorem 77. *Let φ be an S-formula. Then there is a canonical extension S^* of the language S and a canonical universal $\varphi^* \in L^{S^*}$ such that*

$$\varphi \textit{ is consistent iff } \varphi^* \textit{ is consistent.}$$

The formula φ^* is called the Skolem normal form *of φ.*

Proof. By a previous theorem we may assume that φ is in prenex normal form. We prove the theorem by induction on the number of existential quantifiers in φ. If φ does not contain an existential quantifier we are done. Otherwise let

$$\varphi = \forall x_1 ... \forall x_m \exists y \psi$$

where $m < \omega$ may also be 0. Introduce a new m-ary function symbol f (or a constant symbol in case $m = 0$) and let

$$\varphi' = \forall x_1 ... \forall x_m\, \psi \frac{f x_1 ... x_m}{y}.$$

By induction it suffices to show that φ is consistent iff φ' is consistent.
(1) $\varphi' \rightarrow \varphi$.
Proof. Assume φ'. Consider $x_1, ..., x_m$. Then $\psi \frac{f x_1 ... x_m}{y}$. Then $\exists y \psi$. Thus $\forall x_1 ... \forall x_m \exists y \psi$. *qed*(1)
(2) If φ' is consistent then φ is consistent.
Proof. If $\varphi \rightarrow \bot$ then by (1) $\varphi' \rightarrow \bot$. *qed*(2)
(3) If φ is consistent then φ' is consistent.
Proof. Let φ be consistent and let $\mathfrak{M} = (M, ...) \vDash \varphi$. Then

$$\forall a_1 \in M ... \forall a_m \in M\, \exists b \in M\, \mathfrak{M} \frac{\vec{a}\ b}{\vec{x}\ y} \vDash \psi.$$

Using the axiom of choice there is a function $h\colon M^m \rightarrow M$ such that

$$\forall a_1 \in M ... \forall a_m \in M\, \mathfrak{M} \frac{\vec{a}\ h(a_1, ..., a_m)}{\vec{x}\ \ y} \vDash \psi.$$

Expand the model $\mathfrak{M}$ to $\mathfrak{M}'$ by setting $f^{\mathfrak{M}'} = h$. Then $h(a_1, ..., a_m) = \mathfrak{M}' \frac{\vec{a}}{\vec{x}} (f x_1 ... x_m)$ and

$$\forall a_1 \in M ... \forall a_m \in M\, \mathfrak{M}' \frac{\vec{a}\ \mathfrak{M}' \frac{\vec{a}}{\vec{x}} (f x_1 ... x_m)}{\vec{x}\ \ y} = \mathfrak{M}' \frac{\vec{a}}{\vec{x}} \frac{\mathfrak{M}' \frac{\vec{a}}{\vec{x}} (f x_1 ... x_m)}{y} \vDash \psi.$$

By the substitution theorem this is equivalent to

$$\forall a_1 \in M ... \forall a_m \in M\ \mathfrak{M}' \frac{\vec{a}}{\vec{x}} \vDash \psi \frac{f x_1 ... x_m}{y}.$$

Hence

$$\mathfrak{M}' \vDash \forall x_1 ... \forall x_m\, \psi \frac{f x_1 ... x_m}{y} = \varphi'.$$

Thus φ' is consistent. □

Exercise 12. Prove the preceding Theorem syntactically, without using models.

15 HERBRAND's theorem

By the previous chapter we can reduce the question whether a given finite set of formulas is inconsistent to the question whether some universal formula is inconsistent. By the following theorem this can be answered rather schematically.

Theorem 78. *Let S be a language which contains at least one constant symbol. Let*

$$\varphi = \forall x_0 \forall x_1 \dots \forall x_{m-1} \psi$$

be a universal S-sentence with quantifier-free matrix ψ . Then φ is inconsistent iff there are variable-free S-terms ("constant terms")

$$t_0^0, \dots, t_{m-1}^0, \dots, t_0^{N-1}, \dots, t_{m-1}^{N-1}$$

such that

$$\varphi' = \bigwedge_{i<N} \psi \frac{t_0^i \dots t_{m-1}^i}{x_0 \dots x_{m-1}} = \psi \frac{t_0^0 \dots t_{m-1}^0}{x_0 \dots x_{m-1}} \wedge \dots \wedge \psi \frac{t_0^{N-1} \dots t_{m-1}^{N-1}}{x_0 \dots x_{m-1}}$$

is inconsistent.

Proof. All sentences φ', for various choices of constant terms, are logical consequences of φ. So φ is consistent, all φ' are consistent.

Conversely assume that all φ' are consistent. Then by the compactness theorem

$$\Phi = \{\psi \frac{t_0 \dots t_{m-1}}{x_0 \dots x_{m-1}} | t_0, \dots, t_{m-1} \text{ are constant } S\text{-terms}\}$$

is consistent. Let $\mathfrak{M} = (M, \dots) \vDash \Phi$. Let

$$H = \{t^{\mathfrak{M}} | t \text{ is a constant } S\text{-term}\}.$$

Then $H \neq \emptyset$ since S contains a constant symbol. By definition, H is closed under the functions of $\mathfrak{M}$. So we let $\mathfrak{H} = (H, \dots) \subseteq \mathfrak{M}$ be the substructure of $\mathfrak{M}$ with domain H.

(1) $\mathfrak{H} \vDash \varphi$.

Proof. Let $t_0^{\mathfrak{M}}, \dots, t_{m-1}^{\mathfrak{M}} \in H$ where $t_0, \dots, t_{m-1}$ are constant S-terms. Then $\psi \frac{t_0 \dots t_{m-1}}{x_0 \dots x_{m-1}} \in \Phi$, $\mathfrak{M} \vDash \psi \frac{t_0 \dots t_{m-1}}{x_0 \dots x_{m-1}}$, and by the substitution theorem

$$\mathfrak{M} \frac{t_0^{\mathfrak{M}} \dots t_{m-1}^{\mathfrak{M}}}{x_0 \dots x_{m-1}} \vDash \psi.$$

Since ψ is quantifier-free this transfers to $\mathcal{H}$:

$$\mathfrak{H} \frac{t_0^{\mathfrak{M}} \dots t_{m-1}^{\mathfrak{M}}}{x_0 \dots x_{m-1}} \vDash \psi.$$

Thus

$$\mathfrak{H} \vDash \forall x_0 \forall x_1 \dots \forall x_{m-1} \psi = \varphi.$$

qed(1)

Thus φ is consistent. □

In case that the formula ψ does not contain the equality sign $\equiv$ checking for inconsistency of

$$\varphi' = \bigwedge_{i<N} \psi \frac{t_0^i \dots t_{m-1}^i}{x_0 \dots x_{m-1}} = \psi \frac{t_0^0 \dots t_{m-1}^0}{x_0 \dots x_{m-1}} \wedge \dots \wedge \psi \frac{t_0^{N-1} \dots t_{m-1}^{N-1}}{x_0 \dots x_{m-1}}$$

is in principle a straightforward finitary problem. φ' is inconsistent iff $\neg\varphi'$ universally valid. We saw that universal validity can be checked via CNF when the atomic formulas are of the form `Trm ... []` which can be interpreted as propositional variables. Since we work without equality, atomic formulas with a list of constant terms behave just like (independent) propositional variables. So we have explicit (Haskell) algorithms for the required inconsistency checks contains finitely many constant S-terms. This leads to the following (theoretical) algorithm for automatic proving of formulas without $\equiv$ which we call the *Herbrand procedure*:

Let $\Omega \subseteq L^S$ be finite and $\chi \in L^S$. To check whether $\Omega \vdash \chi$:

1. Form $\Phi = \Omega \cup \{\neg\chi\}$ and let $\varphi = \forall(\bigwedge \Phi)$ be the universal closure of $\bigwedge \Phi$. Then $\Omega \vdash \chi$ iff $\Phi = \Omega \cup \{\neg\chi\}$ is inconsistent iff $(\bigwedge \Phi) \vdash \bot$ iff $\forall(\bigwedge \Phi) \vdash \bot$.
2. Transform φ into universal form $\varphi^{\forall} = \forall x_0 \forall x_1 ... \forall x_{m-1} \psi$ (Skolemization).
3. (Systematically) search for constant S-terms
$$t_0^0, ..., t_{m-1}^0, ..., t_0^{N-1}, ..., t_{m-1}^{N-1}$$
such that
$$\varphi' = \bigwedge_{i<N} \psi \frac{t_0^i ... t_{m-1}^i}{x_0 ... x_{m-1}} = \psi \frac{t_0^0 ... t_{m-1}^0}{x_0 ... x_{m-1}} \wedge ... \wedge \psi \frac{t_0^{N-1} ... t_{m-1}^{N-1}}{x_0 ... x_{m-1}}$$
is inconsistent.
4. If an inconsistent φ' is found, output "yes", otherwise carry on.

Obviously, if "yes" is output then $\Omega \vdash \chi$. This is the *correctness* of the algorithm. On the other hand, Herbrand's theorem ensures that if $\Omega \vdash \chi$ then an appropriate φ' will be found, and "yes" will be output, i.e., the algorithm is *complete*.

Example 79. We demonstrate the procedure with a small example. Let
$$\chi = \exists x \forall y (D(x) \to D(y))$$
be a version of the well-known *drinker's paradox*: there is somebody called x such that everybody drinks provided x drinks. To prove χ we follow the above steps.

1. χ is valid iff $\neg\chi$ is inconsistent. $\neg\chi$ is equivalent to $\forall x \exists y (D(x) \wedge \neg D(y))$.
2. The Skolemization of that formula is $\forall x (D(x) \wedge \neg D(f_y(x)))$.
3. Ground terms without free variables can be formed from a new constant symbol c and the unary function symbol f_y: $c, f_y(c), f_y(f_y(c)), ...$. We form the corresponding ground instances of the kernel $D(x) \wedge \neg D(f_y(x))$:
$$D(c) \wedge \neg D(f_y(c)), D(f_y(c)) \wedge \neg D(f_y(f_y(c))), D(f_y(f_y(c))) \wedge \neg D(f_y(f_y(f_y(c)))), ...$$
This leads to a sequence of conjunctions of ground instances:
   - $D(c) \wedge \neg D(f_y(c))$ is consistent since the conjunction does not contain dual literals;
   - $D(c) \wedge \neg D(f_y(c)) \wedge D(f_y(c)) \wedge \neg D(f_y(f_y(c)))$ is **inconsistent** since the conjunction contains the dual literals $\neg D(f_y(c))$ and $D(f_y(c))$.

This concludes the proof of the drinker's paradox via Herbrand's theorem.

The Herbrand procedure method can in principle be carried out automatically. It has for example been implemented in the *Gilmore procedure* which can be found in Harrison's *Handbook*, but the details are too involved to be discussed within this course.

16 Computer implementation of symbolic logic

We implement some syntactical algorithms in the functional computer language Haskell. Some of the code is a simplification of code from the Naproche (Natural Proof Checking) project at Bonn. Naproche is oriented towards a natural mathematical input language and natural proof structurings.

A Haskell module begins with a command like

```
> module FOL where
```

Since the Naproche modelling of syntax will be based on *lists* of syntactic objects, we also import a package with useful functions for lists from the standard library:

```
> import Data.List
```

We are using "literate Haskell" which treats everything as comment except lines which start with the symbol ">".

16.1 Formulas

In Naproche, formulas are defined by the data type

```
data Formula =
  All Decl Formula        | Exi Decl Formula |
  Iff Formula Formula     | Imp Formula Formula     |
  Or  Formula Formula     | And Formula Formula     |
  Tag Tag Formula         | Not Formula             |
  Top                     | Bot                     |
  Trm { trmName :: TermName, trmArgs :: [Formula],
        trmInfo :: [Formula], trmId   :: TermId}         |
  Var { varName :: VariableName, varInfo :: [Formula], varPosition ::
SourcePos } |
  Ind { indIndex :: Int, indPosition :: SourcePos }   | ThisT
  deriving (Eq, Ord)
```

Formulas in this type contain information important for processing in the Naproche-SAD system, like SourcePos for the original position of elements in some input file. We simplify the data type for our purposes:

```
> data Formula =
>   All String Formula      | Exi String Formula |
>   Iff Formula Formula     | Imp Formula Formula     |
>   Or  Formula Formula     | And Formula Formula     |
>   Not Formula             | Bot                     |
>   Trm String [Formula]    | Var String
>   deriving (Eq, Ord, Show)
```

The `Formula` data type also contains terms and relations:

- a variable α can be represented by `Var "alpha"` where sequences of letters between `" "` are *strings*;

- a term $f(x,\ y,\ \ldots)$ can be represented by `Trm "f" [Var "x", Var "y", . . .]` where the arity of function symbols is not specified; the *list* `[ . . . ]` has to provide sufficiently many arguments;
- constant symbols can be represented by empty lists like in `Trm "zero" []`;
- the same formalism is used for relations: `Trm "greater" [Var "x", Var "y"]` can stand for $x > y$;
- then terms with empty lists like `Trm "True" []` can stand for propositional constants.

In this formalism a “drinker’s formula” can be defined as:

```
> drinker = Exi "x" (All "y" (Iff (Trm "drinks" [Var "x"]) (Trm "drinks"
[Var "y"])))
```

The commands so far can be put in a file `FOL.lhs` (`.lhs` is the ending for literate Haskell) and be tried out in some interactive Haskell environment like the interactive Glasgow Haskell Compiler `GHCi`:

```
koepke@dell:~/V/2019/WS/Logik$ ghci FOL.lhs
GHCi, version 8.0.2: http://www.haskell.org/ghc/  :? for help
[1 of 1] Compiling FOL              ( FOL.lhs, interpreted )
Ok, modules loaded: FOL.
*FOL> drinker
Exi "x" (All "y" (Iff (Trm "drinks" [Var "x"]) (Trm "drinks" [Var "y"])))
*FOL> :type drinker
drinker :: Formula
```

The command `drinker` prints the value of the term `drinker` and `:type drinker` prints out the type of the term. Functions are the “first-class” objects of the functional language Haskell. Even constructors of the `Formula` data type are viewed as (generating) functions:

```
*FOL> :type Not
Not :: Formula -> Formula
*FOL> :type And
And :: Formula -> Formula -> Formula
```

16.2 Negation normal form

Let us consider a first example of a syntactic operation in Haskell, the transformation into NNF:

```
> nnf :: Formula -> Formula
> nnf (All string formula)       = All string (nnf formula)
> nnf (Exi string formula)       = Exi string (nnf formula)
> nnf (Iff formula1 formula2)    = nnf (And (Or (Not formula1) formula2)
                                    (Or formula1 (Not formula2)))
> nnf (Imp formula1 formula2)    = nnf (Or (Not formula1) formula2)
> nnf (Or formula1 formula2)     = Or (nnf formula1) (nnf formula2)
> nnf (And formula1 formula2)    = And (nnf formula1) (nnf formula2)
> nnf (Not (All string formula)) = nnf (Exi string (Not formula))
> nnf (Not (Exi string formula)) = nnf (All string (Not formula))
> nnf (Not (Iff f g))           = nnf (And (Or f g) (Or (Not f) (Not
g)))
> nnf (Not (Imp f g))           = nnf (And f (Not g))
> nnf (Not (And f g))           = nnf (Or (Not f) (Not g))
> nnf (Not (Or  f g))           = nnf (And (Not f) (Not g))
> nnf (Not (Not f))             = nnf f
> nnf f                         = f
```

Example 80.

```
*FOL> nnf drinker
Exi "x" (All "y" (And (Or (Not (Trm "drinks" [Var "x"])) (Trm "drinks"
[Var "y"])) (Or (Trm "drinks" [Var "x"]) (Not (Trm "drinks" [Var
"y"])))))
```

16.3 CNF

In Haskell, we can emulate the set representation of CNF using *lists* instead of sets. The disjunctions in CNFs are called clauses. We divide the literals in a clause up into pair consisting of the set of positive literals and of the set of negative literals:

```
> type Clause a = ([a],[a])
```

where the type variable `a` will be instantiated by atomic formulas. A formula in CNF would then be a list of clauses:

```
> type CNF a = [Clause a].
```

NNF quantifier-free formulas can be transformed into CNF by:

```
> cnf (And f g) = (cnf f) ++ (cnf g)
> cnf (Or f1 f2) = [(p1 ++ p2,n1 ++ n2)| (p1,n1) <- cnf(f1),(p2,n2) <-cnf(f2)]
> cnf (Not f)          = [([],[f])]
> cnf f                = [([f],[])]
```

The first line uses the associativity of $\wedge$; the second uses distributivity; the third inserts negated formulas in the negative component of clauses, whereas otherwise the entry goes into the positive component. List concatenation `++` corresponds to the union of two sets; list abstraction `[..|..]` works like set abstraction; `(p1,n1) <- cnf(f1)` means that one ranges over all members of `cnf(f1)` which are of the form `(p1,n1)`.

We use these functions to compute a conjunctive normal form of a formula like $A \wedge B \rightarrow B \wedge A$:

```
*FOL> cnf . nnf $ (Imp (And (Trm "A" []) (Trm "B" [])) (And (Trm "B" [])
(Trm "A" [])))
[([Trm "B" []],[Trm "A" [],Trm "B" []]),([Trm "A" []],[Trm "A" [],Trm "B"
[]])]
```

Such a CNF is universally valid iff every conjunct (or element) is universally valid. An element is a disjunction of literals. Such a disjunction is universally valid iff it contains the negation of `Bot` or some literal together with its dual. This is checked by the following recursive function:

```
> validCNF [] = True
> validCNF ((pos,neg) : tail) = validCNF tail && ((Bot ‘elem‘ neg)
                                || not (intersect pos neg == []))
```

We can now check propositional tautologies by composing the operations of negation normalization, conjunctive normalization and validity checking by the Haskell composition operator “.”.

```
> propTaut = validCNF . cnf . nnf
```

The formula $(p \leftrightarrow (q \leftrightarrow r)) \leftrightarrow ((p \leftrightarrow q) \leftrightarrow r)$ is a tautology since:

```
*FOL> propTaut  $ ((Trm "p" []) ‘Iff‘ ((Trm "q" []) ‘Iff‘ (Trm "r" [])))
‘Iff‘ (((Trm "p" []) ‘Iff‘ ((Trm "q" [])) ‘Iff‘ (Trm "r" [])))
True
```

Note that the corresponding CNF is quite large, since an elimination of ⇔ increases formula size considerably.

```
*FOL> cnf . nnf  $ ((Trm "p" []) ‘Iff‘ ((Trm "q" []) ‘Iff‘ (Trm "r" [])))
‘Iff‘ (((Trm "p" []) ‘Iff‘ ((Trm "q" [])) ‘Iff‘ (Trm "r" [])))
[([Trm "p" [],Trm "r" [],Trm "p" [],Trm "q" [],Trm "r" []],[Trm "q" []]),
([Trm "p" [],Trm "r" [],Trm "r" []],[Trm "q" [],Trm "p" [],Trm "q" []]),
([Trm "p" [],Trm "r" [],Trm "q" []],[Trm "q" [],Trm "p" [],Trm "r" []]),
([Trm "p" [],Trm "r" [],Trm "p" []],[Trm "q" [],Trm "q" [],Trm "r" []]),
([Trm "p" [],Trm "q" [],Trm "p" [],Trm "q" [],Trm "r" []],[Trm "r" []]),
([Trm "p" [],Trm "q" [],Trm "r" []],[Trm "r" [],Trm "p" [],Trm "q" []]),
([Trm "p" [],Trm "q" [],Trm "q" []],[Trm "r" [],Trm "p" [],Trm "r" []]),
([Trm "p" [],Trm "q" [],Trm "p" []],[Trm "r" [],Trm "q" [],Trm "r" []]),
([Trm "q" [],Trm "r" [],Trm "p" [],Trm "q" [],Trm "r" []],[Trm "p" []]),
([Trm "q" [],Trm "r" [],Trm "r" []],[Trm "p" [],Trm "p" [],Trm "q" []]),
([Trm "q" [],Trm "r" [],Trm "q" []],[Trm "p" [],Trm "p" [],Trm "r" []]),
([Trm "q" [],Trm "r" [],Trm "p" []],[Trm "p" [],Trm "q" [],Trm "r" []]),
([Trm "p" [],Trm "q" [],Trm "r" []],[Trm "p" [],Trm "q" [],Trm "r" []]),
([Trm "r" []],[Trm "p" [],Trm "q" [],Trm "r" [],Trm "p" [],Trm "q" []]),
([Trm "q" []],[Trm "p" [],Trm "q" [],Trm "r" [],Trm "p" [],Trm "r" []]),
([Trm "p" []],[Trm "p" [],Trm "q" [],Trm "r" [],Trm "q" [],Trm "r" []]),
([Trm "r" [],Trm "q" [],Trm "r" []],[Trm "p" [],Trm "q" [],Trm "p" []]),
([Trm "r" [],Trm "p" [],Trm "r" []],[Trm "p" [],Trm "q" [],Trm "q" []]),
([Trm "r" [],Trm "p" [],Trm "q" []],[Trm "p" [],Trm "q" [],Trm "r" []]),
([Trm "r" []],[Trm "p" [],Trm "q" [],Trm "p" [],Trm "q" [],Trm "r" []]),
([Trm "q" [],Trm "q" [],Trm "r" []],[Trm "p" [],Trm "r" [],Trm "p" []]),
([Trm "q" [],Trm "p" [],Trm "r" []],[Trm "p" [],Trm "r" [],Trm "q" []]),
([Trm "q" [],Trm "p" [],Trm "q" []],[Trm "p" [],Trm "r" [],Trm "r" []]),
([Trm "q" []],[Trm "p" [],Trm "r" [],Trm "p" [],Trm "q" [],Trm "r" []]),
([Trm "p" [],Trm "q" [],Trm "r" [],Trm "q" [],Trm "r" []],[Trm "p" []]),
([Trm "p" [],Trm "q" [],Trm "r" [],Trm "p" [],Trm "r" []],[Trm "q" []]),
([Trm "p" [],Trm "q" [],Trm "r" [],Trm "p" [],Trm "q" []],[Trm "r" []]),
([Trm "p" [],Trm "q" [],Trm "r" []],[Trm "p" [],Trm "q" [],Trm "r" []]),
([Trm "p" [],Trm "q" [],Trm "r" []],[Trm "q" [],Trm "r" [],Trm "p" []]),
([Trm "p" [],Trm "p" [],Trm "r" []],[Trm "q" [],Trm "r" [],Trm "q" []]),
([Trm "p" [],Trm "p" [],Trm "q" []],[Trm "q" [],Trm "r" [],Trm "r" []]),
([Trm "p" []],[Trm "q" [],Trm "r" [],Trm "p" [],Trm "q" [],Trm "r" []])]
```

If one wants to code this algorithm efficiently, better formula representations and internal simplifications should be used. There are many dedicated algorithms for tautology checking which are much more efficient in practice.

Note the difference between this brute force CNF calculation and an insightful human argument: one might, e.g., observe that the operation $p \leftrightarrow q$ on truth values is isomorphic to addition modulo 2 if one maps $\mathbb{T}$ to 0 and $\mathbb{F}$ to 1. And addition is associative.

Example 81. Electronic circuits.

Binary electronic circuits contain wires that at a given moment can have one out of two electric voltages V_{dd} and V_{ss}, corresponding to the truth values $\mathbb{F}$ and $\mathbb{T}$. Electrical circuits consist of transistors that perform simple logical operations on truth values. The overall function of a circuit is given by a composition of such operations. Proving the correctness of circuits amounts to showing that such a composition satisfies certain propositional properties.

We want to show that the following circuit realizes a `Nor` gate, i.e., a negated `Or`.

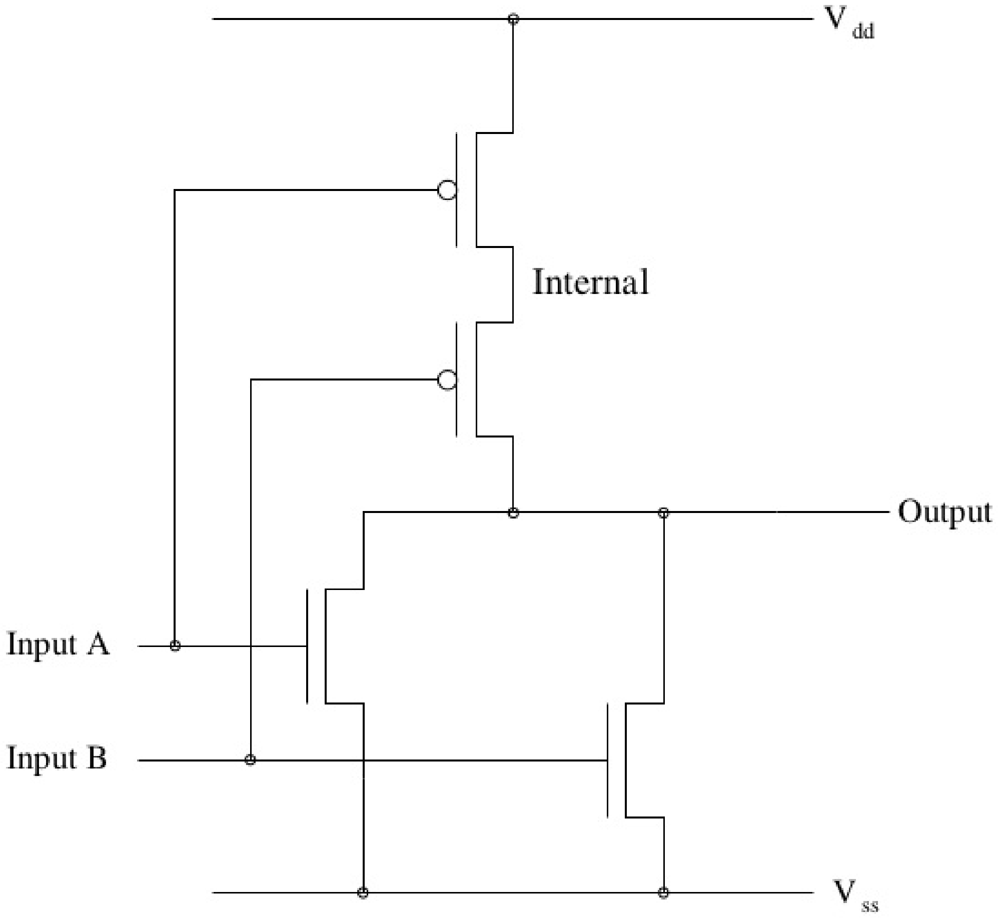


Figure 1: CMOS NOR gate

The circuit employs four CMOS transistors. The two N-type transistors at the bottom shortcut their output wires when the input is $\mathbb{T}$. E.g.,

```
(Trm "InputA" []) ‘Imp‘ ((Trm "Output" []) ‘Iff‘ Bot)
```

The top two P-type transistors shortcut when the input is $\mathbb{F}$:

```
Not (Trm "InputA" []) ‘Imp‘ ((Trm "Internal" []) ‘Iff‘ Top)
```

The logical behaviour of the circuit is described by:

```
> circuit = (Not (Trm "InputA" []) ‘Imp‘ ((Trm "Internal" []) ‘Iff‘ Top))
>     ‘And‘
>     (Not (Trm "InputB" []) ‘Imp‘
>              ((Trm "Output" []) ‘Iff‘ (Trm "Internal" []))) ‘And‘
>     ((Trm "InputA" []) ‘Imp‘ ((Trm "Output" []) ‘Iff‘ Bot)) ‘And‘
>     ((Trm "InputB" []) ‘Imp‘ ((Trm "Output" []) ‘Iff‘ Bot))
```

Proving that the circuit correctly implements the `Nor` function is expressed by

```
>       circuit
>       ‘Imp‘ ((Trm "Output" []) ‘Iff‘
>                 Not ((Trm "InputA" []) ‘Or‘ (Trm "InputB" [])))
```

`propTaut` quickly checks that this is a tautology.

16.4 DNF

Disjunctive normal forms (DNF) are dual to CNF's. We can use the set or list presentation also for DNF's, where we now understand

$$\varphi = \{\{L_{00}, ..., L_{0n_0-1}\}, ..., \{L_{m-1,0}, ..., L_{m-1,n_{m-1}}\}\},$$

as an abbreviation for a disjunction of conjunctions:

$$\varphi = \bigvee_{i<m} (\bigwedge_{j<n_i} L_{ij}).$$

NNF quantifier-free formulas can be transformed into DNF by the “dual” program to `cnf`:

```
> dnf (Or f g) = (dnf f) ++ (dnf g)
> dnf (And f1 f2) = [(p1 ++ p2,n1 ++ n2)| (p1,n1) <- dnf(f1),(p2,n2) <-dnf(f2)]
> dnf (Not f)         = [([],[f])]
> dnf f               = [([f],[])]
```

Such a DNF is universally valid iff some disjunct (or element) is satisfiable. An element is a conjunction of literals. Such a conjunction is satisfiable iff `Bot` does not appear and if every atomic formula occurs at most once, either in positive or negative form. This is expressed by the following recursive function:

```
> satDNF [] = False
> satDNF ((pos,neg) : tail) = sadDNF tail || (not (Bot ‘elem‘ pos)
                               && (intersect pos neg == []))
```

Deciding propositional satisfiability is the famous SAT problem from computer science. SAT is NP-complete which means that it is probably of very high complexity although a given solution can be checked quickly. We can decide small instances of SAT with:

```
> propSAT = satDNF . dnf . nnf
```

Finding a decision algorithm for SAT whose running time is always less than a fixed polynomial in the number of propositional variables amounts to showing that P=NP. The general conjecture these days is, however, that P≠NP.

16.5 Latin squares as a SAT problem

An n by n grid filled with numbers $0, ..., n-1$ so that every row and column contains all the numbers $1, ..., n$ (exactly) once is a *Latin square*. Being a Latin square can be described in propositional logic. In set theory one indentifies the natural number n with the set $\{0, ..., n-1\}$ of its predecessors. So the cartesian product $n \times n$ can be taken as (the index set of) the grid.

Let the propositional variable A_{ij}^k express that the grid position $(i,\ j)$ contains the number k. (A_{ij}^k) describes a Latin square iff:

- any grid position contains at least one number:

$$\bigwedge_{(i,j)\in n\times n} \bigvee_{k\in n} A_{ij}^k$$

- any grid position contains at most one number:

$$\bigwedge_{(i,j)\in n\times n} \bigwedge_{k\in n} \bigwedge_{l\in k} \neg(A_{ij}^k \wedge A_{ij}^l)$$

- any row contains every number:

$$\bigwedge_{i\in n} \bigwedge_{k\in n} \bigvee_{j\in n} A_{ij}^k$$

- any column contains every number:

$$\bigwedge_{j\in n} \bigwedge_{k\in n} \bigvee_{i\in n} A_{ij}^k$$

This amounts to a DNF with n^3 variables and $n^2 + n^2 \cdot \frac{n\,(n-1)}{2} + n^2 + n^2$ clauses.

In *Latin square problems*, a certain grid positions contain a given number, i.e., certain A_{ij}^k are assigned the truth value $\mathbb{T}$. These givens are usually called “clues”. A *solution* extends the assignment to all A_{ij}^k. This a propositional SAT problem.

Note that one could formulate equivalent specifications which look very differently. Instead of requiring that every row contains every number, one could have equivalently postulated that the numbers in a row are pairwise distinct.

For $n = 9$, Latin square problems can be solved in milliseconds by modern general purpose SAT solvers (but *not* by our simple-minded `propSAT`). These solvers incorporate sophisticated strategies and heuristics, as well as efficient programming techniques.

Note that standard *Sudoku* problems are Latin square problems with the further restraint

- that certain 3×3 subsquares contain every number:

$$\bigwedge_{(a,b)\in 3\times 3} \bigwedge_{k\in 9} \bigvee_{(c,d)\in 3\times 3} A_{3a+c,3b+d}^k$$

Using current SAT solvers one can program a fast Sudoku solver by just specifying the propositional problem, instead of programming “intelligent” human-like search strategies.

17 Resolution

The Herbrand procedure is theoretically complete: a formula is provable iff the procedure terminates. Termination can however take very long so that a proof will not be found in practice. Also there is an enormous amount of data to be stored which may cause the program to crash. E.g., disjunctive normal forms in the `gilmore` program which can simply be checked for inconsistency seem to double in length with each iteration of the algorithm. Practical automatic theorem proving requires more efficient algorithms in order to narrow down the search space for inconsistencies and to keep data sizes small.

We shall now present another method based on *conjunctive normal forms*. We assume that the quantifier-free formula ψ is a conjunction of clauses $\psi = c_0 \wedge c_1 \wedge \ldots \wedge c_{l-1}$. Then $\forall x_0 \forall x_1 \ldots \forall x_{m-1}\, \psi$ is inconsistent iff the set

$$\{c_i \frac{t_0 \ldots t_{m-1}}{x_0 \ldots x_{m-1}} \,|\, t_0, \ldots, t_{m-1} \text{ are constant } S\text{-terms}\}$$

is inconsistent.

The method of *resolution* gives an efficient method for showing the inconsistency of sets of clauses. Let us assume until further notice, that the formulas considered do not contain the symbol $\equiv$.

Definition 82. *Let $c^+ = \{K_0, \ldots, K_{k-1}\}$ and $c^- = \{L_0, \ldots, L_{l-1}\}$ be clauses with literals K_i and L_j. Note that $\{K_0, \ldots, K_{k-1}\}$ stands for the disjunction $K_0 \vee \ldots \vee K_{k-1}$. Assume that K_0 and L_0 are* dual*, i.e., $L_0 = \overline{K_0}$. Then the disjunction*

$$\{K_1, \ldots, K_{k-1}\} \cup \{L_1, \ldots, L_{l-1}\}$$

is a resolution of c^+ and c^-.

Resolution is related to the application of modus ponens: $\varphi \rightarrow \psi$ and φ correspond to the clauses $\{\neg\varphi, \psi\}$ and $\{\varphi\}$. $\{\psi\}$ is a resolution of $\{\neg\varphi, \psi\}$ and $\{\varphi\}$.

Theorem 83. *Let C be a set of clauses and let c be a resolution of two clauses $c^+, c^- \in C$. Then if $C \cup \{c\}$ is inconsistent then C is inconsistent.*

Proof. Let $c^+ = \{K_0, \ldots, K_{k-1}\}$, $c^- = \{\neg K_0, L_1 \ldots, L_{l-1}\}$, and $c = \{K_1, \ldots, K_{k-1}\} \cup \{L_1, \ldots, L_{l-1}\}$. Assume that $\mathcal{M} \vDash C$ is a model of C.
Case 1. $\mathcal{M} \vDash K_0$. Then $\mathcal{M} \vDash c^-$, $\mathcal{M} \vDash \{L_1 \ldots, L_{l-1}\}$, and

$$\mathcal{M} \vDash \{K_1, \ldots, K_{k-1}\} \cup \{L_1, \ldots, L_{l-1}\} = c.$$

Case 2. $\mathcal{M} \vDash \neg K_0$. Then $\mathcal{M} \vDash c^+$, $\mathcal{M} \vDash \{K_1 \ldots, K_{k-1}\}$, and

$$\mathcal{M} \vDash \{K_1, \ldots, K_{k-1}\} \cup \{L_1, \ldots, L_{l-1}\} = c.$$

Thus $\mathcal{M} \vDash C \cup \{c\}$. □

Theorem 84. *Let C be a set of clauses closed under resolution. Then C is inconsistent iff $\emptyset \in C$. Note that the empty clause $\{\}$ is logically equivalent to $\perp$.*

Proof. If $\emptyset \in C$ then C is clearly inconsistent.

Assume that the converse implication is false. Consider a set C of clauses such that

$$(*) \quad C \text{ is inconsistent and closed under resolution, but } \emptyset \notin C.$$

By the compactness theorem there is a finite set of atomic formulas $\{\varphi_0, \ldots, \varphi_{n-1}\}$ such that

$$C' = \{c \in C \,|\, \text{for every literal } L \text{ in } c \text{ there exists } i < n \text{ such that } L = \varphi_i \text{ or } L = \neg\varphi_i\},$$

is also inconsistent. Since resolution only *deletes* atomic formulas, C' is also closed under resolution, and of course $\emptyset \notin C'$. So we may assume right away that there is only a finite set $\{\varphi_0, ..., \varphi_{n-1}\}$ of atomic formulas occuring in C, and that n with that property is chosen minimally.

From $n=0$ atomic formulas one can only build the empty clause $\emptyset$. Since C is inconsistent, we must have $C \neq \emptyset$. Thus $C = \{\emptyset\}$ and $\emptyset \in C$, which contradicts $(*)$.

So we have $n = m + 1 > 0$. Let

$$C^+ = \{c \in C | \neg\varphi_m \notin c\}, C^- = \{c \in C | \varphi_m \notin c\}$$

and

$$C_0^+ = \{c \setminus \{\varphi_m\} | c \in C^+\}, C_0^- = \{c \setminus \{\neg\varphi_m\} | c \in C^-\}.$$

(1) C_0^+ and C_0^- are closed under resolution.
Proof. Let d'' be a resolution of $d, d' \in C_0^+$. Let $d = c \setminus \{\varphi_m\}$ and $d' = c' \setminus \{\varphi_m\}$ with c, $c' \in C^+$. The resolution d'' was based on some atomic formula $\varphi_i \neq \varphi_m$. Then we can also resolve c, c' by the same atomic formula φ_i . Let c'' be that resolution of c, c'. Since C is closed under resolution, $c'' \in C$, $c'' \in C^+$, and $d'' = c'' \setminus \{\varphi_m\} \in C_0^+$. *qed*(1)
(2) $\emptyset \notin C_0^+$ or $\emptyset \notin C_0^-$.
Proof. If $\emptyset \in C_0^+$ and $\emptyset \in C_0^-$, and since $\emptyset \notin C$ we have $\{\varphi_m\} \in C^+$ and $\{\neg\varphi_m\} \in C^-$. But then the resolution $\emptyset$ of $\{\varphi_m\}$ and $\{\neg\varphi_m\}$ would be in C, contradiction. *qed*(2)
Case 1. $\emptyset \notin C_0^+$. Since C_0^+ is formed by *removing* the atomic formula φ_m, C_0^+ only contains atomic formulas from $\{\varphi_0, ..., \varphi_{m-1}\}$. By the minimality of n and by (1), C_0^+ is consistent.

Let $\mathcal{M} \vDash C_0^+$. By the proof of the model existence theorem we may assume that $\mathcal{M}$ is a term model. Since the equality sign $\equiv$ does not occur in C the term model can be formed without factoring the terms in T^S by some equivalence relation. This means that different terms are interpreted by different elements of $|\mathcal{M}|$.

We can assume that the atomic formula φ_m is of the form $rt_0...t_{s-1}$ where r is an n-ary relation symbol and $t_0, ..., t_{s-1} \in T^S$. Since the formula $rt_0...t_{s-1}$ does not occur within C_0^+, we can modify the model $\mathcal{M}$ to a model $\mathcal{M}'$ by only modifying the interpretation $\mathcal{M}(r)$ exactly at $(\mathcal{M}(t_0), ..., \mathcal{M}(t_{s-1}))$. So let $\mathcal{M}'(r)(\mathcal{M}(t_0), ..., \mathcal{M}(t_{s-1}))$ be *false*. Then $\mathcal{M}' \vDash \neg\varphi_m$. We show that $\mathcal{M}' \vDash C$.

Let $c \in C$. If $\neg\varphi_m \in c$ then $\mathcal{M}' \vDash c$. So assume that $\neg\varphi_m \notin c$. Then $c \in C^+$ and $c \setminus \{\varphi_m\} \in C_0^+$. Then $\mathcal{M} \vDash c \setminus \{\varphi_m\}$, $\mathcal{M}' \vDash c \setminus \{\varphi_m\}$, and $\mathcal{M}' \vDash c$. But then C is consistent, contradiction.
Case 2. $\emptyset \notin C_0^-$. We can then proceed analogously to case 1, arranging that $\mathcal{M}'(\mathcal{M}(t_0), ..., \mathcal{M}(t_{s-1}))$ be *true*. So we get a contradiction again. □

This means that the inconsistency check in the Herbrand or Gilmore proving algorithm can be carried out even more systematically: produce all relevant resolution instances until the empty clause is generated. Again we have correctness and completeness for the enhanced algorithm with resolution.

Let us present an implementation of resolution (for ground formulas without variables) by S. Panitz in *Theorem Proving in a Russian Room and in Haskell*. We are again using a list presentation of sets:

- `nub` is a library function which removes double entries from lists thus making lists more set-like;
- `concat` is the *concatenation* of a list of lists, corresponding to the union of a set of sets;
- `iterate` yields an *infinite* list of the iterations of the function `allresolvents` applied to the original list `xs`;

- `([],[])` represents the empty clause which stands for a contradiction;
- note that Haskell is able to do some computations with *infinite* lists since it uses *lazy evaluation*: to decide the predicate `resPrf xs`, the iterates are produced and concatenated one by one; whether `([],[])` is an element of these concatenations is checked repeatedly until success, so that a *positive* decision is available at some finite iterate;
- if there is no positive decision the process runs into an infinite iteration and will only stop due to a stack overflow or other intervention.

```
> resolve(p1,n1)(p2,n2)=
          [(nub((p1\\[l])++p2),nub(n1++(n2\\[l])))|l<-p1,elem l n2]
> breadth f xs = [f x y |x<-xs,y<-xs]
> allresolvents xs = xs ++ concat (breadth resolve xs)
> resPrf xs = elem ([],[]) (concat (iterate allresolvents xs))
> propRes = resPrf . cnf . nnf . Not
```

18 Unifikation

Resolution is one of the main mechanisms behind the *logic programming language* `Prolog`. `Prolog` programs can be viewed as conjunctions of universally quantified clauses. A universally quantified clause stands for all clauses that can be reached by substituting into the free variables of the clause. `Prolog` searches systematically for clauses that can be resolved after substitution. `Prolog` uses "minimal" substitutions ("unifications") for those resolutions and keeps track of the required substitutions. The composition of all those substitutions is the computational result of the program: a minimal substitution to reach inconsistency.

To demonstrate how one can compute in `Prolog` let us consider the addition problem "$2 + 2 = ?$". Represent natural numbers by terms in a language with the constant symbol zero and the successor function succ. The ground terms of the language are:

$$\mathrm{zero}, \mathrm{succ}(\mathrm{zero}), \mathrm{succ}(\mathrm{succ}(\mathrm{zero})), \ldots$$

Addition is represented by a ternary predicate

$$\mathrm{add}(X,Y,Z) \leftrightarrow X+Y=Z.$$

The following universal sentences axiomatize addition:

$$\begin{array}{ll} A1. & \forall X.\mathrm{add}(X,\mathrm{zero},X) \\ A2. & \forall X,Y,Z.(\mathrm{add}(X,Y,Z) \rightarrow \mathrm{add}(X,\mathrm{succ}(Y),\mathrm{succ}(Z))) \end{array}$$

Computing $2+2$ can be viewed as an *inconsistency* problem:

$$4 = \mathrm{succ}(\mathrm{succ}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero}))))$$

is the unique term t of the language such that the axioms A1 and A2 are inconsistent with

$$\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})), \mathrm{succ}(\mathrm{succ}(\mathrm{zero})), t).$$

So the aim is to find a possibly iterated substitution for the variable V such that A1 and A2 are inconsistent with

$$\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})), \mathrm{succ}(\mathrm{succ}(\mathrm{zero})), V).$$

We can write these formulas in clausal form by omitting quantifiers.

$$\begin{array}{ll} A1. & \{\mathrm{add}(X,\mathrm{zero},X)\} \\ A2. & \{\neg\mathrm{add}(X,Y,Z),\mathrm{add}(X,\mathrm{succ}(Y),\mathrm{succ}(Z))\} \\ A3. & \{\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})),\mathrm{succ}(\mathrm{succ}(\mathrm{zero})),V)\} \end{array}$$

All variables are understood to be universally quantified. So we can rename variables freely, and we shall do so in order to avoid variable clashes.

In Prolog notation, the program to compute $2+2$ can be written as follows, where the implication in A2 is indicated by ":-":

```
add(X,zero,X).
add(X,succ(Y),succ(Z) :- add(X,Y,Z).
?- add(succ(succ(zero)),succ(succ(zero)),V).
```

Execution of the program means to find substitutions and resolutions leading to inconsistency: we begin with the clauses

1. $\mathrm{add}(X,\mathrm{zero},X)$
2. $\neg\mathrm{add}(X,Y,Z),\mathrm{add}(X,\mathrm{succ}(Y),\mathrm{succ}(Z))$
3. $\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})),\mathrm{succ}(\mathrm{succ}(\mathrm{zero})),V)$

The clauses 2 and 3 can be resolved by making the literals $\mathrm{add}(X,\ \mathrm{succ}(Y),\ \mathrm{succ}(Z))$ and $\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})),\ \mathrm{succ}(\mathrm{succ}(\mathrm{zero})),\ V)$ dual using the **substitutions** $X\colon = \mathrm{succ}(\mathrm{succ}(\mathrm{zero}))$, $Y\colon=\mathrm{succ}(\mathrm{zero})$, $V\colon=\mathrm{succ}(Z)$. This yields the resolution:

4. $\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})),\mathrm{succ}(\mathrm{zero}),Z)$

This should again resolve against 2. To avoid variable clashes, we first rename the (universal) variables in 2:

5. $\neg\mathrm{add}(X1,Y1,Z1),\mathrm{add}(X1,\mathrm{succ}(Y1),\mathrm{succ}(Z1))$

4 and 5 can be resolved by making the literals $\mathrm{add}(X1,\ \mathrm{succ}(Y1),\ \mathrm{succ}(Z1))$ and $\neg$ $\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})),\mathrm{succ}(\mathrm{zero}),Z)$ dual using the **substitutions** $X1\colon=\mathrm{succ}(\mathrm{succ}(\mathrm{zero}))$, $Y1\colon=\mathrm{zero}$, $Z\colon=\mathrm{succ}(Z1)$. This yields the resolution:

6. $\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero}),\mathrm{zero},Z1)$

This should resolve against 1. To avoid variable clashes, we first rename the (universal) variables in 1 by "new" variables:

7. $\mathrm{add}(X2,\mathrm{zero},X2)$.

6 and 7 can be resolved by the substitutions $X2\colon =\mathrm{succ}(\mathrm{succ}(\mathrm{zero}))$, $Z1\colon =X2$. This yields the "false" resolution, as required:

8. $\{\}$

The combined substitution for V which lead to this contradiction is obtained by "chasing" through the substitutions:

$$V=\mathrm{succ}(Z)=\mathrm{succ}(\mathrm{succ}(Z1))=\mathrm{succ}(\mathrm{succ}(X2))=\mathrm{succ}(\mathrm{succ}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})))).$$

Thus 2+2=4!

Exercise 13. Addition and multiplication on the natural numbers can be formalized in Prolog by the following program.

```
add(X,zero,X).
add(X,succ(Y),succ(Z) :- add(X,Y,Z).
mult(X,zero,zero).
mult(X,succ(Y),Z) :- mult(X,Y,W), add(W,X,Z).
```

The question $2\times 2=?$ is expressed by the query:

```
?- mult(succ(succ(zero)),succ(succ(zero)),V).
```

Please describe with pen and paper how Prolog calculates this product.

In the Prolog example, clauses with variables were brought into agreement by substitution of variables by terms. Then resolution was applied by cancelling out complementary literals. So far the substitutions used yielded ground instances, i.e., all variables were instantiated by constant terms. On the other hand the resolution method works for arbitrary substitutions. $\{\varphi(x)\}$ and $\{\neg\varphi(y), \psi(y)\}$ can be resolved into $\{\psi(y)\}$ by first transforming $\{\varphi(x)\}$ into $\{\varphi(y)\}$.

Definition 85. *Let* $\mathrm{Var} = \{v_n | n < \omega\}$ *be the set of first-order variables. A* substitution *is a map* $\sigma\colon \mathrm{Var} \rightarrow T^S$ *into the set of S-terms. If only a finite part of the substitution* σ *is relevant, it is usually written in the form* $\frac{\sigma(v_0)\ldots\sigma(v_{n-1})}{v_0\ldots v_{n-1}}$. *The application of a substitution to a term* t *or a formula* φ *is defined as before and written in the form* $t\sigma$ *or* $\varphi\sigma$. *Consider a finite set* $c = \{L_0, \ldots, L_{l-1}\}$ *of literals. Define the substitution* $c\sigma = \{L_0\sigma, \ldots, L_{l-1}\sigma\}$.

a) A substitution σ *is a* unifier *for* $\{L_0, \ldots, L_{l-1}\}$ *if* $L_0\sigma = \ldots = L_{l-1}\sigma$.

b) $\{L_0, \ldots, L_{l-1}\}$ *is* unifiable *if there is a unifier for* $\{L_0, \ldots, L_{l-1}\}$.

c) A unifier σ *for* $\{L_0, \ldots, L_{l-1}\}$ *is a* most general unifier *for* $\{L_0, \ldots, L_{l-1}\}$ *if every unifier* τ *factors by* σ, *i.e., there is another substitution* ρ *such that* $\tau = \rho \circ \sigma$. *Here the composition of substitutions is defined by*

$$\rho \circ \sigma(v_n) = \sigma(v_n)\,\rho.$$

Theorem 86. *Let* $\{L_0, \ldots, L_l\}$ *be a finite* unifiable *set of literals. Then* $\{L_0, \ldots, L_{l-1}\}$ *possesses a most general unifier, which can be constructed through a recursive syntactical algorithm.*

Proof. Define a sequence $\sigma_0, \ldots, \sigma_N$ of substitutions by recursion. Set $\sigma_0 = \mathrm{id} \restriction \mathrm{Var}$.

Assume that σ_i is defined. If $\{L_0\sigma_i, \ldots, L_l\sigma_i\}$ consists of one element then set $N = i$ and stop the recursion.

Now assume that $\{L_0\sigma_i, \ldots, L_l\sigma_i\}$ consists of more then one element. Let p be minimal such that there are substituted literals $L_j\sigma_i$ and $L_k\sigma_i$ which differ in their p^{th} position (as sequences of symbols). Let $s_j \neq s_k$ be the p^{th} element of $L_j\sigma_i$ and $L_k\sigma_i$ respectively.
Case 1. $s_j, s_k \notin \mathrm{Var}$. Then set $N = i$ and stop the recursion ("unification impossible").
Case 2. $s_j \in \mathrm{Var}$ or $s_k \in \mathrm{Var}$. Without loss of generality we may assume that $s_j \in \mathrm{Var}$, and we write $x = s_j$. Let t be the subterm of $L_k\sigma_i$ which starts at the p^{th} position with the symbol s_k.
Case 2.1. $x \in \mathrm{var}(t)$. Then set $N = i$ and stop the recursion ("occur-check failed").
Case 2.2. $x \notin \mathrm{var}(t)$. Then set

$$\sigma_{i+1} = \frac{t}{x} \circ \sigma_i$$

and continue the recursion.
(1) The recursion stops eventually.
Proof. σ_{i+1} can only be defined via *Case 2.2.* There, the variable x does not occur in t. Applying the substitution $\frac{t}{x}$ to $\{L_0\sigma_i, \ldots, L_l\sigma_i\}$ removes the variable x from

$$\{L_0\sigma_{i+1}, \ldots, L_l\sigma_{i+1}\} = \{L_0\sigma_i\frac{t}{x}, \ldots, L_l\sigma_i\frac{t}{x}\}.$$

So the number of variables in $\{L_0\sigma_i, \ldots, L_l\sigma_i\}$ goes down by at least 1 in each step of the recursion. Therefore the recursion must stop. *qed*(1)

Now let τ be any unifier for $\{L_0, \ldots, L_l\}$: $L_0\tau = \ldots = L_l\tau$.
(2) For $i = 0, \ldots, N$ there is a substitution τ_i such that $\tau = \tau_i \circ \sigma_i$.
Proof. Define τ_i by recursion on i. Set $\tau_0 = \tau$. Then $\tau = \tau \circ (\mathrm{id} \restriction \mathrm{Var}) = \tau_0 \circ \sigma_0$.

Assume that τ_i is defined such that $\tau = \tau_i \circ \sigma_i$ and that $i < N$. Then σ_{i+1} is defined according to *Case 2.2*. With the notations of that case: $\sigma_{i+1} = \frac{t}{x} \circ \sigma_i$. Since $\tau = \tau_i \circ \sigma_i$ is a unifier for $\{L_0, ..., L_l\}$ then τ_i is a unifier for $\{L_0 \sigma_i, ..., L_l \sigma_i\}$. Thus the variable x and the term t are unified by τ_i: $x\tau_i = \tau_i(x) = t\tau_i$. Set

$$\tau_{i+1} = (\tau_i \setminus \{(x, \tau_i(x))\}) \cup \{(x, x)\}.$$

We show that $\tau_{i+1} \circ \frac{t}{x} = \tau_i$: if $y \neq x$ then

$$y \frac{t}{x} \tau_{i+1} = y\tau_{i+1} = y\tau_i\,,$$

if $y = x$ then

$$y \frac{t}{x} \tau_{i+1} = t\tau_{i+1} = t\tau_i \text{ (since } x \text{ does not occur in } t) = x\tau_i = y\tau_i\,.$$

Then

$$\begin{aligned} \tau_{i+1} \circ \sigma_{i+1} &= \tau_{i+1} \circ (\frac{t}{x} \circ \sigma_i) \\ &= (\tau_{i+1} \circ \frac{t}{x}) \circ \sigma_i \\ &= \tau_i \circ \sigma_i \\ &= \tau\,. \end{aligned}$$

□

We can now define first-order resolution.

Definition 87. *Let c' and c'' be clauses. Let the substitutions σ':* Var ↔ Var *and σ'':* Var ↔ Var *be* renamings of variables *so that $c'\sigma'$ and $c''\sigma''$ do not have common variables. Let $\{L_1, ..., L_m\} \subseteq c'\sigma'$ and $\{K_1, ..., K_n\} \subseteq c''\sigma''$ be sets of literals such that*

$$\{L_1, ..., L_m, \bar{K}_1, ..., \bar{K}_n\}$$

is unifiable where $m, n \geqslant 1$. Let σ be a most general unifier of $\{L_1, ..., L_m, \bar{K}_1, ..., \bar{K}_n\}$. Then the clause

$$c = [(c'\sigma' \setminus \{L_1, ..., L_m\}) \cup (c''\sigma'' \setminus \{K_1, ..., K_n\})]\, \sigma$$

is a (first-order) resolution *of c' and c''.*

Given the clauses c' and c'' one just has to find parts (sometimes called *factors*) which are unifiable and compute c. It is not necessary to “find” ground instances of the clauses. On the other hand, resolution with ground instances can be gotten from first-order resolution by lifting-techniques.

Theorem 88. *Let c' and c'' be clauses and let c_0' and c_0'' be ground instances of c' and c'' which are resolvable. Let c_0 be a resolution of c_0' and c_0''. Then there is a first-order resolution c of c' and c'' such that c_0 is a ground instance of c.*

Proof. First let σ': Var ↔ Var and σ'': Var ↔ Var be *renamings of variables* so that $c'\sigma'$ and $c''\sigma''$ do not have common variables. Since c_0' and c_0'' are ground instances of c' and c'' they are also ground instances of $c'\sigma'$ and $c''\sigma''$. Let

$$c_0' = c'\sigma'\tau' \text{ and } c_0'' = c''\sigma''\tau''.$$

Since $c'\sigma'$ and $c''\sigma''$ do not have common variables we can assume that τ' and τ'' substitute disjoint sets of variables. Letting $\tau = \tau' \circ \tau''$ we get

$$c_0' = c'\sigma'\tau \text{ and } c_0'' = c''\sigma''\tau\,.$$

Let the resolution c_0 of c_0' and c_0'' be "based" on the literal L: $L \in c_0'$ and $\bar{L} \in c_0''$ and

$$c_0 = (c_0' \setminus \{L\}) \cup (c_0'' \setminus \{\bar{L}\}).$$

The literal L is a ground instance of possibly several literals $L_1, ..., L_m \in c'\sigma'$ by the ground substitution τ. Similarly the literal $\bar{L}$ is a ground instance of possibly several literals $K_1, ..., K_n \in c''\sigma''$ by the ground substitution τ. Now τ unifies $\{L_1, ..., L_m, \bar{K}_1, ..., \bar{K}_n\}$ into L. By the theorem on the existence of most general unifiers let σ be a most general unifier for

$$\{L_1, ..., L_m, \bar{K}_1, ..., \bar{K}_n\}.$$

Then

$$c = [(c'\sigma' \setminus \{L_1, ..., L_m\}) \cup (c''\sigma'' \setminus \{K_1, ..., K_n\})]\, \sigma$$

is a *(first-order) resolution* of c' and c''. Since σ is most general, take another substitution ρ such that $\tau = \rho \circ \sigma$. Then

$$\begin{aligned} c_0 &= (c_0' \setminus \{L\}) \cup (c_0'' \setminus \{\bar{L}\}) \\ &= (c'\sigma'\tau \setminus \{L\}) \cup (c''\sigma''\tau \setminus \{\bar{L}\}) \\ &= [(c'\sigma' \setminus \{L_1, ..., L_m\}) \cup (c''\sigma'' \setminus \{K_1, ..., K_n\})]\tau \\ &= [(c'\sigma' \setminus \{L_1, ..., L_m\}) \cup (c''\sigma'' \setminus \{K_1, ..., K_n\})]\sigma\rho \\ &= c\rho \end{aligned}$$

is a ground instance of c. □

Theorem 89. *Let C be a set of clauses and let $c_0 = c\sigma_0$ be a ground instance of c. Then $C \vdash c_0$ by resolution with ground clauses iff there is are substitutions σ and τ such that $C \vdash c\sigma$ can be shown by first-order resolution and $c_0 = c\sigma\tau$.*

III Set Theory

Die Mengenlehre ist das Fundament
der gesamten Mathematik
(Felix Hausdorff,
Grundzüge der Mengenlehre, 1914)

19 Set theory

19.1 The origin of set theory

Georg Cantor characterized sets as follows:

> Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten, wohlunterschiedenen Objekten m unsrer Anschauung oder unseres Denkens (welche die "Elemente" von M genannt werden) zu einem Ganzen.

FELIX HAUSDORFF in *Grundzüge* formulated shorter:

> Eine Menge ist eine Zusammenfassung von Dingen zu einem Ganzen, d.h. zu einem neuen Ding.

Sets are ubiquitous in mathematics. According to HAUSDORFF

> Differential- und Integralrechnung, Analysis und Geometrie arbeiten in Wirklichkeit, wenn auch vielleicht in verschleiernder Ausdrucksweise, beständig mit unendlichen Mengen.

19.2 Set theoretic foundations of mathematics

In current mathematics, *many* notions are explicitly defined using sets. The following example indicates that notions which are not set-theoretical *prima facie* can be construed set-theoretically:

> f is a real funktion $\equiv$ f is a **set** of ordered pairs (x, y) of real numbers, such that ... ;
>
> (x, y) is an ordered pair $\equiv$ (x, y) is a **set** ...$\{x, y\}$... ;
>
> x is a real number $\equiv$ x is a left half of a DEDEKIND cut in $\mathbb{Q}$ $\equiv$ x is a **subset** of $\mathbb{Q}$, such that ... ;
>
> r is a rational number $\equiv$ r is an **ordered pair** of integers, such that ... ;
>
> z is an integer $\equiv$ z is an **ordered pair** of natural numbers (= non-negative integers);
>
> $\mathbb{N} = \{0, 1, 2, ...\}$;
>
> 0 is the empty **set**;
>
> 1 is the **set** $\{0\}$;
>
> 2 is the **set** $\{0, 1\}$; etc. etc.

We shall see that *all* mathematical notions can expressed in the language of *sets*.

Besides this foundational role, set theory is also the mathematical study of the *infinite*. There are infinite sets like $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ which can be subjected to the constructions and analyses of set theory; there are various degrees of infinity which lead to a rich theory of infinitary combinatorics.

The notion of set is adequately formalized in first-order axiom systems introduced by ZERMELO, FRAENKEL and others. Together with the GÖDEL completeness theorem for first-order logic this constitutes a "formalistic" answer to the question "what is mathematics": mathematics consists of formal proofs from the axioms of ZERMELO-FRAENKEL set theory.

Definition 90. *Let* $\in$ *be a binary infix relation symbol; read* $x \in y$ *as "x is an* element *of y". The* language of set theory *is the language* $\{\in\}$*. The formulas in* $L^{\{\in\}}$ *are called* set theoretical formulas *or* $\in$*-formulas. We write* $L^{\in}$ *instead of* $L^{\{\in\}}$*.*

The naive notion of *set* is intuitively understood and was used extensively in previous chapters. The following axioms describe properties of naive sets. Note that the axiom system is an infinite *set* of axioms. It seems unavoidable that we have to go back to some previously given set notions to be able to define the collection of set theoretical axioms - another example of the frequent circularity in foundational theories.

Definition 91. *The axiom system* ST *of* set theory *consists of the following axioms:*

a) *The* axiom of extensionality (Ext)*:*

$$\forall x \forall y(\forall z(z \in x \leftrightarrow z \in y) \rightarrow x \equiv y)$$

- a set is determined by its elements, sets having the same elements are identical.

b) *The* pairing axiom (Pair)*:*

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

- z is the unordered pair of x and y.

c) *The* union axiom (Union)*:*

$$\forall x \exists y \forall z(z \in y \leftrightarrow \exists w(w \in x \wedge z \in w))$$

- y is the union of all elements of x.

d) *The* powerset axiom (Pow)*:*

$$\forall x \exists y \forall z(z \in y \leftrightarrow \forall w(w \in z \rightarrow w \in x))$$

- y consists of all subsets of x.

e) *The* separation schema (Sep) *postulates for every $\in$-formula $\varphi(z, x_1, ..., x_n)$:*

$$\forall x_1 ... \forall x_n \forall x \exists y \forall z\, (z \in y \leftrightarrow z \in x \wedge \varphi(z, x_1, ..., x_n))$$

- this is an infinite scheme of axioms, the set z consists of all elements of x which satisfy φ.

f) *The* replacement schema (Rep) *postulates for every $\in$-formula $\varphi(x, y, x_1, ..., x_n)$:*

$$\forall x_1 ... \forall x_n(\forall x \forall y \forall y'((\varphi(x, y, x_1, ..., x_n) \wedge \varphi(x, y', x_1, ..., x_n)) \rightarrow y \equiv y') \rightarrow \\ \forall u \exists v \forall y\, (y \in v \leftrightarrow \exists x(x \in u \wedge \varphi(x, y, x_1, ..., x_n))))$$

- v is the image of u under the map defined by φ.

g) *The* foundation schema (Found) *postulates for every $\in$-formula $\varphi(x, x_1, ..., x_n)$:*

$$\forall x_1 ... \forall x_n(\exists x \varphi(x, x_1, ..., x_n) \rightarrow \exists x(\varphi(x, x_1, ..., x_n) \wedge \forall x'(x' \in x \rightarrow \neg \varphi(x', x_1, ..., x_n))))$$

- if φ is satisfiable then there are $\in$-minimal elements satisfying φ.

The axiom of *extensionality* expresses that a set is only determined by its elements. There is no further structure in a set; the order or multiplicity of elements does not matter. The axiom of extensionality can also be seen as a definition of $\equiv$ in terms of $\in$:

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

The separation schema (“Aussonderung”) is the crucial axiom of ZERMELO set theory. GOTTLOB FREGE had used the more liberal comprehension schema

$$\forall x_1 ... \forall x_n \exists y \forall z\, (z \in y \leftrightarrow \varphi(z, x_1, ..., x_n))$$

without restricting the variable z to some x on the right hand side. This however led to the famous RUSSELL paradox and is thus inconsistent. ZERMELO’s restriction apparently avoids contradiction.

The replacement schema was added by ABRAHAM FRAENKEL to postulate that functional images of sets are sets.

The foundation schema by MIRIMANOFF allows to carry out induction on the binary relation $\in$. To prove a universal property by contradiction one can look at a minimal counterexample and argue that the property is inherited from the elements of a set to the set. The schema is used seldomly in mathematical practice, but it is very convenient for the development of set theory.

Note that the axioms of ST do not postulate the existence of infinite sets, and indeed one can easily build a canonical model of ST consisting only of finite sets. Such a model can be defined over the structure $\mathbb{N} = (\mathbb{N}, +, \cdot, 0, 1)$. The theory ST has the same strength as first-order Peano arithmetic (PA).

The theory would become much stronger, if the *axiom of infinity (Inf)* was added:

$$\exists x(\exists y\,(y \in x \wedge \forall z \neg z \in y) \wedge \forall y(y \in x \rightarrow \exists z(z \in x \wedge \forall w(w \in z \leftrightarrow w \in y \vee w \equiv y)))).$$

Intuitively, the closure properties of x ensure that x is infinite. The strengthened theory is ZERMELO-FRAENKEL set theory (without the axiom of choice), which is usually taken as the universal foundation of mathematics. We work with the weaker theory ST, since we want to show the GÖDEL incompleteness theorems for ST, which are alternative representations of the original GÖDEL incompleteness theorems for PA.

Definition 92. *The system* ZF *of the* ZERMELO-FRAENKEL axioms of set theory *consists of the axioms of* ST *together with the axiom of infinity. The axiom system* ZF$^-$ *consists of the* ZF*-axioms except the power set axiom. The system* EML *("elementary set theory") consists of the axioms* Ex*,* Ext*,* Pair*, and* Union*.*

Exercise 14. The system ST *without* the separation schema implies the separation schema.

19.3 Class terms

Most of the axioms have a form like

$$\forall \vec{x} \exists y \forall z\,(z \in y \leftrightarrow \varphi).$$

Intuitively, y is the collection or *class* of sets z which satisfy φ. The common notation for that class is

$$\{z|\varphi\}.$$

This is to be seen as a term, which assigns to the other parameters in φ the value $\{z|\varphi\}$. Since the result of such a term is not necessarily a set we call such terms *class terms*. It is very convenient to employ class terms *within* $\in$-formulas. We view this notation as an abbreviation for "pure" $\in$-formulas.

Definition 93. *A* class term *is of the form* $\{x|\varphi\}$ *where* x *is a variable and* $\varphi \in L^{\in}$*. If* $\{x|\varphi\}$ *and* $\{y|\psi\}$ *are class terms then*

- $u \in \{x|\varphi\}$ *stands for* $\varphi\frac{u}{x}$ *;*
- $u = \{x|\varphi\}$ *stands for* $\forall v\,(v \in u \leftrightarrow \varphi\frac{v}{x})$*;*
- $\{x|\varphi\} = u$ *stands for* $\forall v\,(\varphi\frac{v}{x} \leftrightarrow v \in u)$*;*
- $\{x|\varphi\} = \{y|\psi\}$ *stands for* $\forall v\,(\varphi\frac{v}{x} \leftrightarrow \psi\frac{v}{y})$*;*
- $\{x|\varphi\} \in u$ *stands for* $\exists v(v \in u \wedge v = \{x|\varphi\}$*;*
- $\{x|\varphi\} \in \{y|\psi\}$ *stands for* $\exists v(\psi\frac{v}{y} \wedge v = \{x|\varphi\}$*.*

In this notation, the separation schema becomes:

$$\forall x_1 ... \forall x_n \forall x \exists y\, y = \{z | z \in x \wedge \varphi(z, x_1, ..., x_n)\}.$$

We shall further extend this notation, first by giving specific names to important formulas and class terms.

Definition 94.

a) $\emptyset := \{x | x \neq x\}$ *is the* empty set*;*

b) $V := \{x | x = x\}$ *is the* universe*.*

We work in the theory ZF for the following propositions.

Proposition 95.

a) $\emptyset \in V$*.*

b) $V \notin V$ *(*Russell*'s antinomy).*

Proof. a) $\emptyset \in V$ abbreviates the formula

$$\exists v (v = v \wedge v = \emptyset).$$

This is equivalent to $\exists v\, v = \emptyset$ which again is an abbreviation for

$$\exists v \forall w\, (w \in v \leftrightarrow w \neq w).$$

Consider an arbitrary set x. Then the formula is equivalent to

$$\exists v \forall w\, (w \in v \leftrightarrow w \in x \wedge w \neq w).$$

This follows from the instance

$$\forall x \exists y \forall z\, (z \in y \leftrightarrow z \in x \wedge z \neq z)$$

of the separation schema for the formula $z \neq z$.
b) Assume that $V \in V$. By the schema of separation

$$\exists y\, y = \{z | z \in V \wedge z \notin z\}.$$

Let $y = \{z | z \in V \wedge z \notin z\}$. Then

$$\forall z\ (z \in y \leftrightarrow z \in V \wedge z \notin z).$$

This is equivalent to

$$\forall z\ (z \in y \leftrightarrow z \notin z).$$

Instantiating the universal quantifier with y yields

$$y \in y \leftrightarrow y \notin y$$

which is a contradiction. □

Definition 96. *Let A be a term. We also say that A is a* class*. A is a* set *iff $A \in V$. A is a* proper class *iff $A \notin V$.*

Set theory deals with sets and proper classes. Sets are the favoured objects of set theory, the axioms mainly state favourable properties of sets and set existence. Sometimes one says that a term A *exists* if $A \in V$. The intention of set theory is to construe important mathematical classes like the collection of natural and real numbers as sets so that they can be treated set-theoretically. Zermelo observed that this is possible by requiring some set existences together with the *restricted* separation principle.

Exercise 15. Show that the class $\{\{x\}|x \in V\}$ of *singletons* is a proper class.

We introduce further abbreviations. By a *term* we understand a class term or a variable, i.e., those terms which may occur in an extended $\in$-formula. We also introduce *bounded quantifiers* to simplify notation.

19.4 Properties of classes

Definition 97. *Let A be a term. Then $\forall x \in A\, \varphi$ stands for $\forall x(x \in A \rightarrow \varphi)$ and $\exists x \in A\, \varphi$ stands for $\exists x\, (x \in A \wedge \varphi)$.*

Definition 98. *Let $x, y, z, \ldots$ be variables and $X, Y, Z, \ldots$ be class terms. Define*

a) $X \subseteq Y := \forall x \in X\, x \in Y$, *$X$ is a* subclass *of Y;*

b) $X \cup Y := \{x|x \in X \vee x \in Y\}$ *is the* union *of X and Y;*

c) $X \cap Y := \{x|x \in X \wedge x \in Y\}$ *is the* intersection *of X and Y;*

d) $X \setminus Y := \{x|x \in X \wedge x \notin Y\}$ *is the* difference *of X and Y;*

e) $\bigcup X := \{x|\exists y \in X\, x \in y\}$ *is the* union *of X;*

f) $\bigcap X := \{x|\forall y \in X\, x \in y\}$ *is the* intersection *of X;*

g) $\mathcal{P}(X) = \{x|x \subseteq X\}$ *is the* power class *of X;*

h) $\{X\} = \{x|x = X\}$ *is the* singleton set *of X;*

i) $\{X, Y\} = \{x|x = X \vee x = Y\}$ *is the* (unordered) pair *of X and Y;*

j) $\{X_0, \ldots, X_{n-1}\} = \{x|x = X_0 \vee \ldots \vee x = X_{n-1}\}$.

One can prove the well-known boolean properties for these operations. We only give a few examples.

Proposition 99. *$X \subseteq Y \wedge Y \subseteq X \rightarrow X = Y$.*

Proposition 100. *$\bigcup \{x, y\} = x \cup y$.*

Proof. We show the equality by two inclusions:
($\subseteq$). Let $u \in \bigcup \{x, y\}$. $\exists v(v \in \{x, y\} \wedge u \in v)$. Let $v \in \{x, y\} \wedge u \in v$. $(v = x \vee v = y) \wedge u \in v$.
Case 1. $v = x$. Then $u \in x$. $u \in x \vee u \in y$. Hence $u \in x \cup y$.
Case 2. $v = y$. Then $u \in y$. $u \in x \vee u \in y$. Hence $u \in x \cup y$.

Conversely let $u \in x \cup y$. $u \in x \vee u \in y$.
Case 1. $u \in x$. Then $x \in \{x, y\} \wedge u \in x$. $\exists v(v \in \{x, y\} \wedge u \in v)$ and $u \in \bigcup \{x, y\}$.
Case 2. $u \in y$. Then $x \in \{x, y\} \wedge u \in x$. $\exists v(v \in \{x, y\} \wedge u \in v)$ and $u \in \bigcup \{x, y\}$. □

Combining the axioms of pairing and unions we obtain:

Lemma 101. *$\forall x_0, \ldots, x_{n-1}\, \{x_0, \ldots, x_{n-1}\} \in V$.*

Note that this is a *schema* of lemmas, one for each ordinary natural number n. We prove the *schema* by complete induction on n.

Proof. For $n = 0, 1, 2$ the lemma states that $\emptyset \in V$, $\forall x\, \{x\} \in V$, and $\forall x, y\, \{x, y\} \in V$ resp., and these are true by previous axioms and lemmas. For the induction step assume that the lemma holds for n, $n \geqslant 1$. Consider sets $x_0, \ldots, x_n$. Then

$$\{x_0, \ldots, x_n\} = \{x_0, \ldots, x_{n-1}\} \cup \{x_n\}.$$

The right-hand side exists in V by the inductive hypothesis and the union axiom. □

Remark 102. We are developing the axiom systems ST and ZF. These will be infinite schemas, lists, or *sets* of formulas. These schemas are formulated in the common mathematical language, which is able to speak about formulas, in particular $\in$-formulas, and is also able to speak about infinite collections of formulas. If we assume infinitely many axioms, we can conclude infinitely many consequences, like the above Lemma(s): $\forall x_0, \ldots, x_{n-1} \{x_0, \ldots, x_{n-1}\} \in V$. We view the common mathematical language as a *meta language* which is able to speak about an *object language* like the language of set theory. The meta language has common mathematical tools available. For example induction and recursion on the common natural numbers, to perform the recursion in the *previous schema of lemmas*. We shall approach the problem of meta theory versus object theory in an informal naive way.

19.5 Set-theoretical axioms in class term notation

We can now reformulate set-theoretical axioms using class terms; for brevity we omit initial universal quantifiers.

a) Extensionality: $x \subseteq y \wedge y \subseteq x \rightarrow x = y$.

b) Pairing: $\{x, y\} \in V$.

c) Union: $\bigcup x \in V$.

d) Powerset: $\mathcal{P}(x) \in V$.

e) Separation schema: for all terms A

$$x \cap A \in V.$$

f) Replacement: see later.

g) Foundation: for all terms A

$$A \neq \emptyset \rightarrow \exists x \in A\; x \cap A = \emptyset.$$

Also the axiom of infinity can be written as

$$\exists x\; (\emptyset \in x \wedge \forall u \in x\; u \cup \{u\} \in x).$$

20 Relations and functions

20.1 Ordered pairs and cartesian products

Ordered pairs are the basis for the theory of relations.

Definition 103. $(x, y) = \{\{x\}, \{x, y\}\}$ *is the* ordered pair *of x and y.*

Remark 104. There are sometimes discussions whether $(x,\ y)$ *is* the ordered pair of x and y , or to what degree it agrees with the intuitive notion of an ordered pair. Anyway, the next proposition shows that the set-theoretical term (x, y) has the properties expected from an intuitive ordered pair within the axiom system ST. There are, however, many other terms $t(x, y)$ that could be used instead of our choice.

Proposition 105. *$(x, y) \in V$, i.e., (x, y) is a set.*

$(x,y)=(x',y')\rightarrow x=y\wedge x'=y'$.

Definition 106. *Let $t(\vec{x})$ be a term in the variables $\vec{x}$ and let φ be an $\in$-formula. Then $\{t(\vec{x})|\varphi\}$ stands for $\{z|\exists\vec{x}(\varphi\wedge z=t(\vec{x})\}$.*

Definition 107. *Let A,B,R be terms. Define the cartesian product of A and B as*

$$A\times B=\{(a,b)|a\in A\wedge b\in B\}.$$

By the specific implementation of Kuratowski ordered pairs:

Lemma 108. *$A\times B\subseteq\mathcal{P}(\mathcal{P}(A\cup B))$.*

Proof. Let $(a,b)\in A\times B$. Then

$$\begin{array}{rcl} a,b & \in & A\cup B\\ \{a\},\{a,b\} & \subseteq & A\cup B\\ \{a\},\{a,b\} & \in & \mathcal{P}(A\cup B)\\ (a,b)=\{\{a\},\{a,b\}\} & \subseteq & \mathcal{P}(A\cup B)\\ (a,b)=\{\{a\},\{a,b\}\} & \in & \mathcal{P}(\mathcal{P}(A\cup B)) \end{array}$$

□

Proposition 109. *$x\times y\in V$.*

Proof. Exercise. □

20.2 Relations

Definition 110. *Let R be a term. Define*

a) R is a (binary) relation *if $R\subseteq V\times V$.*

b) If R is a binary relation write aRb instead of $(a,b)\in R$.

We can now introduce the standard notions and operations for relations:

Definition 111. *Let R,S,A be terms.*

a) The domain *of R is $\mathrm{dom}(R):=\{x|\exists y\,x\,R\,y\}$.*

b) The range *of R is $\mathrm{ran}(R):=\{y|\exists x\,x\,R\,y\}$.*

c) The field *of R is $\mathrm{field}(R):=\mathrm{dom}(R)\cup\mathrm{ran}(R)$.*

d) The restriction *of R to A is $R\upharpoonright A:=\{(x,y)|x\,Ry\wedge x\in A\}$.*

e) The image *of A under R is $R[A]:=R''A:=\{y|\exists x\in A\,x\,Ry\}$.*

f) The preimage *of A under R is $R^{-1}[A]:=\{x|\exists y\in A\,x\,Ry\}$.*

g) The composition *of S and R ("S after R") is $S\circ R:=\{(x,z)|\exists y\,(x\,Ry\wedge y\,Sz)\}$.*

h) The inverse *of R is $R^{-1}:=\{(y,x)|x\,Ry\}$.*

Relations can play different roles in mathematics.

Definition 112. *Let R be a relation.*

a) *R is* reflexive *iff* $\forall x \in \mathrm{field}(R)\ x R x$.

b) *R is* irreflexive *iff* $\forall x \in \mathrm{field}(R)\ \neg x R x$.

c) *R is* symmetric *iff* $\forall x, y\, (x R y \rightarrow y R x)$.

d) *R is* antisymmetric *iff* $\forall x, y\, (x R y \wedge y R x \rightarrow x = y)$.

e) *R is* transitive *iff* $\forall x, y, z\ (x R y \wedge y R z \rightarrow x R z)$.

f) *R is* connex *iff* $\forall x, y \in \mathrm{field}(R)\, (x R y \vee y R x \vee x = y)$.

g) *R is an* equivalence relation *iff R is reflexive, symmetric and transitive.*

h) *Let R be an equivalence relation. Then* $[x]_R := \{y | y R x\}$ *is the* equivalence class *of x modulo R.*

It is possible that an equivalence class $[x]_R$ is not a set: $[x]_R \notin V$. Then the formation of the collection of all equivalence classes modulo R may lead to contradictions. Another important family of relations is given by *order relations*.

Definition 113. *Let R be a relation.*

a) *R is a* partial order *iff R is reflexive, transitive and antisymmetric.*

b) *R is a* linear order *iff R is a connex partial order.*

c) *Let A be a term. Then R is a* partial order on A *iff R is a partial order and* $\mathrm{field}(R) = A$.

d) *R is a* strict partial order *iff R is transitive and irreflexive.*

e) *R is a* strict linear order *iff R is a connex strict partial order.*

Partial orders are often denoted by symbols like $\leqslant$, and strict partial orders by $<$. A common notation in the context of (strict) partial orders R is to write

$$\exists p R q \varphi \text{ and } \forall p R q \varphi \text{ for } \exists p (p R q \wedge \varphi) \text{ and } \forall p (p R q \rightarrow \varphi) \text{ resp.}$$

20.3 Functions

One of the most important notions in mathematics is that of a *function*.

Definition 114. *Let F be a term. Then F is a* function *if it is a relation which satisfies*

$$\forall x, y, y'\ (x F y \wedge x F y' \rightarrow y = y').$$

If F is a function then

$$F(x) := \{u | \forall y\, (x F y \rightarrow u \in y)\}$$

is the value *of F at x.*

If F is a function and $x F y$ then $y = F(x)$. If there is no y such that $x F y$ then

$$F(x) = \bigcap_{x F y} y = \bigcap \emptyset = V.$$

The “value” V at x may be read as “undefined”. A function can also be considered as the (indexed) sequence of its values, and we also write

$$(F(x))_{x \in A} \text{ or } (F_x)_{x \in A} \text{ instead of } F: A \rightarrow V.$$

We define notions associated with functions.

Definition 115. *Let F, A, B be terms.*

a) *F is a* function from A to B*, or* $F\colon A \rightarrow B$*, iff F is a function,* $\mathrm{dom}(F) = A$*, and* $\mathrm{range}(F) \subseteq B$.

b) *F is a* partial function from A to B*, or* $F\colon A \rightharpoonup B$*, iff F is a function,* $\mathrm{dom}(F) \subseteq A$*, and* $\mathrm{range}(F) \subseteq B$.

c) *F is a* surjective *function from A to B iff $F\colon A \rightarrow B$ and* $\mathrm{range}(F) = B$.

d) *F is an* injective *function from A to B iff $F\colon A \rightarrow B$ and*

$$\forall x, x' \in A\, (x \neq x' \rightarrow F(x) \neq F(x'))$$

e) *F is a* bijective *function from A* to *B, or $F\colon A \leftrightarrow B$, iff $F\colon A \rightarrow B$ is surjective and injective.*

f) ${}^{A}B := \{f \mid f\colon A \rightarrow B\}$ *is the class of all functions from A to B.*

Using functional notation we may now write the replacement schema as

F is a function → $F[x] \in V$.

One could now develop the usual theory of functions, formalize notions like surjective, injective, bijective, and prove that fundamental properties hold.

Proposition 116.

a) ${}^{x}y \subseteq \mathcal{P}(x \times y)$.

b) ${}^{x}y \in V$.

21 Ordinal numbers, induction and recursion

As a foundation of mathematics, set theory has to support the common systems of natural and real numbers. These will be constructed using a class of numbers specific for set theory, the *ordinal numbers*, which possibly extend the intuitive natural numbers beyond the finite. Whereas commonly natural numbers are used to enumerate finite sets, ordinal numbers will be used to enumerate arbitrary sets. Ordinal numbers allow induction and recursion.

21.1 ∈-Induction

The *axiom schema of foundation* provides structural information about the set theoretic universe V. Viewing $\in$ as some kind of order relation it states that every non-empty class has an $\in$-minimal element $x \in A$ such that the $\in$-predecessors of x are not in A. In the usual natural numbers, the existence of minimal numbers is equivalent to induction. We have a similar situation in set theory:

Theorem 117. *The foundation scheme is equivalent to the following,* PEANO*-type, induction scheme: for every term B postulate*

$$\forall x\, (x \subseteq B \rightarrow x \in B) \rightarrow B = V.$$

This says that if being in B is always "inherited" from all elements of a set to the set itself, then every set is in B. Since being an element of a class term $B=\{x|\ \varphi(x,\vec{x})\}$ is equivalent to satisfying φ we can rewrite the induction principle in a form similar to "complete induction" for natural numbers

$$\forall x((\forall y\in x\varphi(y,\vec{x}))\rightarrow\varphi(x,\vec{x}))\rightarrow\forall x\varphi(x,\vec{x}).$$

Proof. We prove the theorem by a chain of equivalences:

$$\begin{aligned}&\forall x\,(x\subseteq B\rightarrow x\in B)\rightarrow B=V\\ \Leftrightarrow\ &B\neq V\rightarrow\neg\forall x\,(x\subseteq B\rightarrow x\in B)\\ \Leftrightarrow\ &V\setminus B\neq\emptyset\rightarrow\exists x\,(x\subseteq B\wedge x\notin B)\\ \Leftrightarrow\ &V\setminus B\neq\emptyset\rightarrow\exists x\,(x\in(V\setminus B)\wedge x\cap(V\setminus B)=\emptyset).\end{aligned}$$

The latter is an instance of foundation for the class $V\setminus B$. □

This leads to:

Exercise 16. A relation R on a domain D is called *wellfounded*, iff for all terms A

$$\emptyset\neq A\wedge A\subseteq D\rightarrow\exists x\in A\ A\cap\{y\,|\,yRx\}=\emptyset.$$

Formulate and prove a principle for R-induction on D which coressponds to the assumption that R is wellfounded on D.

Exercise 17. Consider the axiom system HF consisting of the axioms of EML together with the induction principle: for every term B postulate

$$\forall x,y\,(x\subseteq B\wedge y\in B\rightarrow x\cup\{y\}\in B)\rightarrow B=V.$$

Show that every axiom of ZF except Inf is provable in HF, and that HF proves the *negation* of Inf (HF axiomatizes the **h**eriditarily **f**inite sets, i.e., those sets such that the set itself and all its iterated elements are finite).

21.2 Ordinal numbers

Definition 118.

a) $0:=\emptyset$ *is the number* zero.

b) *For any term t, $t+1:=t\cup\{t\}$ is the* successor *of t.*

We have to make sure that the +1-operation produces "new" numbers and does not run into some kind of dead end or circle, where, e.g., $t+1=t$. We use Foundation for this:

Lemma 119. *Let n be a natural number $\geqslant 1$. Then there are* no $x_0,\dots,x_{n-1}$ *such that*

$$x_0\in x_1\in\dots\in x_{n-1}\in x_0.$$

Proof. Assume not and let $x_0\in x_1\in\dots\in x_{n-1}\in x_0$. Let

$$A=\{x_0,\dots,x_{n-1}\}.$$

$A\neq\emptyset$ since $n\geqslant 1$. By foundation take $x\in A$ such that $A\cap x=\emptyset$.
Case 1. $x=x_0$. Then $x_{n-1}\in A\cap x=\emptyset$, contradiction.
Case 2. $x=x_i$, $i>0$. Then $x_{i-1}\in A\cap x=\emptyset$, contradiction. □

Lemma 120.

a) $x\neq x+1$*;*

b) *the function* $x \mapsto x+1$ *is injective.*

Proof. *b)* Assume $x+1=x\cup\{x\}=y\cup\{y\}=y+1$ but $x\neq y$. This implies $x\notin\{y\}$ and $x\in y$. Similarly $y\notin\{x\}$ and $y\in x$. This $\in$-cycle contradicts the previous Lemma. □

Let us define set-theoretic analogues of the standard natural numbers:

Definition 121. *Define*

a) $1:=0+1$*;*

b) $2:=1+1$*;*

c) $3:=2+1$*; ...*

From the context it will be clear, whether "3", say, is meant to be the standard number "three" or the set theoretical object

$$\begin{aligned} 3 &= 2\cup\{2\} \\ &= (1+1)\cup\{1+1\} \\ &= (\{\emptyset\}\cup\{\{\emptyset\}\})\cup\{\{\emptyset\}\cup\{\{\emptyset\}\}\} \\ &= \{\emptyset,\{\emptyset\},\{\emptyset\}\cup\{\{\emptyset\}\}\}. \end{aligned}$$

The set-theoretic axioms ensure that this interpretation of "three" has essential number-theoretic properties of "three".

Remark 122. With our definitions, the axiom of infinity is equivalent to

$$\exists x\,(0\in x\wedge\forall n\in x\; n+1\in x).$$

Intuitively this says that there is a set $\{0,1,2,3,...\}$ which contains all natural numbers (and possibly further elements).

So far, we only have formalizations of specific numbers like 0, 1, 2, ... We arrive at a general notion of "number" by identifying a common property of those numbers and making that the defining property for ordinal numbers. Not that

1. "Numbers" are ordered by the $\in$-relation:

   $$m<n \text{ iff } m\in n.$$

   E.g., $1\in 3$ but not $3\in 1$.

2. On each "number", the $\in$-relation is a *strict linear order*: $3=\{0,1,2\}$ is strictly linearly ordered by $\in$.

3. "Numbers" are "complete" with respect to smaller "numbers"

   $$i<j<m\rightarrow i\in m.$$

   This can be written with the $\in$-relation as

   $$i\in j\in m\rightarrow i\in m.$$

The latter is the notion transitivity essential for (axiomatic) set theory:

Definition 123.

a) A *is* transitive*,* $\mathrm{Trans}(A)$*, iff* $\forall y\in A\forall x\in y\, x\in A$.

b) x *is an* ordinal (number)*,* $\mathrm{Ord}(x)$*, if* $\mathrm{Trans}(x)\wedge\forall y\in x\,\mathrm{Trans}(y)$.

c) *Let* $\mathrm{Ord}:=\{x|\mathrm{Ord}(x)\}$ *be the class of all ordinal numbers.*

We shall use small greek letter α, β, ... as variables for ordinals. So $\exists\alpha\varphi$ stands for $\exists\alpha\in\mathrm{Ord}\,\varphi$, and $\{\alpha|\varphi\}$ for $\{\alpha|\mathrm{Ord}(\alpha)\wedge\varphi\}$.

Exercise 18. Show that arbitrary unions and intersections of transitive sets are again transitive.

We shall see that the ordinals extend the standard natural numbers. Ordinals are particularly adequate for enumerating infinite sets.

Theorem 124.

a) $0\in\mathrm{Ord}$.

b) $\forall\alpha\ \alpha+1\in\mathrm{Ord}$.

Proof. a) $\mathrm{Trans}(\emptyset)$ since formulas of the form $\forall y\in\emptyset...$ are tautologously true. Similarly $\forall y\in\emptyset\,\mathrm{Trans}(y)$.
b) Assume $\alpha\in\mathrm{Ord}$.
(1) $\mathrm{Trans}(\alpha+1)$.
Proof. Let $u\in v\in\alpha+1=\alpha\cup\{\alpha\}$.
Case 1. $v\in\alpha$. Then $u\in\alpha\subseteq\alpha+1$, since α is transitive.
Case 2. $v=\alpha$. Then $u\in\alpha\subseteq\alpha+1$. *qed*(1)
(2) $\forall y\in\alpha+1\,\mathrm{Trans}(y)$.
Proof. Let $y\in\alpha+1=\alpha\cup\{\alpha\}$.
Case 1. $y\in\alpha$. Then $\mathrm{Trans}(y)$ since α is an ordinal.
Case 2. $y=\alpha$. Then $\mathrm{Trans}(y)$ since α is an ordinal. □

Exercise 19.

a) Let $A\subseteq\mathrm{Ord}$ be a term, $A\neq\emptyset$. Then $\bigcap A\in\mathrm{Ord}$.

b) Let $x\subseteq\mathrm{Ord}$ be a set. Then $\bigcup x\in\mathrm{Ord}$.

Theorem 125. Trans(Ord).

Proof. This follows immediately from the transitivity definition of Ord. □

Exercise 20. Show that Ord is a proper class. (Hint: if $\mathrm{Ord}\in V$ then $\mathrm{Ord}\in\mathrm{Ord}$.)

Theorem 126. *The class* Ord *is strictly linearly ordered by* $\in$, *i.e.,*

a) $\forall\alpha,\beta,\gamma\,(\alpha\in\beta\wedge\beta\in\gamma\rightarrow\alpha\in\gamma)$.

b) $\forall\alpha\,\alpha\notin\alpha$.

c) $\forall\alpha,\beta\,(\alpha\in\beta\vee\alpha=\beta\vee\beta\in\alpha)$.

Proof. a) Let $\alpha,\beta,\gamma\in\mathrm{Ord}$ and $\alpha\in\beta\wedge\beta\in\gamma$. Then γ is transitive, and so $\alpha\in\gamma$.
b) follows immediately from the non-circularity of the $\in$-relation.
c) Assume that there are “incomparable” ordinals. By the foundation schema choose $\alpha_0\in\mathrm{Ord}$ $\in$-minimal such that $\exists\beta\neg(\alpha_0\in\beta\vee\alpha_0=\beta\vee\beta\in\alpha_0)$. Again, choose $\beta_0\in\mathrm{Ord}$ $\in$-minimal such that $\neg(\alpha_0\in\beta_0\vee\alpha_0=\beta_0\vee\beta_0\in\alpha_0)$. We obtain a contradiction by showing that $\alpha_0=\beta_0$:

Let $\alpha\in\alpha_0$. By the $\in$-minimality of α_0, α is comparable with β_0: $\alpha\in\beta_0\vee\alpha=\beta_0\vee\beta_0\in\alpha$. If $\alpha=\beta_0$ then $\beta_0\in\alpha_0$ and α_0,β_0 would be comparable, contradiction. If $\beta_0\in\alpha$ then $\beta_0\in\alpha_0$ by the transitivity of α_0 and again α_0, β_0 would be comparable, contradiction. Hence $\alpha\in\beta_0$.

For the converse let $\beta \in \beta_0$. By the $\in$-minimality of β_0 , β is comparable with $\alpha_0 : \beta \in \alpha_0 \vee \beta = \alpha_0 \vee \alpha_0 \in \beta$. If $\beta = \alpha_0$ then $\alpha_0 \in \beta_0$ and α_0, β_0 would be comparable, contradiction. If $\alpha_0 \in \beta$ then $\alpha_0 \in \beta_0$ by the transitivity of β_0 and again α_0, β_0 would be comparable, contradiction. Hence $\beta \in \alpha_0$.

But then $\alpha_0 = \beta_0$ contrary to the choice of β_0 . □

Definition 127. *Let* $<: = \in \cap (\mathrm{Ord} \times \mathrm{Ord}) = \{(\alpha, \beta) | \alpha \in \beta\}$ *be the natural strict linear ordering of* Ord *by the* $\in$*-relation.*

Theorem 128. *Let* $\alpha \in \mathrm{Ord}$*. Then* $\alpha + 1$ *is the immediate successor of* α *in the* $\in$*-relation:*

a) $\alpha < \alpha + 1$*;*

b) if $\beta < \alpha + 1$*, then* $\beta = \alpha$ *or* $\beta < \alpha$*.*

Definition 129. *Let* α *be an ordinal.* α *is a* successor ordinal*,* $\mathrm{Succ}(\alpha)$*, iff* $\exists \beta\, \alpha = \beta + 1$ *.* α *is a limit ordinal,* $\mathrm{Lim}(\alpha)$*, iff* $\alpha \neq 0$ *and* α *is not a successor ordinal. Also let*

$$\mathrm{Succ}: = \{\alpha | \mathrm{Succ}(\alpha)\} \textit{ and } \mathrm{Lim} := \{\alpha | \mathrm{Lim}(\alpha)\}.$$

The existence of limit ordinals will be discussed together with the formalization of the natural numbers.

21.3 Ordinal induction

Ordinals satisfy an *induction theorem* which generalizes *complete induction* on the integers:

Theorem 130. *Let* $\varphi(x, v_0, ..., v_{n-1})$ *be an* $\in$*-formula and* $x_0, ..., x_{n-1} \in V$*. Assume that the property* $\varphi(x, x_0, ..., x_{n-1})$ *is* inductive*, i.e.,*

$$\forall \alpha (\forall \beta \in \alpha\ \varphi(\beta, x_0, ..., x_{n-1}) \rightarrow \varphi(\alpha, x_0, ..., x_{n-1})).$$

Then φ *holds for all ordinals:*

$$\forall \alpha\, \varphi(\alpha, x_0, ..., x_{n-1}).$$

Proof. The inductivity assumption expands to

$$\forall x (x \in \mathrm{Ord} \rightarrow ((\forall y \in x\, (y \in \mathrm{Ord} \rightarrow \varphi(y, \vec{x}))) \rightarrow \varphi(x, \vec{x})))$$

with ordinary variables x, y which are not pretyped as ordinals. Since $A \rightarrow (B \rightarrow C)$ is propositionally equivalent to $B \rightarrow (A \rightarrow C)$ the expansion is equivalent to

$$\forall x ((\forall y \in x\, (y \in \mathrm{Ord} \rightarrow \varphi(y, \vec{x}))) \rightarrow (x \in \mathrm{Ord} \rightarrow \varphi(x, \vec{x}))).$$

This means that the property $(x \in \mathrm{Ord} \rightarrow \varphi(x, \vec{x}))$ is inductive in the sense of the induction schema for $\in$. So by that induction schema:

$$\forall x (x \in \mathrm{Ord} \rightarrow \varphi(x, \vec{x}))$$

which is equivalent to the desired

$$\forall \alpha\, \varphi(\alpha, x_0, ..., x_{n-1}).$$ □

Induction can be formulated in various forms:

Exercise 21. Prove the following transfinite induction principle: Let $\varphi(x) = \varphi(x, v_0, ..., v_{n-1})$ be an $\in$-formula and $x_0, ..., x_{n-1} \in V$. Assume

a) $\varphi(0)$ (the initial case),

b) $\forall\alpha\,(\varphi(\alpha)\rightarrow\varphi(\alpha+1))$ (the successor step),

c) $\forall\lambda\in\mathrm{Lim}\ (\forall\alpha<\lambda\,\varphi(\alpha)\rightarrow\varphi(\lambda))$ (the limit step).

Then $\forall\alpha\,\varphi(\alpha)$.

21.4 Ordinal recursion

Recursion, often also called induction, over the natural numbers is a ubiquitous method for defining mathematical objects. We prove the following *recursion theorem* for ordinals.

Theorem 131. *Let G: $V\rightarrow V$. Then there is a canonical class term F, given by the subsequent proof, such that*

$$F\colon\mathrm{Ord}\rightarrow V \textit{ and } \forall\alpha\ F(\alpha)=G(F\restriction\alpha).$$

We then say that F is defined recursively *(over the ordinals) by the* recursion rule G. *F is unique in the sense that if another term F' satisfies*

$$F'\colon\mathrm{Ord}\rightarrow V \textit{ and } \forall\alpha\ F'(\alpha)=G(F'\restriction\alpha)$$

then $F=F'$.

Proof. We say that $H\colon\mathrm{dom}(H)\rightarrow V$ is *G-recursive* if

$$\mathrm{dom}(H)\subseteq\mathrm{Ord}\,,\mathrm{dom}(H)\text{ is transitive, and }\forall\alpha\in\mathrm{dom}(H)\ H(\alpha)=G(H\restriction\alpha).$$

(1) Let H, H' be G-recursive. Then H, H' are *compatible*, i.e., $\forall\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\ H(\alpha)=H'(\alpha)$.
Proof. We want to show that

$$\forall\alpha\in\mathrm{Ord}\ (\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\rightarrow H(\alpha)=H'(\alpha)).$$

By the induction theorem it suffices to show that $\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\rightarrow H(\alpha)=H'(\alpha)$ is inductive, i.e.,

$\forall\alpha\in\mathrm{Ord}\ (\forall y\in\alpha\ \ (y\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\rightarrow H(y)=H'(y))\rightarrow(\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\rightarrow H(\alpha)=H'(\alpha)))$.

So let $\alpha\in\mathrm{Ord}$ and $\forall y\in\alpha\ (y\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\rightarrow H(y)=H'(y))$. Let $\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')$. Since $\mathrm{dom}(H)$ and $\mathrm{dom}(H')$ are transitive, $\alpha\subseteq\mathrm{dom}(H)$ and $\alpha\subseteq\mathrm{dom}(H')$. By assumption

$$\forall y\in\alpha\ H(y)=H'(y).$$

Hence $H\restriction\alpha=H'\restriction\alpha$. Then

$$H(\alpha)=G(H\restriction\alpha)=G(H'\restriction\alpha)=H'(\alpha).$$

qed(1)

Let

$$F:=\bigcup\ \{f|f\text{ is }G\text{-recursive}\}.$$

be the union of the class of all *approximations* to the desired function F.
(2) F is G-recursive.
Proof. By (1), F is a function. Its domain $\mathrm{dom}(F)$ is the union of transitive classes of ordinals and hence $\mathrm{dom}(F)\subseteq\mathrm{Ord}$ is transitive.

Let $\alpha\in\mathrm{dom}(F)$. Take some G-recursive function$f$ such that $\alpha\in\mathrm{dom}(f)$. Since $\mathrm{dom}(f)$ is transitive, we have

$$\alpha\subseteq\mathrm{dom}(f)\subseteq\mathrm{dom}(F).$$

Moreover

$$F(\alpha) = f(\alpha) = G(f \upharpoonright \alpha) = G(F \upharpoonright \alpha).$$

qed(2)
(3) $\forall \alpha\, \alpha \in \mathrm{dom}(F)$.
Proof. By induction on the ordinals. We have to show that $\alpha \in \mathrm{dom}(F)$ is inductive in the variable α. So let $\alpha \in \mathrm{Ord}$ and $\forall y \in \alpha\, y \in \mathrm{dom}(F)$. Hence $\alpha \subseteq \mathrm{dom}(F)$. Let

$$f = F \upharpoonright \alpha \cup \{(\alpha, G(F \upharpoonright \alpha))\}.$$

f is a function with $\mathrm{dom}(f) = \alpha + 1 \in \mathrm{Ord}$. Let $\alpha' < \alpha + 1$. If $\alpha' < \alpha$ then

$$f(\alpha') = F(\alpha') = G(F \upharpoonright \alpha') = G(f \upharpoonright \alpha').$$

if $\alpha' = \alpha$ then also

$$f(\alpha') = f(\alpha) = G(F \upharpoonright \alpha) = G(f \upharpoonright \alpha) = G(f \upharpoonright \alpha').$$

Hence f is G-recursive and $\alpha \in \mathrm{dom}(f) \subseteq \mathrm{dom}(F)$. *qed*(3)

The extensional uniqueness of F follows from (1) □

Theorem 132. *Let $a_0 \in V$, G_{succ}: $\mathrm{Ord} \times V \to V$, and $G_{\lim}$: $\mathrm{Ord} \times V \to V$. Then there is a canonically defined class term F: $\mathrm{Ord} \to V$ such that*

a) $F(0) = a_0$ *;*

b) $\forall \alpha\, F(\alpha + 1) = G_{\mathrm{succ}}(\alpha, F(\alpha))$*;*

c) $\forall \lambda \in \mathrm{Lim}\ F(\lambda) = G_{\lim}(\lambda, F \upharpoonright \lambda)$.

Again F is unique in the sense that if some F' also satisfies a)-c) then $F = F'$.

We say that F is recursively defined *by the properties a)-c).*

Proof. We incorporate a_0, G_{succ}, and $G_{\lim}$ into a single recursion rule G: $V \to V$,

$$G(f) = \begin{cases} a_0 \text{ , if } f = \emptyset, \\ G_{\mathrm{succ}}(\alpha, f(\alpha)) \text{ , if } f\colon \alpha + 1 \to V, \\ G_{\lim}(\lambda, f) \text{ , if } f\colon \lambda \to V \text{ and } \mathrm{Lim}(\lambda), \\ \emptyset \text{ , else.} \end{cases}$$

Then the term F: $\mathrm{Ord} \to V$ defined recursively by the recursion rule G satisfies the theorem. □

In many cases, the *limit rule* will just require to form the union of the previous values so that

$$F(\lambda) = \bigcup_{\alpha < \lambda} F(\alpha).$$

Such recursions are called *continuous* (at limits).

21.5 Ordinal arithmetic

We extend the recursion rules of standard integer arithmetic continuously to obtain transfinite version of the arithmetic operations. The initial operation of ordinal arithmetic is the +1-operation defined before. Ordinal arithmetic satisfies some but not all laws of integer arithmetic.

Definition 133. *Define* ordinal addition $+\colon \mathrm{Ord}\times\mathrm{Ord}\to\mathrm{Ord}$ *recursively by*

$$\begin{aligned}\delta+0 &= \delta\\ \delta+(\alpha+1) &= (\delta+\alpha)+1\\ \delta+\lambda &= \bigcup_{\alpha<\lambda}(\delta+\alpha)\ ,\ \textit{for limit ordinals } \lambda\end{aligned}$$

Definition 134. *Define* ordinal multiplication $\cdot:\mathrm{Ord}\times\mathrm{Ord}\to\mathrm{Ord}$ *recursively by*

$$\begin{aligned}\delta\cdot 0 &= 0\\ \delta\cdot(\alpha+1) &= (\delta\cdot\alpha)+\delta\\ \delta\cdot\lambda &= \bigcup_{\alpha<\lambda}(\delta\cdot\alpha)\ ,\ \textit{for limit ordinals } \lambda\end{aligned}$$

Definition 135. *Define* ordinal exponentiation $\_^{-}:\mathrm{Ord}\times\mathrm{Ord}\to\mathrm{Ord}$ *recursively by*

$$\begin{aligned}\delta^0 &= 1\\ \delta^{\alpha+1} &= \delta^\alpha\cdot\delta\\ \delta^\lambda &= \bigcup_{\alpha<\lambda}\delta^\alpha\ ,\ \textit{for limit ordinals } \lambda\end{aligned}$$

Exercise 22. Explore which of the standard *ring axioms* hold for the ordinals with addition and multiplication. Give proofs and counterexamples.

21.6 Sequences

(Finite and infinite) *sequences* are important in many contexts.

Definition 136.

a) *A set w is an α-*sequence *iff $w\colon\alpha\to V$; then α is called the* length *of the α-sequence w and is denoted by $|w|$. w is a* sequence *iff it is an α-sequence for some α.*

b) *Let $w\colon\alpha\to V$ and $w'\colon\alpha'\to V$ be sequences. Then the* concatenation $w\hat{\ }w'\colon\alpha+\alpha'\to V$ *is defined by*

$$(w\hat{\ }w')\restriction\alpha = w \text{ and } \forall i<\alpha'\ (w\hat{\ }w')(\alpha+i)=w'(i).$$

c) *Let $w\colon\alpha\to V$ and $x\in V$. Then the* adjunction wx *of w by x is defined as*

$$wx = w\hat{\ }\{(0,x)\}.$$

Sequences and the concatenation operation satisfy algebraic laws of a *monoid* with some cancellation rules.

Proposition 137. *Let w, w', w'' be sequences. Then*

a) $(w\hat{\ }w')\hat{\ }w'' = w\hat{\ }(w'\hat{\ }w'')$.

b) $\emptyset\hat{\ }w = w\hat{\ }\emptyset = w$.

c) $w\hat{\ }w' = w\hat{\ }w'' \to w' = w''$.

There are many other operations on sequences. One can *permute* sequences, substitute elements of a sequence, etc.

22 Cardinals

Set theory is mainly concerned with "sizes" of arbitrary sets.

Definition 138.

a) x *and* y *are* equipollent*, or* equipotent*, or have* the same cardinality*, written* $x\sim y$*, if* $\exists f f\colon x\leftrightarrow y$*.*

b) x *has* cardinality at most that of y*, written* $x\preccurlyeq y$*, if* $\exists f f\colon x\rightarrow y$ *is injective.*

c) We write $x\prec y$ *for* $x\preccurlyeq y$ *and* $x\nsim y$*.*

These relations are easily shown to satisfy

Lemma 139.

a) $\sim$ *is an equivalence relation on* V*.*

b) $x\sim y\rightarrow x\preccurlyeq y\wedge y\preccurlyeq x$*.*

c) $x\preccurlyeq x$*.*

d) $x\preccurlyeq y\wedge y\preccurlyeq z\rightarrow x\preccurlyeq z$*.*

e) $x\subseteq y\rightarrow x\preccurlyeq y$*.*

The next Theorem is Cantor's famous result that a powerset has strictly more elements than the original set, expressed by the existence of injective functions.

Theorem 140. *Let* $x\in V$*.*

a) There is an injective map $f\colon x\rightarrow\mathcal{P}(x)$*.*

b) There is no injective map $g\colon\mathcal{P}(x)\rightarrow x$*.*

c) $x\prec\mathcal{P}(x)$*.*

Proof. a) Define the map $f\colon x\rightarrow\mathcal{P}(x)$ by $u\mapsto\{u\}$. This is a set since

$$f=\{(u,\{u\})|u\in x\}\subseteq x\times\mathcal{P}(x)\in V.$$

f is injective: let $u,u'\in x$, $u\neq u'$. By extensionality,

$$f(u)=\{u\}\neq\{u'\}=f(u').$$

b) Assume there were an injective map $g\colon\mathcal{P}(x)\rightarrow x$. Define the CANTORean set

$$c=\{u|u\in x\wedge u\notin g^{-1}(u)\}\in\mathcal{P}(x)$$

similar to the class R in RUSSELL's paradox.

Let $u_0=g(c)$. Then $g^{-1}(u_0)=c$ and

$$u_0\in c\leftrightarrow u_0\notin g^{-1}(u_0)=c.$$

Contradiction. □

We shall show later that the axiom of choice implies that every set is equipollent with an ordinal (Theorem 163 c). This motivates to take the minimal such ordinal as the canonical representative of the equivalence class with respect to $\sim$, called the *cardinality* of x. But even without the axiom of choice we make the formal definition

Definition 141.

a) $\mathrm{card}(x) = \min\ \{\alpha \mid \exists f f\colon \alpha \leftrightarrow x\}$ *is the* cardinality *of the set* x*. One also writes* $\bar{\bar{x}} = \mathrm{card}(x)$*.*

b) *An ordinal* κ *is a* cardinal *iff* $\kappa = \mathrm{card}(x)$ *for some set* x*.*

c) *Let* $\mathrm{Cd} = \{\kappa \in \mathrm{Ord} \mid \kappa$ *is a cardinal*$\}$ *be the class of all cardinals.*

Note that $\mathrm{card}(x)$ is undefined in case x is not equipollent with an ordinal.

23 Natural numbers and finite sets

23.1 Natural numbers

Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk.
(attributed to LEOPOLD KRONECKER, 1886)

We have $0, 1, \ldots \in \mathrm{Ord}$. All these intuitive natural numbers are equal to 0 or successor ordinals, i.e., not limit ordinals. We use this as the defining property of the natural numbers within the ordinal numbers.

Definition 142. n *is a* natural number *iff* $n \in \mathrm{Ord}$ *and* $\forall m \leqslant n \neg \mathrm{Lim}(m)$*. Let*

$$\mathbb{N} = \{n \mid n \textit{ is a natural number}\}$$

be the class *of natural numbers. We often use letters* k, l, m, n *as variables for natural numbers.*

Theorem 143.

a) $\mathbb{N} \subseteq \mathrm{Ord}$.

b) $0 \in \mathbb{N}$ *and* $n \in \mathbb{N} \rightarrow n + 1 \in \mathbb{N}$.

c) $\mathbb{N}$ *is transitive.*

d) $\mathbb{N}$ *is an initial segment of* Ord *with respect to* $<$*.*

Proof. *a)* and $0 \in \mathbb{N}$ hold trivially. Let $n \in \mathbb{N}$. Then $\forall m \leqslant n \neg \mathrm{Lim}(m)$. This immediately implies $\forall m \leqslant n + 1\ \neg \mathrm{Lim}(m)$ and so $n + 1 \in \mathbb{N}$.
c) Let $x \in n \in \mathbb{N}$. Then $\forall m \leqslant n \neg \mathrm{Lim}(m)$. Since $x \subseteq n$ we have $\forall m \leqslant x \neg \mathrm{Lim}(m)$. Then $x \in \mathbb{N}$ since x is also an ordinal.
d) is a reformulation of *c)*. □

Theorem 144. $\mathbb{N}$ *satisfies the schema of complete induction:*

$$(A \subseteq \mathbb{N} \wedge 0 \in A \wedge \forall n \in A\ n + 1 \in A) \rightarrow A = \mathbb{N}$$

holds for all terms A*.*

Proof. Assume that $A \subseteq \mathbb{N} \wedge 0 \in A \wedge \forall n \in A\ n + 1 \in A$. Assume for a contradiction that $A \neq \mathbb{N}$. By foundation take an $\in$-minimal $k \in \mathbb{N} \setminus A$.
(1) k is a limit ordinal.
Proof. k is an ordinal since it is a natural number. $k \neq 0$ since $0 \in A$. Assume that k were a successor ordinal of the form $k = n + 1$. $n \in A$ by the minimality of k. By the closure assumptions on A, $n + 1 \in A$ and $k \in A$ which contradicts the choice of k. *qed*(1)

But $k\in\mathbb{N}$ cannot be a limit ordinal, contradiction. □

Theorem 145. $\mathbb{N}$ *is closed with respect to ordinal addition and ordinal multiplication:*

$$m+n\in\mathbb{N} \textit{ and } m\cdot n\in\mathbb{N}.$$

Proof. Fix $m\in\mathbb{N}$. We prove the closure properties by induction on $n\in\mathbb{N}$:
(1) $m+n\in\mathbb{N}$.
Proof. Obviously $m+0=m\in\mathbb{N}$. Now assume $m+n\in\mathbb{N}$. Then

$$m+(n+1)=(m+n)+1\in\mathbb{N}.$$

So the property holds by complete induction. *qed*(1)
(2) $m\cdot N\in\mathbb{N}$.
Proof. Obviously $m\cdot 0=0\in\mathbb{N}$. Now assume $m\cdot n\in\mathbb{N}$. Using (1):

$$m\cdot(n+1)=m\cdot n+m\in\mathbb{N}.$$ □

Recall the axioms of Peano arithmetic:

Definition 146. *The axiom system* PA $\subseteq L^{S_{\mathrm{AR}}}$ *of* PEANO arithmetic *consists of the following sentences*

- $\forall x\, x+1\neq 0$
- $\forall x\forall y\ x+1=y+1\rightarrow x=y$
- $\forall x\, x+0=x$
- $\forall x\forall y\, x+(y+1)=(x+y)+1$
- $\forall x\, x\cdot 0=0$
- $\forall x\forall y\, x\cdot(y+1)=x\cdot y+x$
- *Schema of induction: for every formula* $\varphi(x_0,\ldots,x_{n-1},x_n)\in L^{S_{\mathrm{AR}}}$*:*

$$\forall x_0\ldots\forall x_{n-1}(\varphi(x_0,\ldots,x_{n-1},0)\wedge\forall x_n(\varphi\rightarrow\varphi(x_0,\ldots,x_{n-1},x_n+1))\rightarrow\forall x_n\,\varphi)$$

The preceding theorems can be interpreted to express that the class $\mathbb{N}$ of natural numbers together with $+\restriction(\omega\times\omega),\cdot\restriction(\omega\times\omega),<\restriction(\omega\times\omega),0,1$ is a model of Peano arithmetic. Note, that the induction theorem 144 is in general considerably stronger than the induction required in the Peano axioms, since the inductive formula may be any set theoretical formula, not just a formula from the language of arithmetic.

$\mathbb{N}$ is an adequate formalization of arithmetic within set theory since $\mathbb{N}$ satisfies all standard arithmetical axioms.

Exercise 23. Prove:

a) Addition and multiplication are commutative on $\mathbb{N}$.

b) Addition and multiplication on $\mathbb{N}$ satisfy the usual monotonicity laws with respect to $<$.

23.2 Finite cardinals

We shall show that $\mathbb{N}$ is the class of finite cardinals, which corresponds to the usual role of natural numbers to determine the size of finite sets.

Theorem 147. *For all natural numbers* n

a) $\mathrm{card}(n)=n$*;*

b) $n \in \mathrm{Cd}$.

Proof. *a*) By complete induction on n.

For $n = 0$, $\emptyset: 0 \leftrightarrow 0$ and hence $\mathrm{card}(0) = 0$.

Assume that $\mathrm{card}(n) = n$. We claim that $\mathrm{card}(n+1) = n+1$. Obviously $\mathrm{card}(n+1) \leqslant n+1$. Assume for a contradiction that $m = \mathrm{card}(n+1) < n+1$. Take $f: m \leftrightarrow n+1$. Let $f(i_0) = n$.

Case 1: $i_0 = m-1$. Then $f \upharpoonright (m-1): (m-1) \leftrightarrow n$ and $\mathrm{card}(n) \leqslant m-1 < n$, contradiction.

Case 2: $i_0 < m-1$. Then define $g: (m-1) \leftrightarrow n$ by

$$g(i) = \begin{cases} f(i)\,, \text{ if } i \neq i_0; \\ f(m-1)\,, \text{ if } i = i_0\,. \end{cases}$$

Hence $\mathrm{card}(n) \leqslant m-1 < n$, contradiction.

b) follows immediately from *a*). □

23.3 Finite sets

Definition 148. *x is* finite *if* $\mathrm{card}(x) \in \mathbb{N}$.

Theorem 149. *Let a, b finite, let $x \in V$.*

a) *Every subset of a finite set is finite.*

b) *$a \cup \{x\}$, $a \cup b$, $a \cap b$, $a \times b$, $a \setminus b$, and $\mathcal{P}(a)$ are finite. We have* $\mathrm{card}(\mathcal{P}(a)) = 2^{\mathrm{card}(a)}$.

c) *If a_i is finite for $i \in b$ then $\bigcup_{i<b} a_i$ is finite.*

Proof. By induction. □

Finite sets can be distinguished by dependencies between injective and surjective maps.

Theorem 150. *Let a be finite. Then*

a) $\forall f \left(f: a \xrightarrow{\text{inj.}} a \ \textit{implies}\ f: a \xrightarrow{\text{surj.}} a \right)$

b) $\forall f \left(f: a \xrightarrow{\text{surj.}} a \ \textit{implies}\ f: a \xrightarrow{\text{inj.}} a \right)$

Proof. By complete induction on $\mathrm{card}(a) \in \mathbb{N}$.

$\mathrm{card}(a) = 0$: there is exactly on function $\emptyset: \emptyset \rightarrow \emptyset$, and this is injective *and* surjective.

Assume that the theorem holds for all a with $\mathrm{card}(a) = n$. □

Using the axiom of choice one can also show the converse.

23.4 Finite sequences

Definition 151.

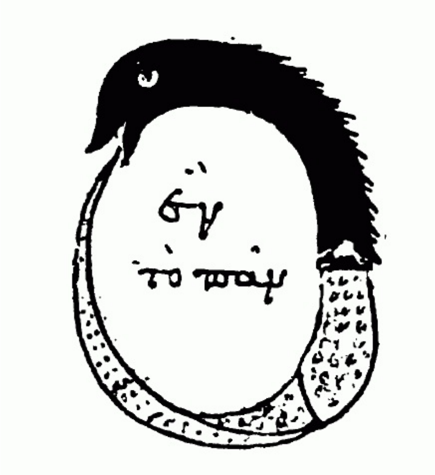
a) *A* sequence $w: |w| \rightarrow V$ *is called* finite *iff* $|w| < \omega$.

b) *A finite sequence $w: n \rightarrow V$ may be denoted by its enumeration $w_0, \ldots, w_{n-1}$ where we write w_i instead of $w(i)$. One also writes $w_0 \ldots w_{n-1}$ instead of $w_0, \ldots, w_{n-1}$, in particular if w is considered to be a* word *formed out of the* symbols $w_0, \ldots, w_{n-1}$.

By this definition, this text has gone full circle, since we started our investigations with finite sequences of symbols:

Definition 152. *Let S be a language. A* word over S *is a finite sequence* $w = w_0 w_1 \ldots w_{n-1}$ *of symbols* $w_0, \ldots, w_{n-1} \in S_0 \cup S$*. The natural number n is the* length *of w, we also write* $|w| = n$.

The empty word *is the unique sequence* $\square$ *with* $|\square| = 0$*. Let S^* be the class of all words over S.*



Ouroboros (tail-eater), 10th century

Recall that formulas are certain *finite sequences*. Sequents are *finite sequences* of formulas. Derivations in the sequent calculus are *finite sequences* of sequents. This will allow to do formal logic and ST itself within ST, leading to paradoxes and Gödel's incompleteness theorems.

Note that we have developed set theory so far from the axioms of ST without assuming the axiom of infinity or the axiom of choice.

24 Infinity

Mathematics is the science of the infinite.
(Herrmann Weyl,
Levels of Infinity, 1930)

Apart from its foundational role, set theory is mainly the study of infinite sets. The axiom of infinity (Inf) postulates the existence of some infinite set which will then spawn a whole universe of infinite sets:

$$\exists x\, (0 \in x \wedge \forall u \in x\ u + 1 \in x).$$

Theorem 153. *In the axiom system* ST*, the axiom of infinity is equivalent to $\mathbb{N}$ being a set:*

$$\mathrm{Inf} \leftrightarrow \mathbb{N} \in V.$$

Proof. If $\mathbb{N} \in V$ then $\mathbb{N}$ obviously is a witness to the axiom of infinity.

For the converse, take a set x such that $0 \in x \wedge \forall u \in x\ u + 1 \in x$. $A = x \cap \mathbb{N}$ is a set by separation. Then $0 \in A \wedge \forall n \in A\ n + 1 \in A$. By complete induction $A = \mathbb{N}$. Hence $\mathbb{N} \in V$. $\square$

Until further notice, we assume the axiom of infinity in the form $\mathbb{N} \in V$.

24.1 ω

Except being the *set* of natural numbers, $\mathbb{N}$ will be an ordinal and a cardinal as well. We introduce a constant symbol for $\mathbb{N}$ intended to emphasizes its role as an ordinal:

Definition 154. *Set* $\omega = \mathbb{N}$.

Note that ω is somewhat similar to the ∞-symbol sometimes used for "infinity".

Theorem 155.

a) $\omega \in V$.

b) $(\omega, 0, +1)$ *satisfy the* second order PEANO axiom*, i.e.,*

$$\forall x \subseteq \omega\, (0 \in x \wedge \forall n \in x\; n+1 \in x \rightarrow x = \omega).$$

c) $\omega \in \mathrm{Ord}$.

d) ω *is the smallest limit ordinal.*

Proof.
d) By b), every element of ω is transitive and it suffices to show that ω is transitive. Let

$$x = \{n | n \in \omega \wedge \forall m \in n\; m \in \omega\} \subseteq \omega.$$

We show that the hypothesis of c) holds for x. $0 \in x$ is trivial. Let $u \in x$. Then $u+1 \in \omega$. Let $m \in u+1$. If $m \in u$ then $m \in \omega$ by the assumption that $u \in x$. If $m = u$ then $m \in x \subseteq \omega$. Hence $u+1 \in x$ and $\forall u \in x\; u+1 \in x$. By b), $x = \omega$. So $\forall n \in \omega\, n \in x$, i.e.,

$$\forall n \in \omega \forall m \in n\; m \in \omega.$$

e) Of course $\omega \neq 0$. Assume for a contradiction that ω is a successor ordinal, say $\omega = \alpha + 1$. Then $\alpha \in \omega$. Since ω is closed under the $+1$-operation, $\omega = \alpha + 1 \in \omega$. Contradiction. Every ordinal smaller than ω is a natural number and not a limit ordinal. Hence ω is the smallest limit ordinal. □

Theorem 156.

a) $\mathrm{card}(\omega) = \omega$ *;*

b) $\omega \in \mathrm{Card}$.

Proof. Assume for a contradiction that $n = \mathrm{card}(\omega) < \omega$. Let $f\colon n \leftrightarrow \omega$. Define g: $(n-1) \rightarrow \omega$ by

$$g(i) = \begin{cases} f(i), \text{ if } f(i) < f(n-1), \\ f(i) - 1, \text{ if } f(i) > f(n-1). \end{cases}$$

(1) g is injective.
Proof. Let $i < j < n-1$.
Case 1. $f(i), f(j) < f(n-1)$. Then $g(i) = f(i) \neq f(j) = g(j)$.
Case 2. $f(i) < f(n-1) < f(j)$. Then $g(i) = f(i) < f(n-1) \leqslant f(j) - 1 = g(j)$.
Case 3. $f(j) < f(n-1) < f(i)$. Then $g(j) = f(j) < f(n-1) \leqslant f(i) - 1 = g(i)$.
Case 4. $f(n-1) < f(i), f(j)$. Then $g(i) = f(i) - 1 \neq f(j) - 1 = g(j)$. *qed*(1)
(2) g is surjective.
Proof. Let $k \in \omega$.
Case 1. $k < f(n-1)$. By the bijectivity of f take $i < n-1$ such that $f(i) = k$. Then $g(i) = f(i) = k$.
Case 2. $k \geqslant f(n-1)$. By the bijectivity of f take $i < n-1$ such that $f(i) = k+1$. Then $g(i) = f(i) - 1 = k$. *qed*(2)

But this is a contradiction to the supposed minimality of $n = \mathrm{card}(\omega)$. □

24.2 Countable sets

Definition 157.

a) x *is* infinite *if* x *is not finite.*

b) x *is* countable *if* $\mathrm{card}(x) \leqslant \omega$ *.*

c) x *is* countably infinite *if* $\mathrm{card}(x) = \omega$ *.*

d) x *is* uncountable *if* x *is not countable.*

Lemma 158.

a) $\mathrm{card}(\omega + 1) = \omega$ *.*

b) $\mathrm{card}(\omega + \omega) = \omega$ *.*

c) $\mathrm{card}(\omega \cdot \omega) = \omega$ *.*

Proof. *a)* Define $f_a \colon \omega \leftrightarrow \omega + 1$ by

$$f(n) = \begin{cases} \omega\,, \text{ if } n = 0 \\ n - 1\,, \text{ else} \end{cases}$$

b) Define $f_b \colon \omega \leftrightarrow \omega + \omega$ by

$$f(n) = \begin{cases} m\,, \text{ if } n = 2 \cdot m \\ \omega + m\,, \text{ if } n = 2 \cdot m + 1 \end{cases}$$

c) Define $f_c \colon \omega \leftrightarrow \omega \cdot \omega$ by

$$f(n) = \omega \cdot k + l, \text{ if } n = 2^k \cdot (2 \cdot l + 1) - 1$$

□

We have the following closure properties for countable sets:

Theorem 159.

a) *If* $z \subseteq \omega$ *then* z *is countable.*

b) *If there is an injection from* y *into* ω *then* y *is countable.*

c) *Every subset of a countable set is countable*

d) *If* a, b *are countable then* $a \cup \{x\}$*,* $a \cup b$*,* $a \cap b$*,* $a \times b$*,* $a \setminus b$ *are countable*

Proof. *a)* This follows from exercise 40.
b) Let $f \colon y \to \omega$ be injective. Then $f[y] \subseteq \omega$. By *a)*, $f[y]$ is countable. Then $y \sim f[y]$ is countable.
c) Let $a \subseteq b$ where b is countable. Then there is an injective $f \colon b \to \omega$. $f \upharpoonright a \colon a \to \omega$ is also injective, and so a is countable.
d) Countability will be shown by exhibiting injections into countable sets. The case $\cap$ and $\setminus$ are trivial. For the other cases let $f_a \colon a \to \omega$ and $f_b \colon b \to \omega$ be injective. Then define injective maps:

$$f_0 \colon a \cup \{x\} \to \omega,\ f_0(u) = \begin{cases} f_a(u) + 1, \text{ if } u \in a \\ 0, \text{ else} \end{cases}$$

$$f_1 \colon a \cup b \to \omega,\ f_1(u) = \begin{cases} 2 \cdot f_a(u) + 1, \text{ if } u \in a \\ 2 \cdot f_b(u), \text{ else} \end{cases}$$

$$f_2 \colon a \times b \rightarrow \omega,\, f_2(u, v) = 2^{f_a(u)} \cdot (2 \cdot f_b(v) + 1) \qquad \square$$

Remark 160. We cannot prove the following standard property within ST + Inf: if a_n is countable for $n < \omega$ then $\bigcup_{n<\omega} a_n$ is countable. Indeed one can show in axiomatic set theory, that the property is *not implied* by ST. We shall later prove the property in the stronger theory ZFC, using the axiom of choice.

24.3 ω-Sequences

Sequences of length or order-type ω are ubiquitous in mathematical analysis. There they are called (infinite) *sequences*. ω-sequences also come up in the context of *infinite series*.

Definition 161. *An (ω-)sequence $w \colon \omega \rightarrow V$ may be denoted by $w_0, w_1, \ldots$ where $w_0, w_1, \ldots$ suggests a definition of w.*

An analysis statement like

$$\lim_{n \rightarrow \infty} \frac{1}{n} = 0$$

is a statement about the ω-sequence $\frac{1}{1}, \frac{1}{2}, \ldots$.

$$\sum_{n=0}^{\infty} \frac{1}{n!} = e$$

is a limit statement about the ω-sequence

$$w_0, w_1, w_2, \ldots = \frac{1}{1}, \frac{1}{1} + \frac{1}{1}, \frac{1}{1} + \frac{1}{1} + \frac{1}{2}, \ldots$$

of partial sums. The factorial $n!$ is defined recursively by

$$\begin{aligned} 0! &= 1; \\ (n+1)! &= n! \cdot (n+1). \end{aligned}$$

(One could extend this continuously to $\alpha!$ for all ordinals α.) The partial sums w_n are defined recursively by

$$\begin{aligned} w_0 &= 1 \\ w_{n+1} &= w_n + \frac{1}{(n+1)!} \end{aligned}$$

Note that the recursions completely formalize the vague ...-notations above.

24.4 Uncountable sets

Recall Cantor's theorem that $x \prec \mathcal{P}(x)$. Thus $\mathcal{P}(\omega) = \mathcal{P}(\mathbb{N})$ is the "first" uncountable set that we encounter. The determination of its size is a central problem in axiomatic set theory, also because $\mathcal{P}(\omega)$ is equipollent to the set $\mathbb{R}$ of real numbers that we shall construct soon. Cantor spent a lot of effort to prove that the "continuum" $\mathbb{R}$ represents the smallest uncountable cardinal. This property is Cantor's *continuum hypothesis*. With the methods of *axiomatic set theory* one can prove that the continuum hypothesis cannot be decided (= proved or disproved) from the axioms of ZF or ZF with the axiom of choice if these theories are consistent.

25 The Axiom of Choice

Natural numbers $n \in \mathbb{N}$ are used to enumerate finite sets a as

$$a = \{a_0, a_1, \ldots, a_{n-1}\}.$$

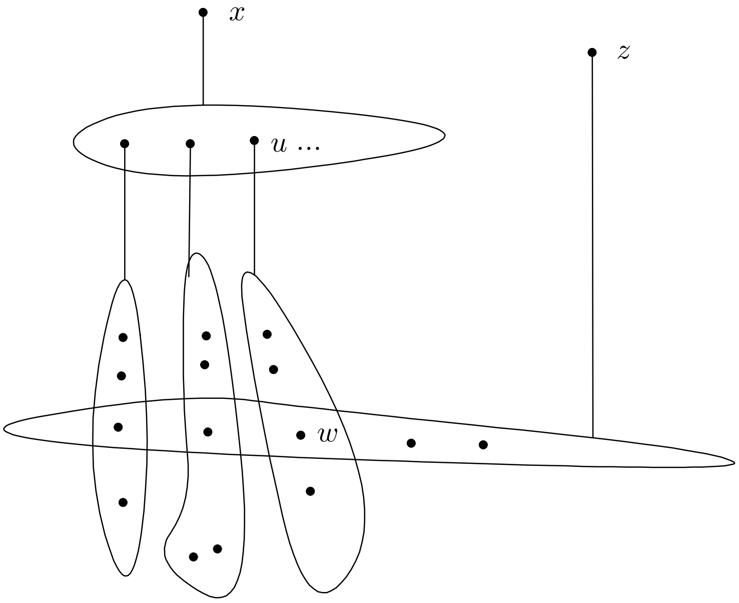
Assuming the *axiom of choice*, one can use ordinals to enumerate any set a as

$$a = \{a_i \mid i < \alpha\}.$$

Definition 162. *The* Axiom of Choice, AC *is the statement*

$$\forall x (\emptyset \notin x \wedge \forall u, v \in x (u \neq v \rightarrow u \cap v = \emptyset) \rightarrow \exists z \forall u \in x \exists w \, u \cap z = \{w\}).$$

The set z "chooses" one element out of every element of x .



It seems intuitively obvious that such choices are possible. On the other hand one can see that the axiom of choice has unintuitive, paradoxical consequences.

Theorem 163. *The following statements are equivalent:*

a) AC *;*

b) $\forall x \exists g$ *(*g *is a function with domain* $x \wedge \forall u \in x \, (u \neq \emptyset \rightarrow g(u) \in u)$*); such a function* g *is called a* choice function *for* x *;*

c) (Zermelo's Wellordering Theorem) $\forall x \exists \alpha \exists f f : \alpha \leftrightarrow x$.

d) $\mathrm{card}(x) \in \mathrm{Ord}$ *for every set* x *.*

Proof. *a)* → *b)* Assume AC. Let x be a set. We may assume that every element of x is nonempty. The class

$$x' = \{\{u\} \times u | u \in x\}$$

is the image of x under the set valued map $u\mapsto\{u\}\times u$, and thus a set by replacement. The elements $\{u\}\times u$ of x' are nonempty and pairwise disjoint. By AC, take a choice set z for x'. Define a choice function $g{:}\,x\to V$ by letting $g(u)$ be the unique element of u such that

$$(\{u\}\times u)\cap z=\{(u,g(u))\}.$$

$b)\to c)$ Assume $b)$. Let x be a set and let $g{:}\,\mathcal{P}(x)\setminus\{\emptyset\}\to V$ be a choice function for $\mathcal{P}(x)$. Define a function $F{:}\,\mathrm{Ord}\to x\cup\{x\}$ by ordinal recursion such that

$$F(\alpha)=\begin{cases} g(x\setminus F[\alpha]),\text{ if } x\setminus F[\alpha]\neq\emptyset;\\ x,\text{ if } x\setminus F[\alpha]=\emptyset.\end{cases}$$

At "time" α, the function F chooses an element $F(\alpha)\in x$ which has not been chosen before. If all elements of x have been chosen, this is signaled by F by the value x which is not an element of x.

(1) Let $\alpha<\beta$ and $F(\beta)\neq x$. Then $F(\alpha),F(\beta)\in x$ and $F(\alpha)\neq F(\beta)$.

Proof. $F(\beta)\neq x$ implies that $x\setminus F[\beta]\neq\emptyset$ and hence $F(\beta)=g(x\setminus F[\beta])\in x\setminus F[\beta]$. Since $\alpha\in\beta$, $x\setminus F[\alpha]\neq\emptyset$ and $F(\alpha)=g(x\setminus F[\alpha])\in x\setminus F[\alpha]$. $F(\alpha)\neq F(\beta)$ follows from $F(\beta)\in x\setminus F[\beta]$. *qed*(1)

(2) There is $\alpha\in\mathrm{Ord}$ such that $F(\alpha)=x$.

Proof. Assume not. Then by (1), F: $\mathrm{Ord}\to x$ is injective. Hence F^{-1} is a function and $\mathrm{Ord}=F^{-1}[x]$. By replacement, Ord is a set, but this is a contradiction. *qed*(2)

By (2) let α be minimal such that $F(\alpha)=x$. Let $f=F\upharpoonright\alpha{:}\,\alpha\to x$. By the definition of F, $x\setminus F[\alpha]=\emptyset$, i.e., $F[\alpha]=x$ and f is surjective. By (1), f is also injective, i.e., $f{:}\,\alpha\leftrightarrow x$.

The equivalence $c)\leftrightarrow d)$ is trivial.

$c)\to a)$ Assume $c)$. Let the set x consist of nonempty pairwise disjoint elements. Apply $c)$ to $\bigcup x$. Take an ordinal α and a function $f{:}\,\alpha\to\bigcup x$. Define a choice set z for x by setting

$$z=\{f(\xi)|\exists u\in x\,(f(\xi)\in u\wedge\forall\zeta<\xi f(\zeta)\notin u)\}.$$

So z chooses for every $u\in x$ that $f(\xi)\in u$ with ξ minimal. □

Let us assume AC until further notice. Then Cantor's two approaches to cardinality agree.

Theorem 164.

a) $x\preccurlyeq y\leftrightarrow\mathrm{card}(x)\leqslant\mathrm{card}(y)$.

b) $x\sim y\leftrightarrow\mathrm{card}(x)=\mathrm{card}(y)$.

Proof. *a)* Let $x\preccurlyeq y$ and let f: $x\to y$ be injective. Further let f_x: $\mathrm{card}(x)\leftrightarrow x$ and f_y: $\mathrm{card}(y)\leftrightarrow y$. Then $f_y^{-1}\circ f\circ f_x$: $\mathrm{card}(x)\to\mathrm{card}(y)$ is injective. Let $z=f_y^{-1}\circ f\circ f_x[\mathrm{card}(x)]\subseteq\mathrm{card}(y)$. By exercise 40(1), $\mathrm{card}(x)=\mathrm{card}(z)\leqslant\mathrm{card}(y)$.

Conversely, let $\mathrm{card}(x)\leqslant\mathrm{card}(y)$ with f_x: $\mathrm{card}(x)\leftrightarrow x$ and f_y: $\mathrm{card}(y)\leftrightarrow y$ as above. Then $f_y\circ f_x^{-1}{:}\,x\to y$ is injective and $x\preccurlyeq y$.

b) is trivial. □

As an immediate corollary we get the Cantor–Schröder–Bernstein theorem with AC. Actually the theorem could also be proven in ZF without the axiom of choice.

Theorem 165. (ZFC) *Let $a\preccurlyeq b$ and $b\preccurlyeq a$. Then $a\sim b$.*

Theorem 166. *Let $F{:}\,x\rightarrow V$. Then there exists a choice function $f{:}\,x\rightarrow V$ for F, i.e.,*

$$\forall u\in x\,(F(u)\neq\emptyset\rightarrow f(u)\in F(u)).$$

Proof. Let $g{:}\,\{F(u)|\,u\in x\}\rightarrow V$ be a choice function for the set $\{F(u)|\,u\in x\}$. The theorem then holds with $f{:}\,x\rightarrow V$ defined by

$$f(u)=g(F(u)).$$

□

Theorem 167. *If a_n is countable for $n<\omega$ then $\bigcup_{n<\omega}a_n$ is countable.*

Proof. By the axiom of choice "choose" a sequence $(h_n|n<\omega)$ of injections $h_n{:}\;a_n\rightarrow\omega$: Define $H{:}\,\omega\rightarrow V$ by

$$H(n)=\{h|\,h{:}\,a_n\rightarrow\omega\text{ is injective}\}.$$

By the previous theorem let $h{:}\,\omega\rightarrow V$ be a choice function for H. Then $h=(h_n|\,n<\omega)$ is as required.

Define an injection

$$f{:}\,\bigcup_{n<\omega}a_n\rightarrow\omega\,,\,f(u)=2^n\cdot(2\cdot h_n(u)+1),\text{ where }n\text{ is minimal such that }u\in a_n\,.$$

□

Zorn's Lemma is an important existence principle which is also equivalent to AC.

Definition 168. *Let $(P,\leqslant)$ be a partial order.*

a) $X\subseteq P$ is a chain *in $(P,\leqslant)$ if $(X,\leqslant)$ is a linear order where $(X,\leqslant)$ is a short notation for the structure $(X,\leqslant\cap X^2)$.*

b) An element $p\in P$ is an upper bound *for $X\subseteq P$ iff $\forall x\in X\,x\leqslant p$.*

c) $(P,\leqslant)$ is inductive *iff every chain in $(P,\leqslant)$ possesses an upper bound.*

d) An element $p\in P$ is a maximal element *of $(P,\leqslant)$ iff $\forall q\in P\,(q\geqslant p\rightarrow q=p)$.*

Theorem 169. *The axiom of choice is equivalent to the following principle, called Zorn's Lemma: every inductive partial order $(P,\leqslant)\in V$ possesses a maximal element.*

Proof. Assume AC and let $(P,\leqslant)\in V$ be an inductive partial order. Let $g{:}\,\mathcal{P}(P)\setminus\{\emptyset\}\rightarrow V$ be a choice function for $\mathcal{P}(P)\setminus\{\emptyset\}$. Define a function F: Ord $\rightarrow P\cup\{P\}$ by ordinal recursion; if there is an upper bound for $F[\alpha]$ which is not an element of $F[\alpha]$ let

$$F(\alpha)=g(\{p\in P\setminus F[\alpha]\,|\,p\text{ is an upper bound for }F[\alpha]\});$$

otherwise set

$$F(\alpha)=P.$$

At "time" α, the function F chooses a strict upper bound of $F[\alpha]$ if possible. If this is not possible, this is signaled by F by the value P.

The definition of F implies immediately:
(1) Let $\alpha<\beta$ and $F(\beta)\neq P$. Then $F(\alpha)<F(\beta)$.
(2) There is $\alpha\in\mathrm{Ord}$ such that $F(\alpha)=P$.
Proof. Assume not. Then by (1), F: Ord $\rightarrow P\in V$ is injective, and we get the same contradiction as in the proof of Theorem 163. *qed*(2)

By (2) let α be minimal such that $F(\alpha) = P$. By (1), $F[\alpha]$ is a chain in $(P, \leqslant)$. Since the partial order is inductive, take an upper bound p of $F[\alpha]$. We claim that p is a maximal element of $(P, \leqslant)$. Assume not and let $q \in P$, $q > p$. Then q is a strict upper bound of $F[\alpha]$ and $q \notin F[\alpha]$. But then the definition of F yields $F(\alpha) \neq P$, contradiction.

For the converse assume Zorn's Lemma and consider a set x consisting of nonempty pairwise disjoint elements. Define the set of "partial choice sets" which have empty or singleton intersection with every element of x:

$$P = \left\{z \subseteq \bigcup x \mid \forall u \in x (u \cap z = \emptyset \vee \exists w u \cap z = \{w\})\right\}.$$

P is partially ordered by $\subseteq$. If X is a chain in $(X, \subseteq)$ then $\bigcup X$ is an upper bound for X. Hence $(X, \subseteq)$ is inductive.

By Zorn's Lemma let z be a maximal element of $(X, \subseteq)$. We claim that z is a "total" choice set for x:
(3) $\forall u \in x \exists w u \cap z = \{w\}$.
Proof. If not, take $u \in x$ such that $u \cap z = \emptyset$. Take $w \in u$ and let $z' = z \cup \{w\}$. Then $z' \in P$, contrary to the the $\subseteq$-maximality of z. □

Theorem 170. *The axiom of choice is equivalent to the following principle, called* Hausdorff's Maximality Principle*: every partial order* $(P, \leqslant) \in V$ *possesses an* $\subseteq$*-maximal chain* $X \subseteq P$*, i.e.,* X *is a chain, and whenever* $X' \subseteq P$ *is a chain with* $X' \supseteq X$ *then* $X' = X$.

Proof. It is straightforward to show the equivalence with Zorn's Lemma. See also: Hausdorff, Grundzüge der Mengenlehre, p. 141: *Wir haben damit für eine teilweise geordnete Menge A die Existenz größter geordneter Teilmengen B bewiesen; natürlich kann es deren verschiedene geben.* □

Definition 171. *The axiom system* ZFC *consists of the* ZF*-axioms together with the axiom of choice* AC.

The system ZFC is the generally accepted foundation of mathematics. It provides adequate formalizations of all mathematical notions. We have seen this for the basic notions of relations, functions, (ordinal) numbers, cardinality, induction, recursion. Further notions like number systems, algebraic structures, etc. are available (We shall do number systems up to the real and complex numbers in the next chapter).

The ZF axioms have good motivations stemming from our intuitions about (small) finite sets. The axiom of choice is more controversial. AC has desirable consequences like Zorn's Lemma and its applications, but on the other hand AC has some paradoxical and problematic consequences like the existence of Lebesgue non-measurable sets of real numbers.

The status of AC within set theory can be compared to the parallel axiom in geometry. In (non-) euclidean geometry one can show that if the axioms without the parallel axiom are consistent then the axioms together with the parralel axiom are consistent. K. Gödel has shown in another of his groundbreaking results:

Theorem 172. *If* ZF *is consistent then* ZFC *is consistent.*

This meta-result about set theory belongs to the area of *axiomatic set theory* which studies the multitude of possible models of the ZF-axioms. Gödel's theorem is proved by defining a substructure L^M for any model M of ZF, so that $L^M \vDash \mathrm{ZFC}$. The proof is sophisticated and combines set theory with logical methods. It would typically be a main topic of an introductory course on "Models of Set Theory".

26 Number systems

To substantiate our claim that set theory is a/the foundation of mathematics, we have to model the standard number systems $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ in set theory. These systems are S_{AR}-structures where $S_{\mathrm{AR}} = \{+, \cdot, 0, 1\}$ is the language of arithmetic.

Theorem 173. *There are S_{AR}-structures*

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} = (\mathbb{C}, +, \cdot, 0, 1)$$

with the following properties:

a) *$\mathbb{C}$ is a field; for $a, b \in \mathbb{C}$ write $a - b$ for the unique element z such that $a = b + z$; for $a, b \in \mathbb{C}$ with $b \neq 0$ write $\frac{a}{b}$ for the unique element z such that $a = b \cdot z$;*

b) *there is a constant i, the* imaginary unit, *such that $i \cdot i + 1 = 0$ and*

$$\mathbb{C} = \{x + i \cdot y \,|x, y \in \mathbb{R}\};$$

c) *there is a strict linear order $<$ on $\mathbb{R}$ such that $(\mathbb{R}, <, + \upharpoonright \mathbb{R}^2, \cdot \upharpoonright \mathbb{R}^2, 0, 1)$ is an ordered field;*

d) *$(\mathbb{R}, <)$ is* complete, *i.e., bounded subsets of $\mathbb{R}$ possess suprema:*

$\forall X \subseteq \mathbb{R} \, (X \neq \emptyset \wedge \exists b \in \mathbb{R} \forall x \in X x \leqslant b \longrightarrow \exists b \in \mathbb{R} \, ((\forall x \in X x \leqslant b) \wedge \neg \exists b' < b \forall x \in X x \leqslant b'))$

e) *$\mathbb{Q}$ is* dense *in $(\mathbb{R}, <)$:*

$$\forall r, s \in \mathbb{R} \, (r < s \longrightarrow \exists a, b, c \in \mathbb{Q} \; a < r < b < s < c);$$

f) *$\mathbb{Q}$ is a field; moreover*

$$\mathbb{Q} = \left\{ \frac{a}{b} \,|a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} \right\};$$

g) *$\mathbb{Z}$ is a ring with unit; moreover*

$$\mathbb{Z} = \{a - b \,|a, b \in \mathbb{N}\};$$

h) $(\mathbb{N}, +1, 0)$ *satisfies the second-order* PEANO *axioms, i.e., the successor function $n \mapsto n + 1$ is injective, 0 is not in the image of the successor function, and*

$$\forall X \subseteq \mathbb{N} \, (0 \in X \wedge \forall n \in X n + 1 \in X \longrightarrow X = \mathbb{N}).$$

The existence proof will be carried out by constructing the systems $\mathbb{N}, \mathbb{Z}, \ldots$ successively in the subsections below. There are many degrees of freedom in the construction. Rational numbers, e.g., can be defined as equivalence classes of fractions, or as cancelled fractions. Nevertheless one can show that number systems satisfying the theorem are essentially unique:

Theorem 174. *If S_{AR}-structures*

$$\mathbb{N}' \subseteq \mathbb{Z}' \subseteq \mathbb{Q}' \subseteq \mathbb{R}' \subseteq \mathbb{C}' = (\mathbb{C}', +', \cdot', 0', 1')$$

also satisfy properties a)-h) of the preceding theorem, then there is a uniquely determined isomorphism

$$\pi: (\mathbb{C}, +, \cdot, 0, 1) \cong (\mathbb{C}', +', \cdot', 0', 1')$$

$\pi \upharpoonright \mathbb{Q}: (\mathbb{Q}, <, +, \cdot, 0, 1) \cong (\mathbb{Q}', <', +', \cdot', 0', 1')$*;*

such that

a) $\pi\restriction\mathbb{N}: (\mathbb{N}, +1, 0) \cong (\mathbb{N}', +'1', 0')$*;*

b) $\pi\restriction\mathbb{Z}: (\mathbb{Z}, +, \cdot, 0, 1) \cong (\mathbb{Z}', +', \cdot', 0', 1')$*;*

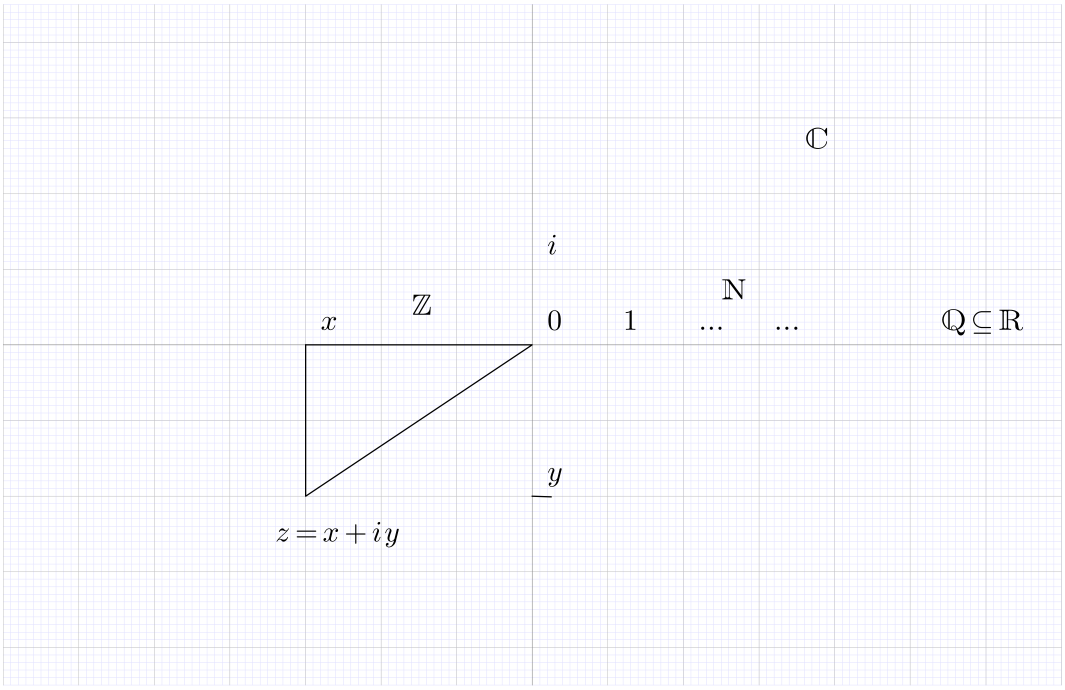
c) $\pi\restriction\mathbb{Q}: (\mathbb{Q}, <, +, \cdot, 0, 1) \cong (\mathbb{Q}', <', +', \cdot', 0', 1')$*;*

d) $\pi\restriction\mathbb{R}: (\mathbb{R}, <, +, \cdot, 0, 1) \cong (\mathbb{R}', <', +', \cdot', 0', 1')$*.*

The theorem can be proved by successively constructing $\pi\restriction\mathbb{N}$, $\pi\restriction\mathbb{Z}$, ...

So we can usually agree that we work with *the* natural numbers $\mathbb{N}$, *the* integers $\mathbb{Z}$, *the* rationals $\mathbb{Q}$, *the* reals $\mathbb{R}$ and *the* complex numbers $\mathbb{C}$. We can understand the concrete construction of the number systems as justification for augmenting the language of set theory by constants $\mathbb{N}, \mathbb{Z}, \ldots$ and axiomatically postulating properties *a)*-*h)*.

We can picture the number systems within the standard complex plane, possibly with an identification of $\mathbb{N}$ and ω.



26.1 Natural numbers

Definition 175. *The structure*

$$\mathbb{N}: = (\omega, +\restriction(\omega\times\omega), \cdot\restriction(\omega\times\omega), <\restriction(\omega\times\omega), 0, 1)$$

is called the structure of natural numbers*, or* arithmetic*. We usually denote this structure by*

$$\mathbb{N}: = (\omega, +, \cdot, <, 0, 1).$$

$\mathbb{N}$ is an adequate formalization of arithmetic within set theory since $\mathbb{N}$ satisfies all standard arithmetical axioms. $\mathbb{N}$ satisfies *h)* and *i)* of Theorem 173.

Exercise 24. Prove:

a) Addition and multiplication are commutative on ω.

b) Addition and multiplication satisfy the usual monotonicity laws with respect to $<$.

26.2 Integers

We shall first define a structure $\mathbb{Z}_0$ which will be isomorphic to the structure $\mathbb{Z}$ of integers. $\mathbb{N}$ can be canonically embedded into $\mathbb{Z}_0$; we obtain $\mathbb{Z}$ by replacing the image of $\mathbb{N}$ under the embedding by $\mathbb{N}$ itself

Definition 176. *We define the structure*

$$\mathbb{Z}_0 := (\mathbb{Z}_0, +^{\mathbb{Z}_0}, \cdot^{\mathbb{Z}_0}, <^{\mathbb{Z}_0}, 0^{\mathbb{Z}_0}, 1^{\mathbb{Z}_0})$$

of integers *as follows:*

a) *Define an equivalence relation* $\approx$ *on* $\mathbb{N} \times \mathbb{N}$ *by*

$$(a, b) \approx (a', b') \text{ iff } a + b' = a' + b.$$

b) *Let* $a - b := [(a, b)]_{\approx}$ *be the equivalence class of* (a, b) *in* $\approx$*. Note that every* $a - b$ *is a set.*

c) *Let* $\mathbb{Z}_0 := \{a - b | a \in \mathbb{N} \wedge b \in \mathbb{N}\}$ *be the set of* integers*.*

d) *Define the* addition $+^{\mathbb{Z}_0}: \mathbb{Z}_0 \times \mathbb{Z}_0 \rightarrow \mathbb{Z}_0$ *by*

$$(a - b) +^{\mathbb{Z}_0} (a' - b') := (a + a') - (b + b').$$

e) *Define the* multiplication $\cdot^{\mathbb{Z}_0}: \mathbb{Z}_0 \times \mathbb{Z}_0 \rightarrow \mathbb{Z}_0$ *by*

$$(a - b) \cdot^{\mathbb{Z}_0} (a' - b') := (a \cdot a' + b \cdot b') - (a \cdot b' + a' \cdot b).$$

f) *Define the strict linear order* $<^{\mathbb{Z}_0}$ *on* $\mathbb{Z}_0$ *by*

$$(a - b) <^{\mathbb{Z}_0} (a' - b') \text{ iff } a + b' < a' + b.$$

g) *Let* $0^{\mathbb{Z}_0} := 0 - 0$ *and* $1^{\mathbb{Z}_0} := 1 - 0$.

Exercise 25. Check that the above definitions are *sound*, i.e., that they do not depend on the choice of representatives of equivalence classes.

Exercise 26. Check that $\mathbb{Z}_0$ satisfies (a sufficient number) of the standard axioms for rings.

Define an injective map $e: \mathbb{N} \rightarrow \mathbb{Z}_0$ by

$$n \mapsto n - 0.$$

The embedding e is a *homomorphism*:

a) $e(0) = 0 - 0 = 0^{\mathbb{Z}_0}$ and $e(1) = 1 - 0 = 1^{\mathbb{Z}_0}$;

b) $e(m + n) = (m + n) - 0 = (m + n) - (0 + 0) = (m - 0) +^{\mathbb{Z}_0} (n - 0) = e(m) +^{\mathbb{Z}_0} e(n)$;

c) $e(m \cdot n) = (m \cdot n) - 0 = (m \cdot n + 0 \cdot 0) - (m \cdot 0 + n \cdot 0) = (m - 0) \cdot^{\mathbb{Z}_0} (n - 0) = e(m) \cdot^{\mathbb{Z}_0} e(n)$;

d) $m < n \leftrightarrow m + 0 < n + 0 \leftrightarrow (m - 0) <^{\mathbb{Z}_0} (n - 0) \leftrightarrow e(m) <^{\mathbb{Z}_0} e(n)$.

Hence $e: \mathbb{N} \rightarrow \mathbb{Z}_0$ is an embedding.

We prove a general theorem that allows to turn an embedded structure into a substructure:

Theorem 177. *Let* $\mathfrak{A}, \mathfrak{B}_0$ *be* S*-structures and let* $h: \mathfrak{A} \hookrightarrow \mathfrak{B}_0$ *be an embedding. Then there is an* S*-structure* $\mathfrak{B}$ *and an isomorphism* $\pi: \mathfrak{B}_0 \cong \mathfrak{B}$ *such that* $\mathfrak{A} \subseteq \mathfrak{B}$ *and*

$$\pi \circ h = \mathrm{id}_A.$$

Proof. Note that $B_0 \times \{A\}$ is disjoint from A. Let $B = (B_0 \setminus h[A]) \times \{A\} \cup A$ be a "disjoint union" of $B_0 \setminus h[A]$ and A. Define a map $\pi: B_0 \rightarrow B$ by

$$\pi(b) = \begin{cases} (b, A), \text{ if } b \in B_0 \setminus h[A] \\ h^{-1}(b), \text{ if } b \in h[A] \end{cases}$$

Let $\mathfrak{B}$ be the S-structure with domain B which is induced by the isomorphism π: for every n-ary relation symbol $R \in S$ and $b_0, ..., b_{n-1} \in B$ define

$$R^{\mathfrak{B}}(b_0, ..., b_{n-1}) \text{ iff } R^{\mathfrak{B}_0}(\pi^{-1}(b_0), ..., \pi^{-1}(b_{n-1}));$$

for every n-ary function symbol $f \in S$ and $b_0, ..., b_{n-1} \in B$ define

$$f^{\mathfrak{B}}(b_0, ..., b_{n-1}) = \pi(f^{\mathfrak{B}_0}(\pi^{-1}(b_0), ..., \pi^{-1}(b_{n-1}))).$$

By definition, $\pi: \mathfrak{B}_0 \cong \mathfrak{B}$.

$\pi \circ h = \mathrm{id}_A$ since for all $a \in A$: $\pi(h(a)) = h^{-1}(h(a)) = a$. id_A is an injective homomorphism since it is the composition of two homomorphisms. Hence $\mathfrak{A}$ is a substructure of $\mathfrak{B}$. □

By the theorem we can finally choose the structure

$$\mathbb{Z} = (\mathbb{Z}, +^{\mathbb{Z}}, \cdot^{\mathbb{Z}}, <^{\mathbb{Z}}, 0^{\mathbb{Z}}, 1^{\mathbb{Z}})$$

of integers, isomorphic to $\mathbb{Z}_0$ by $\pi: \mathbb{Z}_0 \cong \mathbb{Z}$ with $\pi \circ e: \mathbb{N} \subseteq \mathbb{Z}$. We can also write $+, \cdot, <, 0, 1$ instead of $+^{\mathbb{Z}}, \cdot^{\mathbb{Z}}, <^{\mathbb{Z}}, 0^{\mathbb{Z}}, 1^{\mathbb{Z}}$ since the relations and functions of $\mathbb{Z}$ extend those of $\mathbb{N}$. So we have extended the number system $\mathbb{N}$ to the number system $\mathbb{Z}$.

One can check straightforwardly that $\mathbb{Z}$ is a ring with unit. Let us show that

$$\mathbb{Z} = \{a - b \,|a, b \in \mathbb{N}\}:$$

Consider $z \in \mathbb{Z}$. Then $\pi^{-1}(z) \in \mathbb{Z}_0$. Take $a, b \in \mathbb{N}$ such that $\pi^{-1}(z) = a - b$, where the right-hand side is a formal difference as used in the definition of $\mathbb{Z}_0$. In $\mathbb{Z}_0$,

$$e(b) +^{\mathbb{Z}_0} (a - b) = (b - 0) +^{\mathbb{Z}_0} (a - b) = (a + b) - (b) = (a - 0) = e(a),$$

so that $a - b$ is the difference of $e(a)$ and $e(b)$ in $\mathbb{Z}$. Applying the isomorphism π , $z = \pi(a - b)$ is the difference of $\pi \circ e(a) = a$ and $\pi \circ e(b) = b$ in $\mathbb{Z}$. Thus $z = a - b$ in $\mathbb{Z}$.

So $\mathbb{Z}$ satisfies Theorem 162 *g*).

26.3 Rational numbers

As we constructed $\mathbb{Z}$ from formal *differences* $a - b$ of natural numbers, we shall now construct the rational numbers from formal *quotients* $\frac{a}{b}$ of integers.

Definition 178. *Define the structure*

$$\mathbb{Q}_0 := (\mathbb{Q}_0, +^{\mathbb{Q}_0}, \cdot^{\mathbb{Q}_0}, <^{\mathbb{Q}_0}, 0^{\mathbb{Q}_0}, 1^{\mathbb{Q}_0})$$

as follows:

a) Define an equivalence relation $\backsimeq$ *on* $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ *by*

$$(a, b) \backsimeq (a', b') \text{ iff } a \cdot b' = a' \cdot b.$$

b) Let $\frac{a}{b}$: $=[(a, b)]_{\simeq}$ *be the equivalence class of* (a, b) *in* $\simeq$. *Note that* $\frac{a}{b}$ *is a set.*

c) Let $\mathbb{Q}_0$: $=\{\frac{a}{b}|a \in \mathbb{Z} \wedge b \in (\mathbb{Z} \setminus \{0\})\}$.

d) Define the addition $+^{\mathbb{Q}_0}: \mathbb{Q}_0 \times \mathbb{Q}_0 \to \mathbb{Q}_0$ *by*

$$\frac{a}{b} +^{\mathbb{Q}_0} \frac{a'}{b'} := \frac{a \cdot b' + a' \cdot b}{b \cdot b'}.$$

e) Define the multiplication $\cdot^{\mathbb{Q}_0}: \mathbb{Q}_0^+ \times \mathbb{Q}_0^+ \to \mathbb{Q}_0^+$ *by*

$$\frac{a}{b} \cdot^{\mathbb{Q}_0} \frac{a'}{b'} := \frac{a \cdot a'}{b \cdot b'}.$$

f) Define the strict linear order $<^{\mathbb{Q}_0}$ *on* $\mathbb{Q}_0$ *by*

$$\frac{a}{b} <^{\mathbb{Q}_0} \frac{a'}{b'} \text{ iff } a \cdot b' < a' \cdot b.$$

g) Let $0^{\mathbb{Q}_0} := \frac{0}{1}$ *and* $1^{\mathbb{Q}_0} := \frac{1}{1}$.

Again one can check the soundness of the definitions and the well-known laws of standard rational numbers. Also one can canonically embed $\mathbb{Z}$ into $\mathbb{Q}_0$ by

$$a \mapsto \frac{a}{1}.$$

Again by theorem 165 we can now choose the structure

$$\mathbb{Q} = (\mathbb{Q}, +, \cdot, <, 0, 1)$$

of rational numbers to be isomorphic to $\mathbb{Q}_0$ so that $\mathbb{Q}$ extends the number system $\mathbb{Z}$.

26.4 Real numbers

Definition 179. $r \subseteq \mathbb{Q}^+ = \{p \in \mathbb{Q} | p \geqslant 0\}$ *is a* positive real number *if*

a) $\forall p \in r \forall q \in \mathbb{Q}^+ (q <^{\mathbb{Q}} p \to q \in r)$, *i.e., r is an initial segment of* $(\mathbb{Q}^+, <^{\mathbb{Q}})$;

b) $\forall p \in r \exists q \in r\, p <^{\mathbb{Q}} q$, *i.e., r is right-open in* $(\mathbb{Q}^+, <^{\mathbb{Q}})$;

c) $0 \in r \neq \mathbb{Q}^+$, *i.e., r is nonempty and bounded in* $(\mathbb{Q}^+, <^{\mathbb{Q}})$.

Definition 180. *We define the structure*

$$\mathbb{R}^+ := (\mathbb{R}^+, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, <^{\mathbb{R}}, 1^{\mathbb{R}})$$

of positive real numbers *as follows:*

a) Let $\mathbb{R}^+$ *be the set of* positive reals.

b) Define the real addition $+^{\mathbb{R}}: \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$ *by*

$$r +^{\mathbb{R}} r' = \{p +^{\mathbb{Q}} p' | p \in r \wedge p' \in r'\}.$$

c) Define the real multiplication $\cdot^{\mathbb{R}}: \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$ *by*

$$r \cdot^{\mathbb{R}} r' = \{p \cdot^{\mathbb{Q}} p' | p \in r \wedge p' \in r'\}.$$

d) Define the strict linear order $<^{\mathbb{R}}$ *on* $\mathbb{R}^+$ *by*

$$r <^{\mathbb{R}} r' \text{ iff } r \subseteq r' \wedge r \neq r'.$$

e) Let $1^{\mathbb{R}} := \{p \in \mathbb{Q}_0^+ | q <^{\mathbb{Q}} 1\}$.

We justify some details of the definition.

Lemma 181.

a) $\mathbb{R}^+ \in V$.

b) If $r, r' \in \mathbb{R}^+$ *then* $r +^{\mathbb{R}} r'$, $r \cdot^{\mathbb{R}} r' \in \mathbb{R}^+$.

c) $<^{\mathbb{R}}$ *is a strict linear order on* $\mathbb{R}^+$.

Proof. a) If $r \in \mathbb{R}^+$ then $r \subseteq \mathbb{Q}_0^+$ and $r \in \mathcal{P}(\mathbb{Q}_0^+)$. Thus $\mathbb{R}^+ \subseteq \mathcal{P}(\mathbb{Q}_0^+)$, and $\mathbb{R}^+$ is a set by the power set axiom and separation.
b) Let $r, r' \in \mathbb{R}^+$. We show that

$$r \cdot^{\mathbb{R}} r' = \{p \cdot^{\mathbb{Q}} p' | p \in r \wedge p' \in r'\} \in \mathbb{R}^+.$$

Obviously $r \cdot^{\mathbb{R}} r' \subseteq \mathbb{Q}_0^+$ is a non-empty bounded initial segment of $(\mathbb{Q}_0^+, <^{\mathbb{Q}})$.

Consider $p \in r \cdot^{\mathbb{R}} r'$, $q \in \mathbb{Q}_0^+$, $q <^{\mathbb{Q}} p$. Let $p = \frac{a}{b} \cdot^{\mathbb{Q}} \frac{a'}{b'}$ where $\frac{a}{b} \in r$ and $\frac{a'}{b'} \in r'$. Let $q = \frac{c}{d}$. Then $\frac{c}{d} = \frac{c \cdot b'}{d \cdot a'} \cdot^{\mathbb{Q}} \frac{a'}{b'}$, where

$$\frac{c \cdot b'}{d \cdot a'} = q \cdot^{\mathbb{Q}} \frac{b'}{a'} <^{\mathbb{Q}} p \cdot^{\mathbb{Q}} \frac{b'}{a'} = \frac{a}{b} \cdot^{\mathbb{Q}} \frac{a'}{b'} \cdot^{\mathbb{Q}} \frac{b'}{a'} = \frac{a}{b} \in r.$$

Hence $\frac{c \cdot b'}{d \cdot a'} \in r$ and

$$\frac{c}{d} = \frac{c \cdot b'}{d \cdot a'} \cdot^{\mathbb{Q}} \frac{a'}{b'} \in r \cdot^{\mathbb{R}} r'.$$

Similarly one can show that $r \cdot^{\mathbb{R}} r'$ is open on the right-hand side.
c) The transitivity of $<^{\mathbb{R}}$ follows from the transitivity of the relation $\subsetneqq$. To show that $<^{\mathbb{R}}$ is connex, consider $r, r' \in \mathbb{R}^+$, $r \neq r'$. Then r and r' are different subsets of $\mathbb{Q}_0^+$. Without loss of generality we may assume that there is some $p \in r' \setminus r$. We show that then $r <^{\mathbb{R}} r'$, i.e., $r \subsetneqq r'$. Consider $q \in r$. Since $p \notin r$ we have $p \not<^{\mathbb{Q}} q$ and $q \leqslant^{\mathbb{Q}} p$. Since r' is an initial segment of $\mathbb{Q}_0^+$, $q \in r'$. □

Exercise 27. Show that $(\mathbb{R}^+, \cdot^{\mathbb{R}}, 1^{\mathbb{R}})$ is a multiplicative group.

We can now construct the complete real line $\mathbb{R}$ from $\mathbb{R}^+$ just like we constructed $\mathbb{Z}$ from $\mathbb{N}$. Details are left to the reader. We can also proceed to define the structure $\mathbb{C}$ of complex numbers from $\mathbb{R}$.

Exercise 28. Formalize the structure $\mathbb{C}$ of complex numbers such that $\mathbb{R} \subseteq \mathbb{C}$.

27 The Alefs

We assume the theory ZFC for our considerations of cardinalities.

Theorem 182. $\forall \alpha \exists \kappa \in \mathrm{Card}\, \kappa > \alpha$. *Hence* Card *is a proper class of ordinals.*

Proof. Let $\alpha \geqslant \omega$. Then $\kappa = \mathrm{card}(\mathcal{P}(\alpha)) > \mathrm{card}(\alpha)$. And $\kappa > \alpha$ since otherwise $\mathrm{card}(\mathcal{P}(\alpha)) \leqslant \alpha$ and $\mathrm{card}(\mathrm{card}(\mathcal{P}(\alpha))) \leqslant \mathrm{card}(\alpha)$. □

Definition 183. *For any ordinal* δ *let* δ^+ *be the smallest cardinal* $> \delta$.

Theorem 184. *Let* $X \subseteq \mathrm{Cd}$ *be a set. Then* $\bigcup X \in \mathrm{Cd}$.

Proof. Set $\kappa = \bigcup X$. κ is an ordinal. Assume that $\mathrm{card}(\kappa) < \kappa$. Take $\lambda \in X$ such that $\mathrm{card}(\kappa) < \lambda$. Then $\lambda \leqslant \kappa$ and $\mathrm{card}(\lambda) \leqslant \mathrm{card}(\kappa) < \lambda$. But $\mathrm{card}(\lambda) = \lambda$ because λ is a cardinal. □

This allows the following

Definition 185. *Define the alef sequence*

$$(\aleph_\alpha | \alpha \in \mathrm{Ord})$$

recursively by

$$\begin{aligned} \aleph_0 &= \omega \\ \aleph_{\alpha+1} &= \aleph_\alpha^+ \\ \aleph_\lambda &= \bigcup_{\alpha<\lambda} \aleph_\alpha \textit{ for limit ordinals } \lambda \end{aligned}$$

Obviously

$$\mathrm{Card} = \{\aleph_\alpha | \alpha \in \mathrm{Ord}\}$$

is the class of all cardinals.

Exercise 29. There are cardinals κ such that $\kappa = \aleph_k$.

28 Cardinal Arithmetic

For disjoint *finite* sets a and b natural addition and multiplication satisfies

$$\mathrm{card}(a \cup b) = \mathrm{card}(a) + \mathrm{card}(b) \text{ and } \mathrm{card}(a \times b) = \mathrm{card}(a) \cdot \mathrm{card}(b).$$

This motivates the following extension of natural arithmetic to all cardinals.

Definition 186. *Let κ, λ finite or infinite cardinals. Then let*

a) $\kappa + \lambda = \mathrm{card}(a \cup b)$, where a, b are disjoint sets with $\kappa = \mathrm{card}(a)$ and $\lambda = \mathrm{card}(b)$; $\kappa + \lambda$ is the (cardinal) sum *of κ and λ.*

b) $\kappa \cdot \lambda = \mathrm{card}(\kappa \times \lambda)$; $\kappa \cdot \lambda$ is the (cardinal) product *of κ and λ.*

c) $\kappa^\lambda = \mathrm{card}({}^\lambda\kappa)$; κ^λ is the (cardinal) power *of κ and λ.*

Note that we are using the same notations as for *ordinal* arithmetic. It will usually be clear from the context whether ordinal or cardinal operations are intended.

The "arithmetic" properties of certain set operations yield usual arithmetic laws for cardinal arithmetic.

Lemma 187.

a) Cardinal addition is associative and commutative with neutral element 0*.*

b) Cardinal multiplication is associative and commutative with neutral element 1*.*

c) $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.

d) $\kappa^0 = 1$, $0^\kappa = 0$ for $\kappa \neq 0$, $\kappa^1 = \kappa$, $1^\kappa = 1$, $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$, $\kappa^{\lambda \cdot \mu} = (\kappa^\lambda)^\mu$.

Proof. *c)* Let a, b be disjoint sets with $\lambda = \mathrm{card}(a)$ and $\mu = \mathrm{card}(b)$. Then

$$\begin{aligned} \kappa \cdot (\lambda + \mu) &= \mathrm{card}(\kappa \times (a \cup b)) \\ &= \mathrm{card}((\kappa \times a) \cup (\kappa \times b)) \\ &= \mathrm{card}((\kappa \times a)) + \mathrm{card}((\kappa \times b)) \\ &= \kappa \cdot \lambda + \kappa \cdot \mu, \end{aligned}$$

using that $\kappa\times(a\cup b)=(\kappa\times a)\cup(\kappa\times b)$ and that $\kappa\times a$ and $\kappa\times b$ are disjoint.
d)

$$\kappa^0=\mathrm{card}({}^0\kappa)=\mathrm{card}(\{\emptyset\})=\mathrm{card}(1)=1.$$

In case $\kappa\neq 0$ we have that ${}^\kappa 0=\{f\,|\,f{:}\,\kappa\rightarrow\emptyset\}=\emptyset$ and thus

$$0^\kappa=\mathrm{card}({}^\kappa 0)=\mathrm{card}(\emptyset)=0.$$

For $\kappa^1=\kappa$ consider the map $\kappa\leftrightarrow{}^1\kappa$ given by $\alpha\mapsto\{(0,\alpha)\}$.
For $1^\kappa=1$ observe that ${}^\kappa 1=\{\{(\alpha,0)|\alpha<\kappa\}\}$ is a singleton set.

Let a,b be disjoint sets with $\lambda=\mathrm{card}(a)$ and $\mu=\mathrm{card}(b)$. Then

$$\begin{aligned}\kappa^{\lambda+\mu} &= \mathrm{card}({}^{a\cup b}\kappa)\\ &= \mathrm{card}(({}^a\kappa)\times({}^b\kappa))\\ &= \mathrm{card}({}^a\kappa)\cdot\mathrm{card}({}^b\kappa)\\ &= \kappa^\lambda\cdot\kappa^\mu\,,\end{aligned}$$

using that ${}^{a\cup b}\kappa\sim({}^a\kappa)\times({}^b\kappa)$ via the map $f\mapsto(f\upharpoonright a,f\upharpoonright b)$.

Finally,

$$\begin{aligned}\kappa^{\lambda\cdot\mu} &= \mathrm{card}({}^{\lambda\times\mu}\kappa)\\ &= \mathrm{card}({}^\mu({}^\lambda\kappa))\\ &= \mathrm{card}({}^\lambda\kappa)^\mu\\ &= (\kappa^\lambda)^\mu\,,\end{aligned}$$

using that ${}^{\lambda\times\mu}\kappa\sim{}^\mu({}^\lambda\kappa)$ via the map

$$f\mapsto(f_\xi|\xi<\mu)$$

where $f_\xi{:}\,\lambda\rightarrow\kappa$ with $f_\xi(\zeta)=f(\zeta,\xi)$, □

29 Further Cardinal Arithmetic

We determine the values of cardinal addition and multiplication for infinite cardinals.

Theorem 188.

a) *If* $\kappa\in\mathrm{Card}$ *then* $\kappa\cdot\kappa=\kappa$.

b) *If* $\kappa\in\mathrm{Card}$ *and* $\lambda\in\mathrm{Cd}$, $\lambda\neq 0$ *then* $\kappa\cdot\lambda=\max(\kappa,\lambda)$.

c) *If* $\kappa\in\mathrm{Card}$ *and* $\lambda\in\mathrm{Cd}$ *then* $\kappa+\lambda=\max(\kappa,\lambda)$.

Proof. *a)* $\kappa\cdot\kappa=\mathrm{card}(\kappa\times\kappa)=\kappa$, by the properties of the Gödel pairing function.
b) The map $i\mapsto(i,0)$ injects κ into $\kappa\times\lambda$, and the map $j\mapsto(0,j)$ injects λ into $\kappa\times\lambda$. Hence $\kappa,\lambda\leqslant\kappa\cdot\lambda$. Thus

$$\max(\kappa,\lambda)\leqslant\kappa\cdot\lambda\leqslant\max(\kappa,\lambda)\cdot\max(\kappa,\lambda)\overset{(a)}{=\!=}\max(\kappa,\lambda).$$

c) Obviously $\kappa\sim\{0\}\times\kappa$ and $\lambda\sim\{1\}\times\lambda$. The inclusion

$$(\{0\}\times\kappa)\cup(\{1\}\times\lambda)\subseteq\max(\kappa,\lambda)\times\max(\kappa,\lambda)$$

implies

$$\max(\kappa,\lambda)\leqslant\kappa+\lambda\leqslant\max(\kappa,\lambda)\cdot\max(\kappa,\lambda)\overset{(a)}{=\!=}\max(\kappa,\lambda).$$ □

For infinite cardinal *exponentiation* the situation is very different. Only a few values can be determined explicitely.

Lemma 189. *For* $\kappa \in \mathrm{Card}$ *and* $1 \leqslant n < \omega$ *we have* $\kappa^n = \kappa$.

Proof. By complete induction. $\kappa^1 = \kappa$ was proved before. And

$$\kappa^{n+1} = (\kappa^n) \cdot \kappa^1 = \kappa \cdot \kappa = \kappa. \qquad \square$$

The "next" exponential value $2^{\aleph_0}$ is however very undetermined. It is possible, in a sense to be made precise later, that $2^{\aleph_0}$ is any successor cardinal, like e.g. $\aleph_{13}$.

Cantor's continuum hypothesis is equivalent to the cardinal arithmetic statement

$$2^{\aleph_0} = \aleph_1.$$

30 LÖWENHEIM-SKOLEM theorems

We start to apply settheoretic methods to logic. For this we assume that ZFC set theory is part of the "metatheory" in which we study logic. Recall that the basic logical notions were introduced in terms of set theory: a language is a class of symbols, a structure consists of an underlying set together with other components.

Definition 190. *The* cardinality $\mathrm{card}(\mathfrak{A})$ *of an* S*-structure* $\mathfrak{A}$ *is defined as the cardinality of the underlying set* $|\mathfrak{A}|$. *Correspondingly* $\mathfrak{A}$ *is* finite, infinite, countable, *or* uncountable, *resp., iff the underlying set* $|\mathfrak{A}|$ *is finite, infinite, countable, or uncountable, resp.*

The Löwenheim-Skolem theorems study possible cardinalities of structures.

The set

$$S_0 = \{\equiv, \neg, \rightarrow, \bot, \forall, (,)\} \cup \{v_n | n \in \mathbb{N}\}$$

of basic logical symbol has cardinality $\aleph_0$. Recall:

Definition 191. *A* word over *a language* S *is a finite sequence* $w = w_0 w_1 \ldots w_{n-1}$ *of symbols* $w_0, \ldots, w_{n-1} \in S_0 \cup S$. S^* *is the class of all words over* S.

For the rest of the section, let all languages be sets. Then

Lemma 192. $\mathrm{card}(S^*) = \mathrm{card}(S) + \aleph_0$.

Proof. ($\geqslant$) $w \mapsto (w)$ is an injection from S in S^*; $n \mapsto v_n$ is an injection from $\mathbb{N}$ into S^*. Hence

$$\mathrm{card}(S) + \aleph_0 = \max(\mathrm{card}(S), \aleph_0) \leqslant \mathrm{card}(S^*).$$

($\leqslant$) $S^* = {}^{\omega}(S \cup S_0) = \bigcup_{n<\omega} {}^{n}(S \cup S_0)$.
(1) $\mathrm{card}({}^{n}(S \cup S_0)) = \mathrm{card}(S) + S_0$ for $1 \leqslant n < \omega$.
Proof. By complete induction on n. For $n = 1$,

$${}^{1}(S \cup S_0) \sim S \cup S_0 \sim \mathrm{card}(S) + \mathrm{card}(S_0) = \mathrm{card}(S) + \aleph_0.$$

For the induction step,

$${}^{n+1}(S \cup S_0) \sim^{n} (S \cup S_0) \times (S \cup S_0) \sim (\mathrm{card}(S) + \aleph_0) \cdot (\mathrm{card}(S) + \aleph_0) = \mathrm{card}(S) + \aleph_0.$$

qed(1)

Then

$$\operatorname{card}(S^*) = \operatorname{card}\left(\bigcup_{n<\omega} {}^n(S \cup S_0)\right) \leqslant \aleph_0 \times (\operatorname{card}(S) + \aleph_0) = \operatorname{card}(S) + \aleph_0 .$$

□

Theorem 193. *Let S be a language. Then*

$$\operatorname{card}(L^S) = \operatorname{card}(S) + \aleph_0 \geqslant \operatorname{card}(T^S) \geqslant \aleph_0 .$$

Proof. ($\geqslant$) To every symbol in $S \cup S_0$ we can assign a formula in L^S such that the assignment is injective.

($\leqslant$) holds, because $L^S \subseteq S^*$. □

We shall now revisit the Henkin model existence construction to determine the cardinalities of various parts of the construction. The main point from the cardinality viewpoint are the extensions of the language to obtain “witnesses”:

Theorem 194. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. Then there is a language S^ω and $\Phi^\omega \subseteq L^{S^\omega}$ such that*

a) *S^ω extends S by constant symbols, i.e., $S \subseteq S^\omega$ and if $s \in S^\omega \setminus S$ then s is a constant symbol;*

b) *$\Phi^\omega \supseteq \Phi$;*

c) *Φ^ω is consistent;*

d) *Φ^ω contains witnesses;*

e) $\operatorname{card}(L^{S^\omega}) = \operatorname{card}(\Phi^\omega) = \operatorname{card}(L^S)$.

Note that the original version of *e*) said: if L^S is countable then so are L^{S^ω} and Φ^ω.

Proof. We only have to take card of *e*) along the original construction.

We defined language extensions $S \mapsto S^+$ by

$$S^+ = S \cup \{c_\psi | \psi \in L^S\}$$

and extensions $\Phi \mapsto \Phi^+$ of sets of formulas by

$$\Phi^+ = \Phi \cup \{\neg\forall x\varphi \rightarrow \neg\varphi\frac{c_{\forall x\varphi}}{x} | \forall x\varphi \in L^S\}.$$

The cardinality of such unions is defined by the greatest summand, hence:

$$\operatorname{card}(S^+) = \operatorname{card}(\Phi^+) = \operatorname{card}(L^S).$$

We then iterated the +-operation through the integers:

$$\begin{aligned} \Phi^0 &= \Phi \\ S^0 &= S \\ S^{n+1} &= (S^n)^+ \\ \Phi^{n+1} &= (\Phi^n)^+ \\ S^\omega &= \bigcup_{n\in\mathbb{N}} S^n \\ \Phi^\omega &= \bigcup_{n\in\mathbb{N}} \Phi^n . \end{aligned}$$

By complete induction over $\mathbb{N}$ we can show:

$$\operatorname{card}(S^{n+1}) = \operatorname{card}(\Phi^{n+1}) = \operatorname{card}(L^S).$$

Finally

$$\operatorname{card}(L^{S^\omega}) = \operatorname{card}(S^\omega) = \aleph_0 \cdot \operatorname{card}(L^S) = \operatorname{card}(L^S)$$

and

$$\operatorname{card}(\Phi^\omega) = \operatorname{card}(L^S) \qquad \square$$

In the Henkin construction, Φ^ω is further extended to a Henkin set $\Phi^* \subseteq L^{S^\omega}$without further extending the language. So one gets:

Theorem 195. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. Then there is a language S^* and $\Phi^* \subseteq L^{S^*}$ such that*

a) $S^* \supseteq S$ is an extension of S by constant symbols;

b) $\Phi^* \supseteq \Phi$ is a HENKIN *set;*

c) $\operatorname{card}(L^{S^*}) = \operatorname{card}(\Phi^*) = \operatorname{card}(L^S)$.

The corresponding term model $\mathcal{T}^{\Phi^*}$ is build from equivalence sets of L^{S^*}-terms. Hence

$$\operatorname{card}(\mathcal{T}^{\Phi^*}) \leqslant \operatorname{card}(L^S).$$

In the countable case we get:

Theorem 196. (Downward LÖWENHEIM-SKOLEM theorem) *Let $\Phi \subseteq L^S$ be a* countable *consistent set of formulas. Then Φ possesses a model $\mathfrak{M} = (\mathfrak{A}, \beta) \vDash \Phi$, $\mathfrak{A} = (A, \ldots)$ with a* countable *underlying set A.*

Considering the countable theories ZF or ZFC yields:

Theorem 197. (The Skolem paradoxon) *Assume that* ZF *or* ZFC *are consistent. Then there exists a countable model of* ZF *or* ZFC *respectively.*

This is considered a *paradox* since the theories ZF and ZFC imply the existence of very high cardinals $\aleph_\alpha$. Nevertheless such high cardinalities can be realized inside a model, that from the "outside" is countable. Some mathematicians have critisized the theories ZF and ZFC because they do not uniquely determine "the" intuitive model of set theory which should be a proper class and not countable.

The word "downward" emphasises the existence of models of "small" cardinality. We now consider an "upward" LÖWENHEIM-SKOLEM theorem.

Theorem 198. (Upward LÖWENHEIM-SKOLEM theorem) *Let $\Phi \subseteq L^S$ have an infinite S-model. Then Φ has a model of cardinality κ for every cardinal $\kappa \geqslant \operatorname{card}(L^S)$.*

Proof. Let $\mathfrak{M}$ be an infinite model of Φ. Choose a sequence $(c_\alpha \,|\, \alpha < \kappa)$ of pairwise distinct constant symbols which do not occur in S. Let $S' = S \cup \{c_\alpha \,|\, \alpha < \kappa\}$ be the extension of S by the new constant symbols. Set

$$\Phi' = \Phi \cup \{\neg c_\alpha \equiv c_\beta \,|\, \alpha < \beta < \kappa\}.$$

(1) Φ' has a model.
Proof. It suffices to show that every finite $\Phi_0 \subseteq \Phi'$ has a model. Let $\Phi_0 \subseteq \Phi'$ be finite. Take a finite set $X_0 \subseteq \kappa$ such that

$$\Phi_0 \subseteq \Phi \cup \{\neg c_\alpha \equiv c_\beta \,|\, \alpha, \beta \in X_0, \alpha < \beta\}.$$

Since $|\mathfrak{M}|$ is infinite we can choose an injective sequence $(a_\alpha|\alpha\in X_0)$ of elements of $|\mathfrak{M}|$ such that $\alpha\neq\beta$ implies $a_\alpha\neq a_\beta$. For $\alpha\in\kappa\setminus X_0$ choose $a_\alpha\in|\mathfrak{M}|$ arbitrarily. Then in the extended model obtained,

$$\mathfrak{M}'\vDash\Phi_0.$$

qed(1)

$$\mathrm{card}(L^{S'})=\mathrm{card}(S')+\aleph_0=\mathrm{card}(S)+\kappa+\aleph_0=\kappa.$$

Let $\mathfrak{M}'\vDash\Phi'$ with $\mathrm{card}(\mathfrak{M}')\leqslant\mathrm{card}(L^{S'})=\kappa$. The map

$$i\colon\kappa\to|\mathfrak{M}'|,\alpha\mapsto c_\alpha^{\mathfrak{M}'}$$

is injective. Thus $\mathrm{card}(\mathfrak{M}')\geqslant\kappa$.

Let $\mathfrak{M}''$ be the reduct of $\mathfrak{M}'$ to the language S. Then $\mathfrak{M}''\vDash\Phi$ and $\mathrm{card}(\mathfrak{M}'')=\kappa$. □

Theorem 199. *Assume that $\Phi\subseteq L^S$ has arbitrarily large finite models. Then Φ has an infinite model.*

Proof. For $n\in\mathbb{N}$ define the sentence

$$\varphi_{\geqslant n}=\exists v_0,\ldots,v_{n-1}\bigwedge_{i<j<n}\neg v_i\equiv v_j,$$

where the big conjunction is defined by

$$\bigwedge_{i<j<n}\psi_{ij}=\psi_{0,1}\wedge\ldots\wedge\psi_{0,n-1}\wedge\psi_{1,2}\wedge\ldots\wedge\psi_{1,n-1}\wedge\ldots\wedge\psi_{n-1,n-1}.$$

For any model $\mathfrak{M}$

$$\mathfrak{M}\vDash\varphi_{\geqslant n}\ \text{ iff }\ A\text{ has at least }n\text{ elements.}$$

Now set

$$\Phi'=\Phi\cup\{\varphi_{\geqslant n}|n\in\mathbb{N}\}.$$

(1) Φ' has a model.
Proof. By the compactness theorem 63b it suffices to show that every finite $\Phi_0\subseteq\Phi$ has a model. Let $\Phi_0\subseteq\Phi$ be finite. Take $n_0\in\mathbb{N}$ such that

$$\Phi_0\subseteq\Phi\cup\{\varphi_{\geqslant n}|n\leqslant n_0\}.$$

By assumption Φ has a model with at least n_0 elements. Thus $\Phi\cup\{\varphi_{\geqslant n}|n\leqslant n_0\}$ and Φ_0 have a model. *qed*(1)

Let $\mathfrak{M}\vDash\Phi'$. Then $\mathfrak{M}$ is an infinite model of Φ. □

Theorem 200. *Let S be a language.*

a) The class of all finite S-structures is not axiomatizable.

b) The class of all infinite S-structures is axiomatizable but not finitely axiomatizable.

Proof. a) is immediate by Theorem 199.
b) The class of infinite S-structures is axiomatized by

$$\Phi=\{\varphi_{\geqslant n}|n\in\mathbb{N}\}.$$

If that class were *finitely* axiomatizable then the complementary class of finite S-structures would also be (finitely) axiomatizable, contradicting a). □