Mathematical Logic. An Introduction

Summer 2014

by Peter Koepke

1 Introduction

Mathematics models real world phenomena like space, time, number, probability, games, etc. It proceeds from initial assumptions to conclusions by rigorous arguments. Its results are "universal" and "logically valid", in that they do not depend on external or implicit conditions which may change with time, nature or society.

It is remarkable that mathematics is also able to *model itself*: mathematical logic defines rigorously what mathematical statements and rigorous arguments are. The mathematical enquiry into the mathematical method leads to deep insights into mathematics, applications to classical field 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.

1.1 A simple proof

We want to indicate that rigorous mathematical proofs can be generated by applying simple text manipulations to mathematical statements. Let us consider a fragment of the elementary theory of functions which expresses that the composition of two surjective maps is surjective as well:

> Let f and g be *surjective*, i.e., for all y there is x such that $y = f(x)$, and for all y there is x such that $y = g(x)$.
> *Theorem.* $g \circ f$ is surjective, i.e., for all y there is x such that $y = g(f(x))$.
> *Proof.* Consider any y. Choose z such that $y = g(z)$. Choose x such that $z = f(x)$. Then $y = g(f(x))$. Thus there is x such that $y = g(f(x))$. Thus for all y there is x such that $y = g(f(x))$.
> *Qed.*

These statements and arguments are expressed in an austere and systematic language, which can be normalized further. Logical symbols like $\forall$ and $\exists$ abbreviate figures of language like "for all" or "there exists":

> Let $\forall y \exists x\, y = f(x)$.
> Let $\forall y \exists x\, y = g(x)$.
> Theorem. $\forall y \exists x\, y = g(f(x))$.
> Proof. Consider y.
> $\exists x\, y = g(x)$.
> Let $y = g(z)$.
> $\exists x\, z = f(x)$.
> Let $z = f(x)$.
> $y = g(f(x))$.
> Thus $\exists x\, y = g(f(x))$.
> Thus $\exists x\, y = g(f(x))$.
> Thus $\forall y \exists x\, y = g(f(x))$.
> Qed.

These lines can be considered as formal sequences of symbols. Certain sequences of symbols are acceptable as mathematical formulas. There are rules for the formation of formulas which are acceptable in a proof. These rules have a purely formal character and they can be applied irrespectively of the "meaning" of the symbols and formulas.

1.2 Formal proofs

In the example, $\exists x\, y = g(f(x))$ is inferred from $y = g(f(x))$. The rule of *existential quantification*: "put $\exists x$ in front of a formula" can usually be applied. It has the character of a left-multiplication by $\exists x$.

$$\exists x\,, \varphi \mapsto \exists x\, \varphi.$$

Logical rules satisfy certain algebraic laws like associativity. Another interesting operation is *substitution*: From $y = g(z)$ and $z = f(x)$ infer $y = g(f(x))$ by a "find-and-replace"-substitution of z by $f(x)$.

Given a sufficient collection of rules, the above sequence of formulas, involving "keywords" like "let" and "thus" is a *deduction* or *derivation* in which every line is generated from earlier ones by syntactical rules. Mathematical results may be provable simply by the application of formal rules. In analogy with the formal rules of the infinitesimal calculus one calls a system of rules a *calculus*.

1.3 Syntax and semantics

Obviously we do not just want to describe a formal derivation as a kind of domino but we want to *interpret* the occuring symbols as mathematical objects. Thus we let variables x, y, ... range over some domain like the real numbers $\mathbb{R}$ and let f and g stand for functions $F, G\colon \mathbb{R} \to \mathbb{R}$. Observe that the symbol or "name" f is not identical to the function F, and indeed f might also be interpretated as another function F'. To emphasize the distinction between names and objects, we classify symbols, formulas and derivations as *syntax* whereas the interpretations of symbols belong to the realm of *semantics*.

By interpreting x, y, ... and f, g, ... in a structure like $(\mathbb{R}, F, G)$ we can define straightforwardly whether a formula like $\exists x\, g(f(x))$ is *satisfied* in the structure. A formula is *logically valid* if it is satisfied under *all* interpretations. The fundamental theorem of mathematical logic and the central result of this course is GÖDEL's completeness theorem:

Theorem. *There is a calculus with finitely many rules such that a formula is derivable in the calculus iff it is logically valid.*

1.4 Set theory

In modern mathematics notions can usually be reduced to set theory: non-negative integers correspond to cardinalities of finite sets, integers can be obtained via pairs of non-negative integers, rational numbers via pairs of integers, and real numbers via subsets of the rationals, etc. Geometric notions can be defined from real numbers using analytic geometry: a point is a pair of real numbers, a line is a set of points, etc. It is remarkable that the basic set theoretical axioms can be formulated in the logical language indicated above. So mathematics may be understood abstractly as

$$\text{Mathematics} = \text{(first-order) logic} + \text{set theory}.$$

Note that we only propose this as a reasonable abstract viewpoint corresponding to the logical analysis of mathematics. This perspective leaves out many important aspects like the applicability, intuitiveness and beauty of mathematics.

1.5 Circularity

We shall use *sets* as symbols which can then be used to formulate the axioms of *set* theory. We shall *prove* theorems about *proofs*. This kind of circularity seems to be unavoidable in comprehensive foundational science: linguistics has to *talk* about *language*, *brain research* has to be carried out by brains. Circularity can lead to paradoxes like the liar's paradox: "I am a liar", or "this sentence is false". Circularity poses many problems and seems to undermine the value of foundational theories. We suggest that the reader takes a *naive* standpoint in these matters: there are sets and proofs which are just as obvious as natural numbers. Then theories are formed which abstractly describe the naive objects.

A closer analysis of circularity in logic leads to the famous *incompleteness theorems* of Gödel's:

Theorem. *Formal theories which are strong enough to "formalize themselves" are not complete, i.e., there are statements such that neither it nor its negation can be proved in that theory. Moreover such theories cannot prove their own consistency.*

It is no surprise that these results, besides their initial mathematical meaning had a tremendous impact on the theory of knowledge outside mathematics, e.g., in philosophy, psychology, linguistics.

2 Set theoretic preliminaries

To model the mathematical method, we have to formalize mathematical language and general structures by mathematical objects. The most basic mathematical objects seem to be *sets*. We briefly present some facts from set theory which are used in the sequel.

In line with our introductory remarks on circularity we initially treat set theory *naively*, i.e., we view sets and set theoretic operations as concrete mental constructs. We shall later introduce a powerful axiom system for sets. From an axiomatic standpoint most of our arguments can be carried out under weak set theoretical hypotheses. In particular it will not be necessary to use sets of high cardinality.

The theory of *finite* sets is based on the *empty set* $\emptyset = \{\}$ and operations like

$$x \mapsto \{x\};\ x, y \mapsto \{x, y\};\ x, y \mapsto x \cup y;\ x, y \mapsto x \cap y;\ x, y \mapsto x \setminus y\,.$$

The operation $x,\ y \mapsto \{\{x\}, \{x,\ y\}\}$ defines the *ordered pair* of x and y. Its crucial property is that

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} \text{ if and only if } x = x' \text{ and } y = y'.$$

The ordered pair $\{\{x\}, \{x,\ y\}\}$ is denoted by $(x,\ y)$. Ordered pairs allow to formalize (binary) relations and functions:

- a *relation* is a set R of ordered pairs;
- a *function* is a relation f such that for all x, y, y' holds: if $(x, y) \in f$ and $(x, y') \in f$ then $y = y'$. Then $f(x)$ denotes the unique y such that $(x, y) \in f$.

We assume standard notions and notations from relation theory, see also Definition 2 below. For binary relations R we can use the *infix* notation $a\,R\,b$ instead of $(a, b) \in R$.

If a function maps the elements of a set a into a set b we write

$$f\colon a \to b\,.$$

In case we do not want to specify the target set b, we can also write $f\colon a \to V$ where V is understood to be the *universe* of all sets. We assume the usual notions of function theory like *injective*, *surjective*, *bijective*, etc.

It is natural to formalize the integer n by some set with n elements. We shall later see that the following formalization can be carried out uniformly in set theory:

$$\begin{aligned}
0 &= \emptyset \\
1 &= \{0\} \\
2 &= \{0, 1\} \\
&\vdots \\
n+1 &= \{0, 1, ..., n\} = \{0, 1, ..., n-1\} \cup \{n\} = n \cup \{n\} \\
&\vdots \\
\mathbb{N} = \omega &= \{0, 1, ...\}
\end{aligned}$$

These integers satisfy the usual laws of complete induction and recursion.

A *finite sequence* is a function $w\colon n \to V$ for some integer $n \in \mathbb{N}$ which is the *length* of w. We write w_i instead of $w(i)$, and the sequence w may also be denoted by $w_0 \ldots w_{n-1}$. Note that the empty set $\emptyset$ is the unique finite sequence of length 0.

For finite sequences $w = w_0 \ldots w_{m-1}$ and $w' = w'_0 \ldots w'_{n-1}$ let $w \hat{} w' = w_0 \ldots w_{m-1} w'_0 \ldots w'_{n-1}$ be the *concatenation* of w and w'. $w \hat{} w' \colon m+n \to V$ can be defined by

$$w \hat{} w'(i) = \begin{cases} w(i), \text{ if } i < m; \\ w'(i-m), \text{ if } i \geqslant m. \end{cases}$$

We also write ww' for $w \hat{} w'$. This operation is a *monoid* satisfying some cancellation rules:

Proposition 1. *Let w, w', w'' be finite sequences. Then*

a) $(w \hat{} w') \hat{} w'' = w \hat{} (w' \hat{} w'')$.

b) $\emptyset \hat{} w = w \hat{} \emptyset = w$.

c) $w \hat{} w' = w \hat{} w'' \to w' = w''$.

d) $w' \hat{} w = w'' \hat{} w \to w' = w''$.

Proof. We only check the associative law a). Let $n, n', n'' \in \mathbb{N}$ such that $w = w_0 \ldots w_{n-1}$, $w' = w'_0 \ldots w'_{n'-1}$, $w'' = w''_0 \ldots w''_{n''-1}$. Then

$$\begin{aligned} (w \hat{} w') \hat{} w'' &= (w_0 \ldots w_{n-1} w'_0 \ldots w'_{n'-1}) \hat{} w''_0 \ldots w''_{n''-1} \\ &= w_0 \ldots w_{n-1} w'_0 \ldots w'_{n'-1} w''_0 \ldots w''_{n''-1} \\ &= w_0 \ldots w_{n-1} \hat{} (w'_0 \ldots w'_{n'-1} w''_0 \ldots w''_{n''-1}) \\ &= w_0 \ldots w_{n-1} \hat{} (w'_0 \ldots w'_{n'-1} \hat{} w''_0 \ldots w''_{n''-1}) \\ &= w \hat{} (w' \hat{} w''). \end{aligned}$$

The trouble with this argument is the intuitive but vague use of the *ellipses* "...". In mathematical logic we have to ultimately eliminate such vaguenesses. So we show that for all $i < n + n' + n''$

$$((w \hat{} w') \hat{} w'')(i) = (w \hat{} (w' \hat{} w''))(i).$$

Case 1: $i < n$. Then

$$\begin{aligned} ((w \hat{} w') \hat{} w'')(i) &= (w \hat{} w')(i) \\ &= w(i) \\ &= (w \hat{} (w' \hat{} w''))(i). \end{aligned}$$

Case 2: $n \leqslant i < n + n'$. Then

$$\begin{aligned} ((w \hat{} w') \hat{} w'')(i) &= (w \hat{} w')(i) \\ &= w'(i-n) \\ &= (w' \hat{} w'')(i-n) \\ &= (w \hat{} (w' \hat{} w''))(i). \end{aligned}$$

Case 3: $n + n' \leqslant i < n + n' + n''$. Then

$$\begin{aligned} ((w \hat{} w') \hat{} w'')(i) &= w''(i - (n+n')) \\ &= w' \hat{} w''(i - (n+n') + n') = w' \hat{} w''(i-n) \\ &= (w \hat{} (w' \hat{} w''))(i-n+n) \\ &= (w \hat{} (w' \hat{} w''))(i). \end{aligned}$$

□

A set x is *finite*, if there is an integer $n \in \mathbb{N}$ and a surjective function $f\colon n \to x$. The smallest such n is called the *cardinality* of the finite set x and denoted by $n = \mathrm{card}(x)$. The usual cardinality properties for finite sets follow from properties of finite sequences.

A set x is *denumerable* or *countable* if there is a surjective function $f\colon \mathbb{N} \to x$. If the set is not finite, it is *countably infinite*. Its cardinality is ω, written as $\omega = \operatorname{card}(x)$. Under sufficient set theoretical assumptions, the union

$$\bigcup_{n\in\omega} x_n$$

where each x_n is countable is again countable.

If a set x is not countable, it is *uncountable*. Within set theory one can develop an efficient notion of cardinality for uncountable sets.

The theory of infinite sets usually requires the *axiom of choice* which is equivalent to Zorn's lemma.

Definition 2. *Let A be a set and $\leqslant$ be a binary relation. Define*

a) $(A, \leqslant)$ *is* transitive *if for all $a, b, c \in A$*

$$a \leqslant b \text{ and } b \leqslant c \text{ implies } a \leqslant c.$$

b) $(A, \leqslant)$ *is* reflexive *if for all $a \in A$ holds $a \leqslant a$.*

c) $(A, \leqslant)$ *is a* partial order *if $(A, \leqslant)$ is transitive and reflexive and $A \neq \emptyset$.*

So let $(A, \leqslant)$ is be a partial order.

a) $z \in A$ *is a* maximal element *of A if there is no $a \in A$ with $z \leqslant a$ and $z \neq a$.*

b) If $X \subseteq A$ then u is an upper bound *for X if for all $x \in X$ holds $x \leqslant u$.*

c) $I \subseteq A$ *is* linear *if for all $a, b \in I$*

$$a \leqslant b \text{ or } b \leqslant a.$$

d) $(A, \leqslant)$ *is* inductive *if every linear subset of A has an upper bound.*

Zorn*'s lemma* states

Theorem 3. *Every inductive partial order has a maximal element.*

3 Symbols and words

Intuitively and also in our theory a word is a finite sequence of symbols. A symbol has some basic information about its role within words. E.g., the symbol $\leqslant$ is usually used to stand for a binary relation. So we let symbols include such type information. We provide us with a sufficient collection of symbols.

Definition 4. *The* basic symbols *of first-order logic are*

a) $\equiv$ *for* equality*,*

b) $\neg, \to, \bot$ *for the logical operations of* negation*,* implication *and the truth value* false*,*

c) $\forall$ *for* universal quantification*,*

d) (*and*) *for auxiliary* bracketing.

e) variables v_n for $n \in \mathbb{N}$.

Let $\mathrm{Var} = \{v_n | n \in \mathbb{N}\}$ *be the set of variables and let S_0 be the set of basic symbols.*

An n-ary relation symbol*, for $n \in \mathbb{N}$, is (a set) of the form $R = (x, 0, n)$; here* 0 *indicates that the values of a relation will be* truth values*.* 0*-ary relation symbols are also called* propositional constant symbols*. An n-ary* function symbol*, for $n \in \mathbb{N}$, is (a set) of the form $f = (x, 1, n)$ where* 1 *indicates that the values of a function will be elements of a structure.* 0*-ary function symbols are also called* constant symbols*.*

A symbol set *or a* language *is a set of relation symbols and function symbols.*

We assume that the basic symbols are pairwise distinct and are distinct from any relation or function symbol. For concreteness one could for example set $\equiv$*=0,* $\neg$*=1,* $\to$*=2,* $\bot = 3$*,* (*=4,*) *=* 5*, and $v_n = (1, n)$ for $n \in \mathbb{N}$.*

An n-ary relation symbol is intended to denote an n-ary relation; an n-ary function symbol is intended to denote an n-ary function. A symbol set is sometimes called a *type* because it describes the type of structures which will later interpret the symbols. We shall denote variables by letters like x, y, z, ..., relation symbols by P, Q, R, ..., functions symbols by f, g, h, ... and constant symbols by $c, c_0, c_1, \ldots$ We shall also use other typographical symbols in line with standard mathematical practice. A symbol like $<$, e.g., usually denotes a binary relation, and we could assume for definiteness that there is some fixed set theoretic formalization of $<$ like $<=$ $(999, 0, 2)$. Instead of the arbitrary 999 one could also take the number of $<$ in some typographical font.

Example 5. The *language of group theory* is the language

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

where $\circ$ is a binary ($=$ 2-ary) function symbol and e is a constant symbol. Again one could be definite about the coding of symbols and set $S_{\mathrm{Gr}} = \{(80, 1, 2), (87, 1, 0)\}$, e.g., but we shall not care much about such details. As usual in algebra, one also uses an *extended language of group theory*

$$S_{\mathrm{Gr}} = \{\circ, ^{-1}, e\}$$

to describe groups, where $^{-1}$ is a unary ($=$ 1-ary) function symbol.

Definition 6. *Let S be a language. A* word *over S is a finite sequence*

$$w\colon n \to S_0 \cup S\,.$$

Let S^* be the set of all words over S. The empty set $\emptyset$ is also called the empty word.

Let S be a symbol set. We want to formalize how a word like $\exists x\, y = g(f(x))$ can be produced from a word like $y = g(f(x))$.

Definition 7. *A relation $R \subseteq (S^*)^n \times S^*$ is called a* rule *(over S). A* calculus *(over S) is a set $\mathcal{C}$ of rules (over S).*

We work with rules which *produce* words out of given words. A rule

$$\{(\text{arguments, production})|\ldots\}$$

is usually written as a *production rule* of the form

$$\frac{\text{arguments}}{\text{production}} \quad \text{or} \quad \frac{\text{preconditions}}{\text{conclusion}}\,.$$

For the existential quantification mentioned in the introduction we may for example write

$$\frac{\varphi}{\exists x\, \varphi}$$

where the production is the concatenation of $\exists x$ and φ.

Definition 8. *Let $\mathcal{C}$ be a calculus over S. Let $R \subseteq (S^*)^n \times S^*$ be a rule of $\mathcal{C}$. For $X \subseteq S^*$ set*

$$R[X] = \{w \in S^* \mid \textit{there are words } u_0, \ldots, u_{n-1} \in X \textit{ such that } R(u_0, \ldots, u_{n-1}, w) \textit{ holds}\}.$$

Then the product *of $\mathcal{C}$ is the smallest subset of S^* closed under the rules of $\mathcal{C}$:*

$$\mathrm{Prod}(\mathcal{C}) = \bigcap \{X \subseteq S^* \mid \textit{for all rules } R \in \mathcal{C} \textit{ holds } R[X] \subseteq X\}.$$

The product of a calculus can also be described "from below" by:

Definition 9. *Let $\mathcal{C}$ be a calculus over S. A sequence $w^{(0)}, \ldots, w^{(k-1)} \in S^*$ is called a* derivation *in $\mathcal{C}$ if for every $l < k$ there exists a rule $R \in \mathcal{C}$, $R \subseteq (S^*)^n \times S^*$ and $l_0, \ldots, l_{n-1} < l$ such that*

$$R(w^{(l_0)}, \ldots, w^{(l_{n-1})}, w^{(l)}).$$

This means that every word of the derivation can be derived from earlier words of the derivation by application of one of the rules of the calculus. We shall later define a calculus such that the sequence of sentences

Let $\forall y \exists x\, y = f(x)$.
Let $\forall y \exists x\, y = g(x)$.
Consider y.
$\exists x\, y = g(x)$.
Let $y = g(z)$.
$\exists x\, z = f(x)$.
Let $z = f(x)$.
$y = g(f(x))$.
Thus $\exists x\, y = g(f(x))$.
Thus $\exists x\, y = g(f(x))$.
Thus $\forall y \exists x\, y = g(f(x))$.
Qed.

is basically a derivation in that calculus.

Everything in the product of a calculus can be obtained by a derivation.

Proposition 10. *Let $\mathcal{C}$ be a calculus over S. Then*

$$\mathrm{Prod}(\mathcal{C}) = \{w \,|\, \textit{there is a derivation } w^{(0)}, ..., w^{(k-1)} = w \textit{ in } \mathcal{C}\}.$$

Proof. The equality of sets can be proved by two inclusions.
($\subseteq$) The set

$$X = \{w \,|\, \text{there is a derivation } w^{(0)}, ..., w^{(k-1)} = w \text{ in } \mathcal{C}\}$$

satisfies the closure property $R[X] \subseteq X$ for all rules $R \in \mathcal{C}$. Since $\mathrm{Prod}(\mathcal{C})$ is the intersection of all such sets, $\mathrm{Prod}(\mathcal{C}) \subseteq X$.
($\supseteq$) Consider $w \in X$. Consider a derivation $w^{(0)}, ..., w^{(k-1)} = w$ in $\mathcal{C}$. We show by induction on $l < k$ that $w^{(l)} \in \mathrm{Prod}(\mathcal{C})$. Let $l < k$ and assume that for all $i < l$ holds $w^{(i)} \in \mathrm{Prod}(\mathcal{C})$. Take a rule $R \in \mathcal{C}$, $R \subseteq (\mathbb{A}^*)^n \times \mathbb{A}^*$ and $l_0, ..., l_{n-1} < l$ such that $R(w^{(l_0)}, ..., w^{(l_{n-1})}, w^{(l)})$. Since $\mathrm{Prod}(\mathcal{C})$ is closed under application of R we get $w^{(l)} \in \mathrm{Prod}(\mathcal{C})$. Thus $w = w^{(k-1)} \in \mathrm{Prod}(\mathcal{C})$. □

Exercise 1. (Natural numbers 1) Consider the symbol set $S = \{\,|\,\}$. The set $S^* = \{\emptyset, |, ||, |||, ...\}$ of words may be identified with the set $\mathbb{N}$ of natural numbers. Formulate a calculus $\mathcal{C}$ such that $\mathrm{Prod}(\mathcal{C}) = S^*$.

4 Induction and recursion on calculi

Derivations in a calculus have finite length so that one can carry out inductions and recursions along the lengths of derivations. We formulate appropriate induction and recursion theorems which generalize *complete induction* and *recursion* for natural numbers. Note the recursion is linked to induction but requires stronger hypothesis.

Theorem 11. (Induction Theorem) *Let $\mathcal{C}$ be a calculus over S and let $\varphi(-)$ be a property which is inherited along the rules of $\mathcal{C}$:*

$$\forall R \in \mathcal{C}, R \subseteq (S^*)^k \times S^* \forall w^{(1)}, ..., w^{(k)}, w \in S^*, R(w^{(1)}, ..., w^{(k)}, w)\ (\varphi(w^{(1)}) \wedge ... \wedge \varphi(w^{(k)}) \to \varphi(w)).$$

Then

$$\forall w \in \mathrm{Prod}(\mathcal{C})\ \varphi(w).$$

Proof. By assumption, $\{w \in S^* | \varphi(w)\}$ is closed under the rules of $\mathcal{C}$. Since $\mathrm{Prod}(\mathcal{C})$ is the intersection of all sets which are closed under $\mathcal{C}$,

$$\mathrm{Prod}(\mathcal{C}) \subseteq \{w \in S^* | \varphi(w)\}.$$ □

Definition 12. *A calculus $\mathcal{C}$ over S is* uniquely readable *if for every $w \in \mathrm{Prod}(\mathcal{C})$ there are a unique rule $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ and unique $w^{(1)}, ..., w^{(k)} \in S^*$ such that*

$$R(w^{(1)}, ..., w^{(k)}, w).$$

Theorem 13. (Recursion Theorem) *Let $\mathcal{C}$ be a calculus over S which is uniquely readable and let $(G_R | R \in \mathcal{C})$ be a sequence of* recursion rules*, i.e., for $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ let $G_R \colon V^k \to V$ where V is the universe of all sets. Then there is a uniquely determined function $F \colon \mathrm{Prod}(\mathcal{C}) \to V$ such that the following* recursion equation *is satisfied for all $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ and $w^{(1)}, ..., w^{(k)}, w \in \mathrm{Prod}(\mathcal{C})$, $R(w^{(1)}, ..., w^{(k)}, w)$:*

$$F(w) = G_R(F(w^{(1)}), ..., F(w^{(k)})).$$

We say that F is defined by recursion along $\mathcal{C}$ *by the recursion rules $(G_R | R \in \mathcal{C})$.*

Proof. We define $F(w)$ by complete recursion on the length of the shortest derivation of w in $\mathcal{C}$. Assume that $F(u)$ is already uniquely defined for all $u \in \mathrm{Prod}(\mathcal{C})$ with shorter derivation length. Let w have shortest derivation $w^{(0)}, ..., w^{(l-1)}$. By the unique readability of $\mathcal{C}$ there are $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ and $w^{(i_0)}, ..., w^{(i_{k-1})}$ with $i_0, ..., i_{k-1} < l - 1$ such that

$$R(w^{(i_0)}, ..., w^{(i_{k-1})}, w).$$

Then we can uniquely define

$$F(w) = G_R(F(w^{(i_0)}), ..., F(w^{(i_{k-1})})). \qquad \square$$

Remark 14. The previous Theorem states the existence of a function F as a set of ordered pairs, but the proof argues that F can be defined (by some intuitive "procedure"). To complete the argument one would have to use the recursion theorem from set theory which says that definitions of a certain kind correspond to certain functions in the set theoretic universe.

5 Terms and formulas

Fix a symbol set S for the remainder of this section. We generate the *terms* and *formulas* of the corresponding language L^S by calculi.

Definition 15. *The* term calculus *(for S) consists of the following rules:*

a) $\dfrac{}{x}$ *for all variables x;*

b) $\dfrac{}{c}$ *for all constant symbols $c \in S$;*

c) $\dfrac{t_0 t_1 \dots t_{n-1}}{f t_0 \dots t_{n-1}}$ *for all n-ary function symbols $f \in S$.*

*Let T^S be the product of the term calculus. T^S is the set of all S-*terms*.*

Definition 16. *The* formula calculus *(for S) consists of the following rules:*

a) $\dfrac{}{\bot}$ *produces* falsity*;*

b) $\dfrac{}{t_0 \equiv t_1}$ *for all S-terms $t_0, t_1 \in T^S$ produces* equations*;*

c) $\dfrac{}{R t_0 \dots t_{n-1}}$ *for all n-ary relation symbols $R \in S$ and all S-terms $t_0, ..., t_{n-1} \in T^S$ produces* relational formulas*;*

d) $\dfrac{\varphi}{\neg \varphi}$ *produces* negations *of formulas;*

e) $\dfrac{\varphi \quad \psi}{(\varphi \to \psi)}$ *produces* implications*;*

f) $\dfrac{\varphi}{\forall x \varphi}$ *for all variables x produces* universalizations*.*

Let L^S be the product of the formula calculus. L^S is the set of all S-formulas, and it is also called the first-order language *for the symbol set S. Formulas produced by rules a-c) are called* atomic formulas *since they constitute the initial steps of the formula calculus.*

Example 17. S-terms and S-formulas formalize the naive concept of a "mathematical formula". The standard axioms of *group theory* can be written as in the extended language of group theory as $S_{\mathrm{Gr}'}$-formulas:

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) $\forall v_0 \circ v_0\, {}^{-1} v_0 \equiv e$.

Note that in c) the $^{-1}$-operator is "applied" to the variable v_0 . The term calculus uses the bracket-free *polish notation* which writes operators before the arguments (*prefix* operators). In line with standard notations one also writes operators in *infix* and *postfix* notation, using bracket, to formulate, e.g., associativity:

$$\forall v_0 \forall v_1 \forall v_2\; v_0 \circ (v_1 \circ v_2) \equiv (v_0 \circ v_1) \circ v_2 .$$

Since the particular choice of variables should in general be irrelevant they may be denoted by letters $x, y, z, \ldots$ instead. Thus the group axioms read:

a) $\forall x \forall y \forall z\; x \circ (y \circ z) \equiv (x \circ y) \circ z$;

b) $\forall x\, x \circ e \equiv x$;

c) $\forall x\, x \circ x^{-1} \equiv e$.

Let $\Phi_{\mathrm{Gr}'} = \{\forall x \forall y \forall z\; x \circ (y \circ z) \equiv (x \circ y) \circ z, \forall x\, x \circ e \equiv x, \forall x\, x \circ x^{-1} \equiv e\}$ be the *axioms of group theory* in the extended language.

To work with terms and formulas, it is crucial that the term and formula calculi are uniquely readable. We leave the proof of these facts as exercises.

Although the language introduced will be theoretically sufficient for all mathematical purposes it is often convenient to further extend its expressiveness. We view some additional language constructs as *abbreviations* for formulas in L^S.

Definition 18. *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* $\neg\forall x \neg\varphi$.

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

6 Structures and models

We shall *interpret* formulas like $\forall y \exists x\; y = g(f(x))$ in adequate *structures*. This interaction between language and structures is usually called *semantics*. Fix a symbol set S.

Definition 19. *An S-*structure *is a function $\mathfrak{A}\colon \{\forall\} \cup S \to V$ such that*

a) $\mathfrak{A}(\forall) \neq \emptyset$; $\mathfrak{A}(\forall)$ is the underlying set *of $\mathfrak{A}$ and is usually denoted by A or $|\mathfrak{A}|$;*

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

c) for every n-ary function symbol $f \in S$, $\mathfrak{A}(f)$ is an n-ary function *on A, i.e., $a(r)\colon A^n \to A$.*

Again we use customary or convenient notations for the *components* of the structure $\mathfrak{A}$, i.e., the values of $\mathfrak{A}$. One often writes $R^{\mathfrak{A}}$, $f^{\mathfrak{A}}$, or $c^{\mathfrak{A}}$ instead of $\mathfrak{A}(r)$, $\mathfrak{A}(f)$, or $\mathfrak{A}(c)$ resp. In simple cases, one may simply list the components of the structure and write, e.g.,

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

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

One also 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 one notation is quite common in mathematics (and in natural language). There are methods of "disambiguating" the ambiguities introduced by multiple usage. Another common overloading is given by a naive identification of syntax and semantics, i.e., by writing

$$A = (A, R_0, R_1, f).$$

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

Example 20. Formalize the *ordered field of reals* $\mathbb{R}$ as follows. Define the language of ordered fields

$$S_{\text{oF}} = \{<, +, \cdot, 0, 1\}.$$

Then define the structure $\mathbb{R}\colon \{\forall\} \cup S_{\text{oF}} \to V$ by

$$\begin{aligned}
\mathbb{R}(\forall) &= \mathbb{R} \\
\mathbb{R}(<) = <^{\mathbb{R}} &= \{(u,v) \in \mathbb{R}^2 \,|\, u < v\} \\
\mathbb{R}(+) = +^{\mathbb{R}} &= \{(u,v,w) \in \mathbb{R}^3 \,|\, u + v = w\} \\
\mathbb{R}(\cdot) = \cdot^{\mathbb{R}} &= \{(u,v,w) \in \mathbb{R}^3 \,|\, u \cdot v = w\} \\
\mathbb{R}(0) = 0^{\mathbb{R}} &= 0 \in \mathbb{R} \\
\mathbb{R}(1) = 1^{\mathbb{R}} &= a \in \mathbb{R}
\end{aligned}$$

This defines the standard structure $\mathbb{R} = (\mathbb{R}, <^{\mathbb{R}}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, 0^{\mathbb{R}}, 1^{\mathbb{R}})$.

Observe that the symbols could in principle be interpreted in completely different, counterintuitive ways like

$$\begin{aligned}
\mathbb{R}'(\forall) &= \mathbb{N} \\
\mathbb{R}'(<) &= \{(u,v) \in \mathbb{N}^2 \,|\, u > v\} \\
\mathbb{R}'(+) &= \{(u,v,w) \in \mathbb{N}^3 \,|\, u \cdot v = w\} \\
\mathbb{R}'(\cdot) &= \{(u,v,w) \in \mathbb{N}^3 \,|\, u + v = w\} \\
\mathbb{R}'(0) &= 1 \\
\mathbb{R}'(1) &= 0
\end{aligned}$$

Example 21. Define the language of *Boolean algebras* by

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

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 $B = |\mathbb{B}| = \{0, 1\}$ with $0 = \mathbb{B}(0)$ and $1 = \mathbb{B}(1)$. Define the operations and $= \mathbb{B}(\wedge)$, or $= \mathbb{B}(\vee)$, and not $= \mathbb{B}(-)$ by *operation tables* in analogy to standard multiplication tables:

and	0	1
0	0	0
1	0	1

,

or	0	1
0	0	1
1	1	1

, and

not	
0	1
1	0

.

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

The notion of structure leads to some related definitions.

Definition 22. *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 $S \subseteq S'$ and $\mathfrak{A}' \restriction (\{\forall\} \cup S) = \mathfrak{A}$.*

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

Definition 23. *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 $R \in S$ holds $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$;

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

Definition 24. *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.

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

Definition 25. *Let S be a symbol set. An S-*model *is a function*

$$\mathfrak{M}\colon \{\forall\} \cup S \cup \mathrm{Var} \to V$$

such that $\mathfrak{M} \restriction \{\forall\} \cup S$ is an S-structure and for all $n \in \mathbb{N}$ holds $\mathfrak{M}(v_n) \in |\mathfrak{M}|$. $\mathfrak{M}(v_n)$ is the interpretation of the variable v_n in $\mathfrak{M}$.

It will sometimes be important to modify a model $\mathfrak{M}$ at specific variables. For pairwise distinct variables $x_0, \ldots, x_{r-1}$ and $a_0, \ldots, a_{r-1} \in |\mathfrak{M}|$ define

$$\mathfrak{M}\frac{a_0 \ldots a_{r-1}}{x_0 \ldots x_{r-1}} = (\mathfrak{M} \setminus \{(x_0, \mathfrak{A}(x_0)), \ldots, (x_{r-1}, \mathfrak{A}(x_{r-1}))\}) \cup \{(x_0, a_0), \ldots, (x_{r-1}, a_{r-1})\}.$$

7 The satisfaction relation

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

Definition 26. *Let $\mathfrak{M}$ be an S-model. Define the* interpretation *$\mathfrak{M}(t) \in |\mathfrak{M}|$ of a term $t \in T^S$ by recursion on the term calculus:*

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

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

$$\mathfrak{M}(ft_0...t_{n-1}) = f^{\mathfrak{A}}(\mathfrak{M}(t_0), ..., \mathfrak{M}(t_{n-1})).$$

This explains the interpretation of a term like $v_3^2 + v_{200}^3$ in the reals.

Definition 27. *Let* $\mathfrak{M}$ *be an S-model. Define the* interpretation $\mathfrak{M}(\varphi) \in \mathbb{B}$ *of a formula* $\varphi \in L^S$, *where* $\mathbb{B} = \{0, 1\}$ *is the Boolean algebra of truth values, by recursion on the formula calculus:*

a) $\mathfrak{M}(\bot) = 0$;

b) for terms $t_0, t_1 \in T^S$: $\mathfrak{M}(t_0 \equiv t_1) = 1$ *iff* $\mathfrak{M}(t_0) = \mathfrak{M}(t_1)$;

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

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

d) $\mathfrak{M}(\neg\varphi) = 1$ *iff* $\mathfrak{M}(\varphi) = 0$;

e) $\mathfrak{M}(\varphi \to \psi) = 1$ *iff* $\mathfrak{M}(\varphi) = 1$ *implies* $\mathfrak{M}(\psi) = 1$;

f) $\mathfrak{M}(\forall v_n \varphi) = 1$ *iff for all* $a \in |\mathfrak{M}|$ *holds* $\mathfrak{M}\frac{a}{v_n}(\varphi) = 1$.

We write $\mathfrak{M} \vDash \varphi$ *instead of* $\mathfrak{M}(\varphi) = 1$. *We also say that* $\mathfrak{M}$ satisfies φ *or that* φ holds *in* $\mathfrak{M}$. *For* $\Phi \subseteq L^S$ *write* $\mathfrak{M} \vDash \Phi$ *iff* $\mathfrak{M} \vDash \varphi$ *for every* $\varphi \in \Phi$.

Definition 28. *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 extensions by the symbols $\vee, \wedge, \leftrightarrow, \exists$ is consistent with the expected meanings of the additional symbols:

Exercise 2. Prove:

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

b) $\mathfrak{M} \vDash (\varphi \vee \psi)$ 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 29. *For* $t \in T^S$ *define* $\mathrm{var}(t) \subseteq \{v_n | n \in \mathbb{N}\}$ *by recursion on the term calculus:*

- $\mathrm{var}(x) = \{x\}$;
- $\mathrm{var}(c) = \emptyset$;
- $\mathrm{var}(ft_0...t_{n-1}) = \bigcup_{i<n} \mathrm{var}(t_i)$.

Definition 30. *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 formula calculus:*

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

For $\Phi \subseteq L^S$ *define the set* $\mathrm{free}(\Phi)$ *of* free variables *as*

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

Example 31.

$$\begin{aligned}\text{free}(Ryx \to \forall y \neg y = z) &= \text{free}(Ryx) \cup \text{free}(\forall y \neg y = z)\\ &= \text{free}(Ryx) \cup (\text{free}(\neg y = z) \setminus \{y\})\\ &= \text{free}(Ryx) \cup (\text{free}(y = z) \setminus \{y\})\\ &= \{y, x\} \cup (\{y, z\} \setminus \{y\})\\ &= \{y, x\} \cup \{z\}\\ &= \{x, y, z\}.\end{aligned}$$

Definition 32.

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

b) $\varphi \in L^S$ *is an* S-sentence *if* $\text{free}(\varphi) = \emptyset$*;* L^S_0 *is the set of* S*-sentences.*

Theorem 33. *Let* t *be an* S*-term and let* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *be* S*-models with the same structure* $\mathfrak{M} \restriction \{\forall\} \cup S = \mathfrak{M}' \restriction \{\forall\} \cup S$ *and* $\mathfrak{M} \restriction \text{var}(t) = \mathfrak{M}' \restriction \text{var}(t)$*. Then* $\mathfrak{M}(t) = \mathfrak{M}'(t)$.

Theorem 34. *Let* t *be an* S*-term and let* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *be* S*-models with the same structure* $\mathfrak{M} \restriction \{\forall\} \cup S = \mathfrak{M}' \restriction \{\forall\} \cup S$ *and* $\mathfrak{M} \restriction \text{free}(t) = \mathfrak{M}' \restriction \text{free}(t)$*. Then*

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

Proof. By induction on the formula calculus.
$\varphi = t_0 \equiv t_1$: Then $\text{var}(t_0) \cup \text{var}(t_1) = \text{free}(\varphi)$ and

$$\begin{aligned}\mathfrak{M} \vDash \varphi \;\text{ iff }\; & \mathfrak{M}(t_0) = \mathfrak{M}(t_1)\\ \text{iff }\; & \mathfrak{M}'(t_0) = \mathfrak{M}'(t_1) \text{ by the previous Theorem,}\\ \text{iff }\; & \mathfrak{M}' \vDash \varphi.\end{aligned}$$

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

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

$\varphi = \forall v_n \psi$ and assume the claim to be true for ψ. Then $\text{free}(\psi) \subseteq \text{free}(\varphi) \cup \{v_n\}$. For all $a \in A = |\mathfrak{M}|$: $\mathfrak{M}\frac{a}{v_n} \restriction \text{free}(\psi) = \mathfrak{M}'\frac{a}{v_n} \restriction \text{free}(\psi)$ and so

$$\begin{aligned}\mathfrak{M} \vDash \varphi \;\text{ iff }\; & \text{for all } a \in A \text{ holds } \mathfrak{M}\frac{a}{v_n} \vDash \psi\\ \text{iff }\; & \text{for all } a \in A \text{ holds } \mathfrak{M}'\frac{a}{v_n} \vDash \psi \text{ by the inductive assumption,}\\ \text{iff }\; & \mathfrak{M}' \vDash \varphi.\end{aligned}$$

□

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

Definition 35. *Let* $\mathfrak{A}$ *be an* S*-structure and let* $(a_0, ..., a_{n-1})$ *be a sequence of elements of* A*. Let* t *be an* S*-term with* $\text{var}(t) \subseteq \{v_0, ..., v_{n-1}\}$*. Then define*

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

where $\mathfrak{M} \supseteq \mathfrak{A}$ *is an* S*-model with* $\mathfrak{M}(v_0) = a_0, ..., \mathfrak{M}(v_{n-1}) = a_{n-1}$.
Let φ *be an* S*-formula with* $\text{free}(t) \subseteq \{v_0, ..., v_{n-1}\}$*. Then define*

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

where $\mathfrak{M} \supseteq \mathfrak{A}$ *is an* S*-model with* $\mathfrak{M}(v_0) = a_0, ..., \mathfrak{M}(v_{n-1}) = a_{n-1}$.

In case $n = 0$ *also write* $t^{\mathfrak{A}}$ *instead of* $t^{\mathfrak{A}}[a_0, ..., a_{n-1}]$ *and* $\mathfrak{A} \vDash \varphi$ *instead of* $\mathfrak{A} \vDash \varphi[a_0, ..., a_{n-1}]$.
In this 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 set of sentences also write

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

Example 36. *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 define the axiom set

$$\Phi_{\mathrm{Gr}} = \{\forall v_0 \forall v_1 \forall v_2 \circ v_0 \circ v_1 v_2 \equiv \circ\circ v_0 v_1 v_2,\ \forall v_0 \circ v_0 e \equiv v_0,\ \forall v_0 \exists v_1 \circ v_0 v_1 \equiv e\}.$$

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

Definition 37. *Let S be a language and let $\Phi \subseteq L_0^S$ be a set of S-sentences. Then*

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

is the model class *of Φ. In case $\Phi = \{\Phi\}$ 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 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? Can we extend $\mathrm{Mod}^S\Phi$ by adequate morphisms between models?

8 Logical implication and propositional connectives

Definition 38. *For a symbol set 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 using the semantic notion of interpretation. We show that $\vDash$ satisfies certain syntactical laws. These laws correspond to the rules of a logical proof calculus.

Theorem 39. *Let S be a symbol set, $t \in T^S$, $\varphi, \psi \in L^S$, 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) ($\to$-Introduction) If $\Gamma \cup \varphi \vDash \psi$ then $\Gamma \vDash \varphi \to \psi$.

d) ($\to$-Elimination) If $\Gamma \vDash \varphi$ and $\Gamma \vDash \varphi \to \psi$ 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 $\Gamma \vDash \varphi$. □

9 Substitution and quantification rules

To prove further rules for equalities and quantification, we first have to formalize *substitution*.

Definition 40. *For a term $s \in T^S$, pairwise distinct variables x_0, ..., x_{r-1} and terms t_0, ..., $t_{r-1} \in T^S$ 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) $c\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = c$ *for all constant symbols c;*

c) $(f s_0 \ldots s_{n-1})\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = f s_0\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \ldots s_{n-1}\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ *for all n-ary function symbols f.*

Note that the simultaneous substitution

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

is in general different from a succesive substitution

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

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 $x\,\frac{y}{y}\,\frac{y}{x} = x\,\frac{y}{x} = y$.

Definition 41. *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

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

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

a) $(s_0 \equiv s_1)\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = s_0\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \equiv s_1\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ *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 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 $(\forall x \varphi)\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ *distinguish two cases:*

- *if $x \in \{x_0, \ldots, x_{r-1}\}$, assume that $x = x_0$. Choose $i \in \mathbb{N}$ minimal such that $u = v_i$ does not occur in $\forall x \varphi$, $t_0, \ldots, t_{r-1}$ and $x_0, \ldots, x_{r-1}$. Then set*

$$(\forall x \varphi)\,\frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = \forall u\,(\varphi\,\frac{t_1 \ldots t_{r-1}\,u}{x_1 \ldots x_{r-1}\,x}).$$

- *if $x \notin \{x_0, \ldots, x_{r-1}\}$, choose $i \in \mathbb{N}$ minimal such that $u = v_i$ does not occur in $\forall x \varphi$, $t_0, \ldots, t_{r-1}$ and $x_0, \ldots, x_{r-1}$ and set*

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

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

Theorem 42. *Consider an S-model $\mathfrak{M}$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$.*

a) If $s \in T^S$ is a term,

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

b) If $\varphi \in L^S$ is a formula,

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

Proof. By induction on the complexities of s and φ.
a) *Case 1*: $s = x$.
Case 1.1: $x \notin \{x_0, \ldots, x_{r-1}\}$. Then

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

Case 1.2: $x = x_i$. Then

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

Case 2: $s = c$ is a constant symbol. Then

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

Case 3: $s = f s_0 \ldots s_{n-1}$ where $f \in S$ is an n-ary function symbol and the terms $s_0, \ldots, s_{n-1} \in T^S$ satisfy the theorem. Then

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

□