

Notes on propositional logic and first order logic

M. Viale

Contents

1	Propositional logic	3
1.1	Semantics	3
1.2	Disjunctive normal forms	8
1.3	Proof systems	9
1.4	The sequent calculus LK	9
1.5	Exercises on propositional logic and LK -calculus	22
2	Basics of first order logic	23
2.1	Examples of first order languages	24
2.2	Syntax and semantics for arbitrary first order languages	31
2.3	Free and bounded variables and substitution of symbols inside formulae: what are the problems to match?	36
2.4	Syntactic complexity of terms and formulae	39
2.5	Free and bounded variables of a formula	40
2.6	Basic rules for logic equivalence and prenex normal forms of formulae	45
2.7	Substitution of terms inside formulae	48
2.8	Geometric interpretation of formulae	49
2.9	Definable sets with and without parameters	52
2.10	Exercises on first order logic	54
3	More on first order logic	55
3.1	First order LK -calculus	55
3.2	Satisfiable theories and compactness	57
3.3	Classes of \mathcal{L} -structures	59
3.4	Substructures, morphisms, and products	60
3.5	Elementary equivalence and completeness	68
3.6	More exercises on first order logic	69
4	Compactness	69
4.1	Proof of the compactness theorem	69
5	First order logic and set theory	79

WARNING: These notes are a compendium to Alessandro Andretta's textbook [1] meant as a complement to [1, Chapter I.3]. In particular sections 2 and 3 of these notes consists of the material covered in [1, Chapter I.3] and our presentation draws heavily from it. We invite the reader to look at [1, Chapter I.3] as a further source of reference for our treatment of the basics of first order logic.

1 Propositional logic

Propositional logic formalizes in a mathematically rigorous theory certain concepts and procedures which rule our way to reason about mathematics. For example by means of propositional logic we can give a mathematically precise counterpart of the concepts of theorem, mathematical truth, contradiction, logical deduction, equivalence of meaning between two different linguistic expressions, etc.... Nonetheless propositional logic is still a theory too weak to develop a mathematical theory which reflects *all kind of* mathematical reasoning. This can be accomplished to a really satisfactory extent by means of first order logic, whose basic properties will be introduced in the second part of these notes. We believe that a short introduction to propositional logic can help to understand the key ideas which leads to develop a rigorous and effective mathematical theory of mathematical reasoning.

Definition 1.1. Given an infinite list of propositional variables $\text{PropVar} = \{A_i : i \in \mathbb{N}\}$, a propositional formula is defined by induction using the following clauses out of propositional variables and connectives $\{\neg, \wedge, \vee, \rightarrow\}$:

- each propositional variable A_i is a formula,
- if ϕ is a formula $(\neg\phi)$ is a formula,
- if ϕ, ψ are formulae, also $(\phi \wedge \psi), (\phi \vee \psi), (\phi \rightarrow \psi)$ are formulae.

We let Form be the set of propositional formulae.

Given a formula ϕ the set of its propositional variables $\text{propvar}(\phi)$ is given by the propositional letters occurring in ϕ .

1.1 Semantics

We assign truth values to propositional formulae according to the following definition:

Definition 1.2. Let $v : \text{PropVar} \rightarrow \{0, 1\}$. We extend v to a unique map $v : \text{Form} \rightarrow \{0, 1\}$ satisfying:

- $v((\neg\phi)) = 1 - v(\phi)$,
- $v((\phi \wedge \psi)) = v(\phi) \cdot v(\psi)$,
- $v((\phi \vee \psi)) = \max\{v(\phi), v(\psi)\}$,
- $v((\phi \rightarrow \psi)) = v(\neg\phi \vee \psi)$.

The intended meaning of the above definition being: we regard 1 as a truth and 0 as a falsity. We are interested to study only propositions which have a definite truth value, such as “*There are infinitely many prime numbers*”, “*Every continuous functions $f : \mathbb{R} \rightarrow \mathbb{R}$ is bounded*”, “*Every continuous functions $f : [0, 1] \rightarrow \mathbb{R}$ is bounded*”, ..., we know that the first and the third statements are true, while the second is false (as witnessed for example by $f(x) = x^2$).

Propositional logic is not suited to study propositions for which we are not able to assign a definite truth value among true and false; an example of a statement on which propositional logic is not able to say much is the following: “*This sentence*

is false". The latter statement can be neither true (otherwise it asserts its falsity), nor false (otherwise it would be true).

A basic intuition regarding valuations is that a propositional variable A can range among all propositions which are either true or false and that a valuation v decides whether we assign to A a true proposition or a false one. Under the decision made by v regarding the propositional variables, the connectives give a truth value to the other formulae reflecting certain propositional constructions typical of the natural language:

- $(\neg\phi)$ stands for the negation of the formula/proposition ϕ ,
- $(\phi \wedge \psi)$ stands for the conjunction of the formulae/propositions ϕ, ψ ,
- $(\phi \vee \psi)$ stands for the disjunction of the formulae/propositions ϕ, ψ ,
- $(\phi \rightarrow \psi)$ stands for the statement "Whenever ϕ holds also ψ holds".

Remark 1.3. A key observation is that the truth value assigned to a formula ϕ by a valuation v depends only on the truth value the valuation assigns to the free variable of ϕ , i.e.:

$$v_0 \upharpoonright \text{varprop}(\phi) = v_1 \upharpoonright \text{varprop}(\phi)$$

entails that $v_0(\phi) = v_1(\phi)$.

This allows to define finite truth tables for each formula ϕ with $2^{|\text{varprop}(\phi)|}$ rows¹ (one row for each possible assignment of 0,1 to the propositional variables of ϕ), and $|\text{varprop}(\phi)| + 1$ columns (one column for ϕ and another column for each of the propositional variables of ϕ).

For example let ϕ be the formula $((B \rightarrow A) \wedge ((B \vee C) \rightarrow A))$ with propositional variables A, B, C . Its truth table can be computed as follows:

A	B	C	$(B \rightarrow A)$	$(B \vee C)$	$((B \vee C) \rightarrow A)$	ϕ
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	1	1	1	1
1	0	0	1	0	1	1
0	1	1	0	1	0	0
0	1	0	0	1	0	0
0	0	1	1	1	0	0
0	0	0	1	0	1	1

We may omit the truth values of the columns for the subformulae of ϕ , which are

$$(B \rightarrow A), (B \vee C), ((B \vee C) \rightarrow A)$$

and obtain the smaller table in 4 columns (3 for the propositional variables A, B, C occurring in ϕ and 1 for ϕ), and 8 rows (as many as the 2^3 possible distinct assignments of truth values to the three propositional variables A, B, C occurring in ϕ):

¹ $|X|$ denotes the number of elements of the set X

A	B	C	ϕ
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

Remark however that the truth table of all subformulae of ϕ needs to be computed in order to be able to compute the one of ϕ .

Remark 1.4. A formula ϕ is built in a finite number of stages starting from the propositional variables and introducing at each stage some propositional connective attached to one or two simpler sub-formulae of ϕ ; parentheses are needed to understand in which order the process of building ϕ occurs.

$\phi \equiv ((A \wedge B) \wedge C)$ is a formula built in two steps out of the three variables A, B, C : first we build $\psi \equiv (A \wedge B)$ out of the propositional variables A, B and then $\phi \equiv (\psi \wedge C)$ out of ψ and C .

Due to the fact that we are interested in formulae up to logical equivalence (i.e. we identify formulae having the same truth table, see Def. 1.11), and we do not want to burden our notation, we will drop parentheses when we believe this cannot cause confusion in the intended meaning of the formula. For example $A \wedge B \wedge C$ can stand either for $((A \wedge B) \wedge C)$ or for $(A \wedge (B \wedge C))$, since the two formulae are logically equivalent. On the other hand a writing of the form $A \wedge B \vee C$ is ambiguous, since it could stand either for the formula $\theta_0 \equiv ((A \wedge B) \vee C)$ or for the formula $\theta_1 \equiv (A \wedge (B \vee C))$, which are not logically equivalent. In such cases we will keep enough parentheses to avoid ambiguities, i.e. for θ_0 we will write $(A \wedge B) \vee C$ and for θ_1 we will write $A \wedge (B \vee C)$ dropping in both cases the most external parentheses but keeping the ones that clarifies the priorities on the order of introduction of the connectives.

So from now on we will write $\neg\phi$ rather than $(\neg\phi)$, $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$ rather than $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$, $\phi_1 \wedge \dots \wedge \phi_n$ rather than $(\dots((\phi_1 \wedge \phi_2) \wedge \dots) \wedge \phi_n)$ (or any of the possible rearrangements of the parentheses yielding a formula logically equivalent to the conjunction of all the ϕ_i).

Definition 1.5. A propositional formula ϕ is:

- a tautology if $v(\phi) = 1$ for *all* valuations $v : \text{VarProp} \rightarrow \{0, 1\}$,
- a contradiction if $v(\phi) = 0$ for *all* valuations $v : \text{VarProp} \rightarrow \{0, 1\}$,
- satisfiable if $v(\phi) = 1$ for *some* valuation $v : \text{VarProp} \rightarrow \{0, 1\}$.

Remark 1.6. ϕ is a tautology if and only if $\neg\phi$ is a contradiction, ϕ is satisfiable if and only if it is not a contradiction.

A tautology is a proposition which is true regardless of the context in which it is meaningfully interpreted, a contradiction is a proposition which is false regardless of the context in which it is meaningfully interpreted, a satisfiable proposition is a proposition which is true in some of the contexts in which it can be meaningfully interpreted.

Example 1.7. The following are examples of tautologies:

Peirce's law: $((A \rightarrow B) \rightarrow A) \rightarrow A$

A	B	$A \rightarrow B$	$(A \rightarrow B) \rightarrow A$	$((A \rightarrow B) \rightarrow A) \rightarrow A$
1	1	1	1	1
1	0	0	1	1
0	1	1	0	1
0	0	1	0	1

Dummet's law: $(A \rightarrow B) \vee (B \rightarrow A)$

A	B	$A \rightarrow B$	$B \rightarrow A$	$(A \rightarrow B) \vee (B \rightarrow A)$
1	1	1	1	1
1	0	0	1	1
0	1	1	0	1
0	0	1	1	1

The formula

$$(A \rightarrow \neg B) \wedge (A \rightarrow B) \wedge (B \rightarrow A) \wedge (\neg B \rightarrow A)$$

is an example of a contradiction.

A	B	$A \rightarrow \neg B$	$A \rightarrow B$	$B \rightarrow A$	$B \rightarrow \neg A$	$(A \rightarrow \neg B) \wedge (A \rightarrow B) \wedge (B \rightarrow A) \wedge (B \rightarrow \neg A)$
1	1	0	1	1	0	0
1	0	1	0	1	1	0
0	1	1	1	0	1	0
0	0	0	1	1	0	0

The formula $(B \rightarrow A) \wedge ((B \vee C) \rightarrow A)$ whose truth table we already computed is satisfiable (and thus it is not a contradiction), but it is not a tautology having value 0 for some of its possible valuations.

Now we want to formalize in our semantic the concept of logical consequence and ultimately the concept of being a theorem.

Notation 1.8. A set is given by providing its elements. We do not care neither on the ordering by which these elements are provided nor on the possible repetitions. For example for us

$$\{a, b, c\}, \{b, c, a\}, \{a, b, b, c\}, \{b, a, b, c\},$$

are all different way to describe the unique set whose elements are the objects a, b, c . \emptyset denotes the set with no elements.

Given a finite set of propositional formulae $\Gamma = \{\phi_1, \dots, \phi_n\}$

$$\bigwedge \Gamma = \phi_1 \wedge \dots \wedge \phi_n,$$

$$\bigvee \Gamma = \phi_1 \vee \dots \vee \phi_n.$$

We take the convention that

$$\bigwedge \emptyset,$$

denotes a true assertion (given that a conjunction is true iff all its conjuncts are, hence, if there are none, it is vacuously true), and that $v(\bigwedge \emptyset) = 1$ for all valuations v .

We also stipulate that

$$\bigvee \emptyset,$$

denotes a contradiction, and that $v(\bigvee \emptyset) = 0$ for all valuations v (given that a disjunction is true iff at least one of its disjuncts is true, hence, if there are no disjuncts, it cannot be true).

Definition 1.9. Let Γ be a finite set of formulae and ϕ be a formula.

$\Gamma \models \phi$ (to be read as “ ϕ is a logical consequence of Γ ” or as “ Γ models ϕ ”)

if all valuations v which make true all the formulae in Γ make also true ϕ ; equivalently $\Gamma \models \phi$ if and only if any of the two following conditions is met:

- $\min \{v(\psi) : \psi \in \Gamma\} \leq v(\phi)$ for all valuations v ,
- $(\bigwedge \Gamma) \rightarrow \phi$ is a tautology.

Let Δ be another finite set of formulae.

$\Gamma \models \Delta$ (to be read as “ Δ is a logical consequence of Γ ” or as “ Γ models Δ ”)

holds if all valuations v which make true all the formulae in Γ make also true some formula in Δ ; equivalently $\Gamma \models \Delta$ if and only if any of the following conditions is met:

- $\min \{v(\phi) : \phi \in \Gamma\} \leq \max \{v(\psi) : \psi \in \Delta\}$ for all valuations v ,
- $(\bigwedge \Gamma) \rightarrow (\bigvee \Delta)$ is a tautology.

Remark 1.10. Note the following:

- $\emptyset \not\models \emptyset$, since $\bigwedge \emptyset$ stands for a tautology while $\bigvee \emptyset$ stands for a contradiction: it is clear that the truth cannot have as a logical consequence a falsity.
- More generally $\Gamma \models \emptyset$ (or more succinctly $\Gamma \models$) holds if and only if $\bigwedge \Gamma$ is a contradiction: there cannot be a valuation making all the formula in Γ true, since such a valuation should make $\bigvee \emptyset$ true as well, which cannot be the case, since $\bigvee \emptyset$ is a contradiction.
- $\emptyset \models \Delta$ (or more succinctly $\models \Delta$) holds if and only if $\bigvee \Delta$ is a tautology, since by our conventions $v(\bigwedge \emptyset) = 1$ for all valuations v , hence $v(\bigvee \Delta) = 1$ for all valuations v .

Our intuition is that a theorem is a statement which can be formalized in our propositional logic as $\Gamma \models \phi$, where Γ is the set of premises of the theorem and ϕ is the thesis, or equivalently such that the formula $(\bigwedge \Gamma) \rightarrow \phi$ is a tautology of the propositional logic. A statement of the form $\Gamma \models \Delta$ formalizes a theorem of the form: “If all the hypothesis in Γ hold, then at least one of the possibilities in Δ occurs”.

Definition 1.11. Let ϕ, ψ be propositional formulae. We say that ϕ, ψ are logically equivalent if and only if

$$\phi \models \psi \models \phi$$

equivalently if:

- $\phi \leftrightarrow \psi$ is a tautology, (where $\phi \leftrightarrow \psi$ is a shorthand for $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$),
- ϕ and ψ have the same truth table when computing this table over the propositional variables appearing either in ϕ or in ψ .

1.2 Disjunctive normal forms

We seek for canonical representatives of the equivalence classes induced on the set of formulae by the notion of logical equivalence. These representatives are provided by formulae in disjunctive normal form.

Definition 1.12. A literal is either a propositional variable or the negation of a propositional variable

A *normal conjunction* is a formula of type $\bigwedge \Gamma$ with Γ a finite set of literals (for example $A \wedge \neg B \wedge C$ is a normal conjunction $A \wedge \neg \neg B$, $A \wedge (A \rightarrow B)$ are not).

A formula is in *disjunctive normal form* (also written DNF) if it is of the form $\bigvee \Delta$ with Δ a finite set of normal conjunctions (for example A , $\neg A$, $A \wedge \neg B$, $A \vee \neg A$, $(A \wedge \neg B \wedge C) \vee (D \wedge B \wedge \neg C) \vee \neg C$ are formulae in DNF).

Theorem 1.13. Every propositional formula ϕ is logically equivalent to a formula in DNF.

Proof. Let us prove a specific instance of the theorem. We leave to the reader to understand how the theorem can be proved in general. Let us take for example the formula $\phi \equiv ((B \rightarrow A) \wedge ((B \vee C) \rightarrow A))$ whose truth table has been already computed and is:

A	B	C	ϕ
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

Let us find a ψ in DNF logically equivalent to ϕ , i.e. with the same truth table. We take for each row of the above table in which a 1 appears, the conjunctions of literals according to the following rule:

If a propositional variable X has value 0 we take the literal $\neg X$, if it has value 1 we take the literal X .

Hence we get the following five normal conjunctions one for each of the five rows of the above table in which a 1 appears on the column for ϕ (rows 1,2,3,4,8):

$$\begin{aligned}\psi_1 &\equiv A \wedge B \wedge C \text{ for row 1} \\ \psi_2 &\equiv A \wedge B \wedge \neg C \text{ for row 2} \\ \psi_3 &\equiv A \wedge \neg B \wedge C \text{ for row 3} \\ \psi_4 &\equiv A \wedge \neg B \wedge \neg C \text{ for row 4} \\ \psi_8 &\equiv \neg A \wedge \neg B \wedge \neg C \text{ for row 8}\end{aligned}$$

Now observe that the unique truth assignment which makes true the normal conjunction ψ_i is that of row i , while all other truth assignments make ψ_i false. Hence

$$\psi \equiv \psi_1 \vee \psi_2 \vee \psi_3 \vee \psi_4 \vee \psi_8$$

is true only on rows 1,2,3,4,8, exactly as ϕ . Therefore ϕ and ψ are logically equivalent. Observe that ψ is in DNF. \square

1.3 Proof systems

In the previous section we have given some arguments to assert that the notion of logical consequence $\Gamma \models \phi$ gives a counterpart in propositional logic of the concept of a theorem. Is it possible to convey in a rigorous mathematical definition a counterpart of the notion of proof? So far we have an operational method: a “proof” of $\Gamma \models \phi$ amounts to show that $(\bigwedge \Gamma) \rightarrow \phi$ has a truth table consisting just of 1 in its column. However this operational method does not seem to reflect in any way our notion of proof. The general mathematical practice to prove a theorem of the form $\Gamma \models \phi$ is to start from the premises Γ of the theorem and, by means of basic inference rules, start to derive from the premises Γ more and more of their logical consequences up to a stage in which ϕ is obtained among the logical consequences of Γ .

In particular the notion of logical consequence $\Gamma \models \phi$ captures the concept that $\Gamma \models \phi$ is a theorem, but it doesn’t give any hint on how we should find a “proof” of this theorem: the computation of the truth table of $(\bigwedge \Gamma) \rightarrow \phi$ doesn’t seem to be the natural notion of a proof which from premises Γ yields the conclusion ϕ .

For reasons that will become transparent when we will analyze first order logic, it is better for us to dispose of another characterization of the concept of theorem which is rooted in the formalization of the concept of mathematical proof rather than in the formalization of the notion of logical consequence.

1.4 The sequent calculus LK

Let us write $\Gamma \vdash \Delta$ to be read as “ Γ proves $\bigvee \Delta$ ”, and to signify that we have a proof (whatever that means) of $\bigvee \Delta$ from premises Γ .

Notation 1.14. To simplify notation in the remainder of these notes we will write Γ, ϕ to denote the set consisting of all elements in Γ and ϕ , i.e. if $\Gamma = \{\phi_1, \dots, \phi_n\}$, Γ, ϕ is a shorthand for the set $\{\phi_1, \dots, \phi_n, \phi\}$. Hence it may occur that we confuse a formula ϕ with the set $\{\phi\}$ whose unique element is ϕ . Similarly for $\Gamma = \{\phi_1, \dots, \phi_n\}$

and $\Delta = \{\psi_1, \dots, \psi_m\}$ finite sets of formulae, Γ, Δ is a shorthand for $\Gamma \cup \Delta = \{\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m\}$.

We introduce the sequent calculus LK.

Definition 1.15. A sequent is a string of the form $\Gamma \vdash \Delta$ with Γ, Δ finite sets of formulae.

The LK-calculus has the following LK-axioms and LK-deduction rules:

- **LK-Axioms:** for all formulae ϕ the sequent

$$\phi \vdash \phi$$

is an axiom of LK.

- **LK-Structural rules:**

$$\frac{\Gamma \vdash \phi, \Delta \quad \Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta} \text{ (Cut)}$$

$$\frac{\Gamma \vdash \Delta}{\Sigma, \Gamma \vdash \Delta, \Pi} \text{ (Weakening)}$$

- **LK-Logical rules:**

$$\frac{\Gamma \vdash \phi, \Delta \quad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \wedge \psi, \Delta} \text{ (\wedge-R)}$$

$$\frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta} \text{ (\wedge-L)}$$

$$\frac{\Gamma, \phi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta} \text{ (\vee-L)}$$

$$\frac{\Gamma \vdash \phi, \psi, \Delta}{\Gamma \vdash \phi \vee \psi, \Delta} \text{ (\vee-R)}$$

$$\frac{\Gamma \vdash \phi, \Delta}{\Gamma, \neg \phi \vdash \Delta} \text{ (\neg-L)}$$

$$\frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \neg \phi, \Delta} \text{ (\neg-R)}$$

$$\frac{\Gamma \vdash \phi, \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \rightarrow \psi \vdash \Delta} \text{ (\rightarrow-L)}$$

$$\frac{\Gamma, \phi \vdash \psi, \Delta}{\Gamma \vdash \phi \rightarrow \psi, \Delta} (\rightarrow\text{-R})$$

An **LK**-deduction is obtained by any finite repeated applications of **LK**-deduction rules, either to axioms, or to sequents which are at the bottom of some previously applied deduction rule.

In other terms an **LK**-deduction is a finite tree whose leafs are **LK**-axioms and whose other nodes are always the bottom sequent whose immediate successor(s) is (are) the top sequent(s) of a deduction rule of **LK**.

$\Gamma \vdash \Delta$ is an **LK**-derivable sequent if there is an **LK**-deduction whose bottom sequent is $\Gamma \vdash \Delta$ (i.e. $\Gamma \vdash \Delta$ is the root of the tree given by this **LK**-deduction).

We give several examples of **LK**-deductions so to get the reader acquainted with this notion.

Example 1.16. A proof of Dummett's law $(A \rightarrow B) \vee (B \rightarrow A)$ (we show that $\vdash (A \rightarrow B) \vee (B \rightarrow A)$ is the bottom sequent of an **LK**-deduction, this suffices by Theorem 1.18):

$$\frac{\frac{\frac{A \vdash A}{B, A \vdash A, B} (\text{Weakening})}{B \vdash A, A \rightarrow B} (\rightarrow\text{-R})}{\vdash B \rightarrow A, A \rightarrow B} (\rightarrow\text{-R}) \quad \frac{}{\vdash (B \rightarrow A) \vee (A \rightarrow B)} (\vee\text{-R})$$

A proof of De Morgan's law $\neg(A \wedge B) \equiv \neg A \vee \neg B$. More precisely we show that $\neg(A \wedge B) \vdash \neg A \vee \neg B$ and $\neg A \vee \neg B \vdash \neg(A \wedge B)$. This suffices by Theorem 1.18:

$$\begin{array}{c} \frac{\frac{A \vdash A}{B, A \vdash A} (\text{Weakening})}{B, A \vdash A \wedge B} (\wedge\text{-R}) \\ \frac{}{\neg(A \wedge B), B, A \vdash} (\neg\text{-L}) \\ \frac{}{\neg(A \wedge B), A \vdash \neg B} (\neg\text{-R}) \\ \frac{}{\neg(A \wedge B) \vdash \neg A, \neg B} (\neg\text{-R}) \\ \frac{}{\neg(A \wedge B) \vdash \neg A \vee \neg B} (\vee\text{-R}) \end{array}$$

$$\begin{array}{c} \frac{\frac{A \vdash A}{B, A \vdash A} (\text{Weakening})}{B \wedge A \vdash A} (\wedge\text{-L}) \\ \frac{}{\neg A, B \wedge A \vdash} (\neg\text{-L}) \\ \frac{}{\neg A \vdash \neg(B \wedge A)} (\neg\text{-R}) \end{array} \quad \begin{array}{c} \frac{\frac{B \vdash B}{B, A \vdash B} (\text{Weakening})}{B \wedge A \vdash B} (\wedge\text{-L}) \\ \frac{}{\neg B, B \wedge A \vdash} (\neg\text{-L}) \\ \frac{}{\neg B \vdash \neg(B \wedge A)} (\neg\text{-R}) \end{array}$$

$$\frac{}{\neg A \vee \neg B \vdash \neg(A \wedge B)} (\vee\text{-R})$$

Exercise 1.17. Find **LK**-derivations of $A \wedge B \vdash B \wedge A$ and of $A \vee B \vdash B \vee A$.

This is the main result we aim for:

Theorem 1.18. *Let Γ, Δ be finite sets of propositional formulae. The following are equivalent:*

1. $\Gamma \models \Delta$
2. $\Gamma \vdash \Delta$ is an LK-derivable sequent.

2 implies 1 is usually referred to as “the soundness theorem”, while 1 implies 2 is usually referred to as “the completeness theorem”.

Exercise 1.19. Is $A \rightarrow B \vdash B \rightarrow A$ a LK-derivable sequent? (HINT: use the above theorem).

To simplify our discussions we will often say that $\Gamma \vdash \Delta$ is a valid sequent to signify that $\Gamma \models \Delta$ holds.

The keys for the proof of the above theorem are given by the following Lemma:

Lemma 1.20. *Let $v : \text{VarProp} \rightarrow \{0, 1\}$ be a valuation. Then the followig holds:*

1. Assume $v(\bigwedge \Gamma_0) \leq v(\bigvee \Delta_0)$ and

$$\frac{\Gamma_0 \vdash \Delta_0}{\Gamma \vdash \Delta} (R)$$

is an LK-structural rule with one top sequent (i.e. the Weakening rule). Then $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$.

2. Assume $v(\bigwedge \Gamma_i) \leq v(\bigvee \Delta_i)$ for $i = 0, 1$ and

$$\frac{\Gamma_0 \vdash \Delta_0 \quad \Gamma_1 \vdash \Delta_1}{\Gamma \vdash \Delta} (R)$$

is an LK-structural rule with two top sequents (i.e. the Cut rule). Then $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$.

3. Assume

$$\frac{\Gamma_0 \vdash \Delta_0}{\Gamma \vdash \Delta} (R)$$

is an LK-logical rule with one top sequent (i.e. \wedge -L, \vee -R, \rightarrow -R, \neg -L, \neg -R). Then $v(\bigwedge \Gamma_0) \leq v(\bigvee \Delta_0)$ if and only if $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$.

4. Assume

$$\frac{\Gamma_0 \vdash \Delta_0 \quad \Gamma_1 \vdash \Delta_1}{\Gamma \vdash \Delta} (R)$$

is an LK-logical rule with two top sequents (i.e. \wedge -R, \vee -L, \rightarrow -L). Then $v(\bigwedge \Gamma_0) \leq v(\bigvee \Delta_0)$ and $v(\bigwedge \Gamma_1) \leq v(\bigvee \Delta_1)$ hold simultaneously if and only if $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$.

The above Lemma has the following immediate corollaries:

Lemma 1.21. *Let R be an LK-structural rule. Let $\Gamma_i \vdash \Delta_i$ be the top sequent(s) of R for $i = 0$ ($i = 0, 1$ if the rule has two sequents above the horizontal line). Let $\Gamma \vdash \Delta$ be the bottom sequent of R (i.e. the sequent below the horizontal line).*

Then $\Gamma \models \Delta$ holds whenever all the sequents $\Gamma_i \vdash \Delta_i$ on top of the horizontal line are such that $\Gamma_i \models \Delta_i$.

Lemma 1.22. *Let R be an LK-logical rule. Let $\Gamma_i \vdash \Delta_i$ be the top sequent(s) of R for $i = 0$ ($i = 0, 1$ if the rule has two sequents above the horizontal line). Let $\Gamma \vdash \Delta$ be the bottom sequent of R (i.e. the sequent below the horizontal line).*

Then $\Gamma \models \Delta$ if and only if all the sequents $\Gamma_i \vdash \Delta_i$ on top of the horizontal line are such that $\Gamma_i \models \Delta_i$.

We defer the proof of the above Lemmas to a later stage and for now we assume they all hold. Now we can prove Theorem 1.18

Proof. We prove both implications by a suitable induction on the complexity of proofs or of the formulae in Γ, Δ .

2 implies 1. The proof is done by induction on the height of an LK-derivation whose bottom sequent (or root) is $\Gamma \vdash \Delta$.

We define the height of an LK-derivation as the longest path connecting its bottom sequent to one of its leaves, where a path from the root to a leaf is the number of horizontal lines one crosses to go from the root of the LK-derivation to the given leaf. In the examples of 1.16:

- The LK-derivation corresponding to Dummett's law has root $\vdash (A \rightarrow B) \vee (B \rightarrow A)$, one leaf $A \vdash A$, and a unique path of length 5 connecting the root to this leaf, hence its height is 5.
- Both of the LK-derivations corresponding to DeMorgan's law have two leaves and two paths both of the same length which are respectively 7 - for the topmost LK-derivation - and 6 - for the lower LK-derivation -. Hence these LK-derivations have height respectively 7 and 6.
- The LK-derivation in Example 1.24 which establishes that

$$\phi \equiv (P \rightarrow (Q \rightarrow R)) \wedge \neg((P \rightarrow Q) \rightarrow (P \rightarrow R)).$$

is a contradiction has 4 leaves (from left to right $R \vdash R$, $Q \vdash Q$, $P \vdash P$, $P \vdash P$) and the corresponding paths from the root $\phi \vdash \emptyset$ to the leaves have length 8, 8, 7, 6. Hence this LK-derivation has height 8.

An axiom $\phi \vdash \phi$ is an LK-derivation of height 0 and it is trivial to check that $\phi \models \phi$. Hence 2 implies 1 holds for the axioms of LK, i.e. for all trees of an LK-derivation of height 0.

Now observe that the Lemmas 1.21 and 1.22 grant that whenever the premises of a deduction rule are valid sequents, so is the conclusion. So assume we pick an LK-derivation of height $n + 1$ and we know that 2 implies 1 holds for all LK-derivations of height at most n . The LK-derivation will either look like

$$\frac{\begin{array}{c} T_0 \\ \vdots \\ \Gamma_0 \vdash \Delta_0 \end{array}}{\Gamma \vdash \Delta} \text{ (R)}$$

with T_0 an LK-derivation of height n whose bottom sequent is $\Gamma_0 \vdash \Delta_0$, or it will look like

$$\frac{\begin{array}{c} T_1 \\ \vdots \vdots \vdots \vdots \vdots \vdots \\ \Gamma_1 \vdash \Delta_1 \end{array} \quad \begin{array}{c} T_2 \\ \vdots \vdots \vdots \vdots \vdots \vdots \\ \Gamma_2 \vdash \Delta_2 \end{array}}{\Gamma \vdash \Delta} \text{ (R)}$$

where both T_i are LK-derivations of height at most n whose bottom sequent is $\Gamma_i \vdash \Delta_i$. We can apply the induction hypothesis to the LK-derivations T_i for $i = 0, 1, 2$, since these trees have height at most n . In either cases the induction hypotheses give that **2** implies **1** for Γ_i, Δ_i for $i = 0$ or for $i = 1, 2$. Hence we conclude that $\Gamma_i \models \Delta_i$ for $i = 0, 1, 2$, given that the LK-derivations T_i witness that $\Gamma_i \vdash \Delta_i$ for $i = 0, 1, 2$.

By Lemmas 1.21 or 1.22 (according to whether R is an LK-structural rule or an LK-logical rule), we conclude that $\Gamma \models \Delta$.

1 implies 2. We suppose that $\Gamma \models \Delta$, and we must find an LK-derivation of $\Gamma \vdash \Delta$.

In this case we proceed by induction on the number of connectives appearing in the finite set of formulae $\Gamma \cup \Delta$:

Given a formula ϕ , we let $c(\phi)$ be the number of propositional connectives appearing in ϕ , for example if $\phi \equiv (A \wedge \neg B) \rightarrow C$, we have $c(\phi) = 3$, since the 3 connectives appearing in ϕ are $\wedge, \neg, \rightarrow$.

Given a finite set of formulae $\Sigma = \{\phi_1, \dots, \phi_n\}$ we let $c(\Sigma) = \sum_{i=1, \dots, n} c(\phi_i)$.

We prove by induction on $c(\Gamma \cup \Delta)$ that $\Gamma \models \Delta$ entails that there is an LK-derivation with root $\Gamma \vdash \Delta$.

Assume $c(\Gamma \cup \Delta) = 0$. This occurs only if $\Gamma \cup \Delta$ consists of a finite set of propositional variables. Thus assume that Γ is the finite set of propositional variables $\{A_1, \dots, A_n\}$ and Δ is the finite set of propositional variables $\{B_1, \dots, B_m\}$. Assume towards a contradiction that $\Gamma \cap \Delta = \emptyset$, i.e. $A_i \neq B_j$ for all $i = 1, \dots, n$ and $j = 1, \dots, m$. Set $v(A_i) = 1$ for all i and $v(B_j) = 0$ for all j . Then $v(\bigwedge \Gamma) = 1 > 0 = v(\bigvee \Delta)$, hence v witnesses that $\Gamma \not\models \Delta$, a contradiction. Hence $A_i = B_j = A$ for some i, j . We obtain an LK-derivation of $\Gamma \vdash \Delta$ by means of the weakening rule as follows:

$$\frac{A \vdash A}{\Gamma \vdash \Delta} \text{ (Weakening)}$$

Now assume that that $\Gamma \models \Delta$ entails that there is an LK derivation with root $\Gamma \vdash \Delta$ for all finite sets of formulae Γ, Δ such that $c(\Gamma \cup \Delta) \leq n$. Let us prove that this holds also for all finite sets of formulae Γ, Δ such that $c(\Gamma \cup \Delta) = n+1$.

Since $c(\Gamma \cup \Delta) = n+1 > 0$, there is at least one formula $\phi \in \Gamma \cup \Delta$ such that $c(\phi) > 0$.

If ϕ appears both in Γ, Δ , then as before $\Gamma \vdash \Delta$ can be obtained from the axiom $\phi \vdash \phi$ by an instance of the weakening rule.

Hence we can suppose that ϕ belongs just to one of the sets Γ, Δ and contains at least one connective.

For the sake of the discussion, let us assume that $\phi = \psi \wedge \theta$ is an element of Δ but not of Γ . Let $\Delta_0 = \Delta \setminus \{\phi\}$. Then we have that $\phi \notin \Gamma$, $\phi \notin \Delta_0$ and

$$\frac{\Gamma \vdash \psi, \Delta_0 \quad \Gamma \vdash \theta, \Delta_0}{\Gamma \vdash \Delta} (\wedge\text{-R})$$

is an instance of the deduction rule (\wedge -R) applied to the sequents $\Gamma \vdash \psi, \Delta_0$, $\Gamma \vdash \theta, \Delta_0$.

By Lemma 1.22, we get that $\Gamma \models \Delta$ if and only if $\Gamma \models \psi, \Delta_0$ and $\Gamma \models \theta, \Delta_0$ hold simultaneously. But our assumption is that $\Gamma \models \Delta$, hence we conclude that $\Gamma \models \psi, \Delta_0$ and $\Gamma \models \theta, \Delta_0$ hold simultaneously.

Now observe that

$$c(\Gamma \cup \{\psi\} \cup \Delta_0), c(\Gamma \cup \{\theta\} \cup \Delta_0) < c(\Gamma \cup \Delta) = n + 1.$$

This occurs since $c(\phi) = c(\psi) + c(\theta) + 1$, and ϕ is an element neither of Γ nor of Δ_0 , hence

$$c(\Gamma \cup \{\psi\} \cup \Delta_0) \leq c(\psi) + c(\Gamma \cup \Delta_0) < c(\phi) + c(\Gamma \cup \Delta_0) = c(\Gamma \cup \Delta),$$

and similarly for θ (the first inequality may be strict in case ψ belongs to $\Gamma \cup \Delta_0$, in this case $c(\Gamma \cup \{\psi\} \cup \Delta_0) = c(\Gamma \cup \Delta_0)$). Hence by induction hypotheses, we can find **LK**-derivations

$$\frac{T_0}{\Gamma \vdash \psi, \Delta_0}$$

$$\frac{T_1}{\Gamma \vdash \theta, \Delta_0}$$

of $\Gamma \vdash \psi, \Delta_0$ and of $\Gamma \vdash \theta, \Delta_0$.

Now we can find a derivation of $\Gamma \vdash \phi$ as follows:

$$\frac{\begin{array}{c} T_0 \\ \vdots \\ \Gamma \vdash \psi, \Delta_0 \end{array} \quad \begin{array}{c} T_1 \\ \vdots \\ \Gamma \vdash \theta, \Delta_0 \end{array}}{\Gamma \vdash \Delta} (\wedge\text{-R})$$

We leave to the reader to handle the other possible cases which are:

- $\phi = \psi \wedge \theta \in \Gamma$,
- $\phi = \psi \vee \theta \in \Gamma$,
- $\phi = \psi \vee \theta \in \Delta$,
- $\phi = \neg\psi \in \Gamma$,
- $\phi = \neg\psi \in \Delta$,
- $\phi = \psi \rightarrow \theta \in \Gamma$,
- $\phi = \psi \rightarrow \theta \in \Delta$.

The proofs are all the same and use the following observations:

- $\Gamma \vdash \Delta$ is the bottom sequent of an LK-logical rule R introducing ϕ either in Γ or in Δ .

- The fact that for *all* LK-logical rules R the bottom sequent of the rule is valid if and only if the top sequent(s) is (are).
- The inductive assumptions to find LK-derivation(s) of the top sequent(s) of R , which must be valid by the above observations.

In all cases one can patch this (these) LK-derivations together on top of the rule R to yield the desired LK-derivation of $\Gamma \vdash \Delta$.

This concludes the proof of 1 implies 2.

The proof of Theorem 1.18 is completed (modulo the proofs of Lemmas 1.20, 1.21, 1.22). \square

So we are left with the proof of Lemmas 1.20, 1.21, 1.22.

We prove Lemma 1.20 and leave the proof of the other two to the reader.

Proof. We divide the proof in two parts: one for the LK-structural rules (i.e the first two items of the Lemma), and one for the LK-logical rules (i.e the last two items of the Lemma).

LK-structural rules: Assume R is the weakening rule

$$\frac{\Gamma \vdash \Delta}{\Sigma, \Gamma \vdash \Delta, \Pi} \text{ (Weakening)}$$

and $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$. We must show that $v(\bigwedge(\Sigma \cup \Gamma)) \leq v(\bigvee(\Delta \cup \Pi))$. But

$$v(\bigwedge(\Sigma \cup \Gamma)) \leq v(\bigwedge \Gamma) \leq v(\bigvee \Delta) \leq v(\bigvee(\Delta \cup \Pi)).$$

Hence the thesis holds for the Weakening rule.

Assume R is the cut rule

$$\frac{\Gamma \vdash \phi, \Delta \quad \Sigma, \phi \vdash \Pi}{\Sigma, \Gamma \vdash \Delta, \Pi} \text{ (Cut)}$$

and

$$v(\bigwedge \Gamma) \leq v(\phi \vee \bigvee \Delta),$$

$$v(\phi \wedge \bigwedge \Sigma) \leq v(\bigvee \Pi)$$

simultaneously hold. So assume $v(\bigwedge(\Sigma \cup \Gamma)) = 1$. We must show that $v(\bigvee(\Delta \cup \Pi)) = 1$: Clearly

$$1 = v(\bigwedge(\Sigma \cup \Gamma)) \leq v(\bigwedge \Gamma) \leq v(\phi \vee \bigvee \Delta),$$

and

$$1 = v(\bigwedge(\Sigma \cup \Gamma)) \leq v(\bigwedge \Sigma).$$

Hence we get that $v(\phi \vee \bigvee \Delta) = 1$. Now there are two cases:

- $v(\phi) = 0$. Then

$$1 = v(\phi \vee \bigvee \Delta) = \max \{v(\phi), v(\bigvee \Delta)\} = v(\bigvee \Delta) \leq v(\bigvee (\Delta \cup \Pi)).$$

- $v(\phi) = 1$. Then

$$1 = \min \{v(\phi), v(\bigwedge \Sigma)\} = v(\phi \wedge \bigwedge \Sigma) \leq v(\bigvee \Pi) \leq v(\bigvee (\Delta \cup \Pi)).$$

In either cases we proved that if $v(\bigwedge (\Sigma \cup \Gamma)) = 1$, then $v(\bigvee (\Delta \cup \Pi)) = 1$. Hence the thesis holds also for the Cut rule.

LK-logical rules: We provide the proof for two of the eight logical rules we introduced, and we invite the reader to provide proofs for the remaining ones. We choose an “easy” one (\neg -R) and a “more difficult” one (\vee -L).

So let us pick the LK-logical rule

$$\frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta, \neg \phi} (\neg\text{-R})$$

and a valuation v .

We must show that

$$v(\bigwedge \Gamma) \leq v(\neg \phi \vee \bigvee \Delta) \text{ if and only if } v(\phi \wedge \bigwedge \Gamma) \leq v(\bigvee \Delta)$$

First assume $v(\bigwedge \Gamma) \leq v(\neg \phi \vee \bigvee \Delta)$. We must show that $v(\phi \wedge \bigwedge \Gamma) \leq v(\bigvee \Delta)$. If $v(\phi) = 0$, this is trivially the case, since

$$v(\phi \wedge \bigwedge \Gamma) = 0 \leq v(\bigvee \Delta).$$

So let us consider the case $v(\phi) = 1$, hence

$$\begin{aligned} v(\phi \wedge \bigwedge \Gamma) &= v(\bigwedge \Gamma) \leq v(\neg \phi \vee \bigvee \Delta) = \\ &= \max \{v(\neg \phi), v(\bigvee \Delta)\} = \max \{0, v(\bigvee \Delta)\} = v(\bigvee \Delta), \end{aligned}$$

and we are done also in this case.

Now assume $v(\phi \wedge \bigwedge \Gamma) \leq v(\bigvee \Delta)$. We must show that $v(\bigwedge \Gamma) \leq v(\neg \phi \vee \bigvee \Delta)$. If $v(\phi) = 0$, this is trivially the case, since

$$v(\bigwedge \Gamma) \leq 1 = v(\neg \phi) \leq v(\neg \phi \vee \bigvee \Delta).$$

So let us consider the case $v(\phi) = 1$, as before

$$v(\bigwedge \Gamma) = \min \{1, v(\bigwedge \Gamma)\} = v(\phi \wedge \bigwedge \Gamma) \leq v(\bigvee \Delta) \leq v(\neg \phi \vee \bigvee \Delta),$$

and we are done also in this case.

Now let us deal with the LK-logical rule

$$\frac{\Gamma, \phi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta} \text{ (}\vee\text{-L)}$$

and a valuation v .

We must show that

$$v((\phi \vee \psi) \wedge \bigwedge \Gamma) \leq v(\bigvee \Delta)$$

if and only if

$$\max \left\{ v(\phi \wedge \bigwedge \Gamma), v(\psi \wedge \bigwedge \Gamma) \right\} \leq v(\bigvee \Delta).$$

Let $\Gamma = \{\theta_1, \dots, \theta_n\}$. Then we have

$$\begin{aligned} v((\phi \vee \psi) \wedge \bigwedge \Gamma) &= \min \{ \max \{ v(\phi), v(\psi) \}, v(\theta_1), \dots, v(\theta_n) \} = \\ &= \max \{ \min \{ v(\phi), v(\theta_1), \dots, v(\theta_n) \}, \min \{ v(\psi), v(\theta_1), \dots, v(\theta_n) \} \} = \\ &= \max \left\{ v(\phi \wedge \bigwedge \Gamma), v(\psi \wedge \bigwedge \Gamma) \right\}. \end{aligned}$$

The desired conclusion is now immediate. □

Remark 1.23. LK-structural rules do not enjoy the stronger properties which can be inferred for the LK-logical rules (i.e. inequalities are not only downward preserved but also upward preserved along an LK-logical rule). There can be valuations v for which $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$ holds for the bottom sequent of an LK-structural rule but fails for at least one of the top sequents:

For example let $v(A) = 1, v(B) = 0$. Then this is the case for the following instances of the Cut rule with $\Gamma = \Pi = \{A\}, \Delta = \Sigma = \emptyset$

$$\frac{A \vdash B \quad B \vdash A}{A \vdash A} \text{ (Cut)}$$

and of the Weakening rule:

$$\frac{A \vdash B}{A, B \vdash B} \text{ (Weakening)}$$

We leave to the reader to provide a proof of Lemmas 1.21, 1.22.

LK as a tool to solve satisfiability problems

It is in general much faster to tackle the problem of checking whether a given propositional formula is satisfiable, or a tautology, or a contradiction using the LK-calculus, rather than resorting to the computation of its truth table. Lemma 1.20 and the proof of the completeness theorem give an efficient algorithm to check whether $\Gamma \models \Delta$ holds or not. We give a number of examples below.

Example 1.24. Show that $(A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]$ is a tautology. This amounts to show that the sequent $\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]$ is LK-derivable.

We follow the proof of the completeness theorem: we seek a proof of the above sequent backward, starting from the root of a possible derivation of the above sequent. By means of successive applications of LK-logical rules, we try to build with a bottom-up procedure an LK-derivation of this sequent as follows:

STEP 1: We apply \rightarrow -R to the sequent

$$\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]$$

with $\Gamma = \emptyset, \Delta = \emptyset$:

$$\frac{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)}{\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]} (\rightarrow\text{-R})$$

STEP 2: We apply \rightarrow -R to the sequent

$$A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)$$

with $\Gamma = \{A \rightarrow B\}, \Delta = \emptyset$:

$$\frac{\frac{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C}{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)} (\rightarrow\text{-R})}{\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]} (\rightarrow\text{-R: } \Gamma = \emptyset, \Delta = \emptyset)$$

STEP 3: We apply \rightarrow -R to the sequent

$$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$$

with $\Gamma = \{B \rightarrow C, A \rightarrow B\}, \Delta = \emptyset$

$$\frac{\frac{\frac{A \rightarrow B, B \rightarrow C, A \vdash C}{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C} (\rightarrow\text{-R})}{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)} (\rightarrow\text{-R: } \Gamma = \{A \rightarrow B\}, \Delta = \emptyset)}{\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]} (\rightarrow\text{-R: } \Gamma = \emptyset, \Delta = \emptyset)$$

STEP 4: We apply \rightarrow -L to the sequent

$$A \rightarrow B, B \rightarrow C, A \vdash C$$

with $\Gamma = \{B \rightarrow C, A\}, \Delta = \{C\}$

$$\frac{\frac{\frac{B \rightarrow C, A \vdash A, C \quad B, B \rightarrow C, A \vdash C}{A \rightarrow B, B \rightarrow C, A \vdash C} (\rightarrow\text{-L})}{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C} (\rightarrow\text{-R: } \Gamma = \{B \rightarrow C, A \rightarrow B\}, \Delta = \emptyset)}{\frac{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)}{\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]} (\rightarrow\text{-R: } \Gamma = \emptyset, \Delta = \emptyset)} (\rightarrow\text{-R: } \Gamma = \{A \rightarrow B\}, \Delta = \emptyset)$$

STEP 5: We apply \rightarrow -L to the sequent

$$B, B \rightarrow C, A \vdash C$$

with $\Gamma = \{B, A\}, \Delta = \{C\}$

$$\begin{array}{c}
\frac{B \rightarrow C, A \vdash A, C \quad \frac{B, A \vdash B, C \quad B, A, C \vdash C}{B, B \rightarrow C, A \vdash C} (\rightarrow\text{-L})}{\frac{A \rightarrow B, B \rightarrow C, A \vdash C}{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C} (\rightarrow\text{-R: } \Gamma = \{B \rightarrow C, A \rightarrow B\}, \Delta = \emptyset)} (\rightarrow\text{-L: } \Gamma = \{B \rightarrow C, A\}, \Delta = \{C\}) \\
\frac{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C}{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)} (\rightarrow\text{-R: } \Gamma = \{A \rightarrow B\}, \Delta = \emptyset) \\
\frac{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)}{\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]} (\rightarrow\text{-R: } \Gamma = \emptyset, \Delta = \emptyset)
\end{array}$$

FINAL STEP: We apply the relevant weakening rules to obtain the sequents

$$B \rightarrow C, A \vdash A, C$$

$$B, A \vdash B, C$$

$$B, A, C \vdash C$$

as weakenings of the axioms $A \vdash A$, $B \vdash B$, $C \vdash C$.

The LK-derivation of

$$\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]$$

we constructed is:

$$\begin{array}{c}
\frac{A \vdash A}{B \rightarrow C, A \vdash A, C} (\text{Weakening}) \quad \frac{\frac{B \vdash B}{B, A \vdash B, C} (\text{Weakening}) \quad \frac{C \vdash C}{B, A, C \vdash C} (\text{Weakening})}{B, B \rightarrow C, A \vdash C} (\rightarrow\text{-L: } \Gamma = \{B, A\}, \Delta = \{C\}) \\
\frac{A \rightarrow B, B \rightarrow C, A \vdash C}{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C} (\rightarrow\text{-R: } \Gamma = \{B \rightarrow C, A \rightarrow B\}, \Delta = \emptyset) \\
\frac{A \rightarrow B, B \rightarrow C \vdash A \rightarrow C}{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)} (\rightarrow\text{-R: } \Gamma = \{A \rightarrow B\}, \Delta = \emptyset) \\
\frac{A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)}{\vdash (A \rightarrow B) \rightarrow [(B \rightarrow C) \rightarrow (A \rightarrow C)]} (\rightarrow\text{-R: } \Gamma = \emptyset, \Delta = \emptyset)
\end{array}$$

Now let's check the following formula is a contradiction:

$$\phi \equiv (P \rightarrow (Q \rightarrow R)) \wedge \neg((P \rightarrow Q) \rightarrow (P \rightarrow R)).$$

ϕ is a contradiction iff $\phi \models \emptyset$ iff $\phi \vdash \emptyset$ is LK-derivable. Thus we must find a LK-derivation of $\phi \vdash \emptyset$. We proceed as before to build such a derivation and we get:

$$\begin{array}{c}
\frac{R \vdash R}{Q, P, R \vdash R} \quad \frac{Q \vdash Q}{Q, P \vdash R, Q} \quad \frac{P \vdash P}{Q \rightarrow R, P \vdash P, R} \quad \frac{P \vdash P}{P \rightarrow Q, P \vdash P, R} \\
\frac{Q, Q \rightarrow R, P \vdash R}{P \rightarrow Q, Q \rightarrow R, P \vdash R} \quad \frac{Q \rightarrow R, P \vdash P, R}{P \rightarrow Q, P \vdash P, R} \\
\frac{P \rightarrow Q, Q \rightarrow R, P \vdash R}{P \rightarrow (Q \rightarrow R), P \rightarrow Q, P \vdash R} \quad \frac{P \rightarrow Q, P \vdash P, R}{P \rightarrow Q, P \vdash P, R} \\
\frac{P \rightarrow (Q \rightarrow R), P \rightarrow Q, P \vdash R}{P \rightarrow (Q \rightarrow R), P \rightarrow Q \vdash P \rightarrow R} \\
\frac{P \rightarrow (Q \rightarrow R), P \rightarrow Q \vdash P \rightarrow R}{P \rightarrow (Q \rightarrow R) \vdash (P \rightarrow Q) \rightarrow (P \rightarrow R)} \\
\frac{P \rightarrow (Q \rightarrow R) \vdash (P \rightarrow Q) \rightarrow (P \rightarrow R)}{P \rightarrow (Q \rightarrow R), \neg((P \rightarrow Q) \rightarrow (P \rightarrow R)) \vdash} \\
\frac{P \rightarrow (Q \rightarrow R), \neg((P \rightarrow Q) \rightarrow (P \rightarrow R)) \vdash}{(P \rightarrow (Q \rightarrow R)) \wedge \neg((P \rightarrow Q) \rightarrow (P \rightarrow R)) \vdash}
\end{array}$$

We leave to the reader to check which rules have been applied in each of the steps of the above derivation.

Now we want to address the satisfiability problem. We want to check whether

$$\phi \equiv [\neg A \wedge \neg C] \wedge [(D \rightarrow A) \vee Q]$$

is a satisfiable formula. One can check this computing its truth table, but this is an awkward task given that we have 4 propositional variables in ϕ , hence $2^4 = 16$ rows in its truth table. Moreover to compute the truth table of ϕ , along the way, we must also compute the truth tables of all the formula concurring to the construction of ϕ , i.e.: $\neg A \wedge \neg C$, $(D \rightarrow A) \vee Q$, $\neg A$, $\neg C$, $D \rightarrow A$.

There is a more efficient strategy to find a valuation witnessing the satisfiability of ϕ by means of Lemma 1.20, which goes as follows:

We start by building a derivation of $\phi \vdash \emptyset$ as in the previous examples, using just LK-logical rules, and *not using* in the last step the weakening rule.

This will give us a tree whose leaves j are of the form $\Gamma_j \vdash \Delta_j$ with $\Gamma_j \cup \Delta_j$ contained in the finite sets of propositional variables of ϕ .

If for all the leaves j there is some propositional variable A_j in $\Gamma_j \cap \Delta_j$, then all the sequents $\Gamma_j \vdash \Delta_j$ can be obtained from $A_j \vdash A_j$ by means of the weakening rule, hence $\phi \vdash \emptyset$ admits an LK-derivation, i.e. ϕ is a contradiction.

Otherwise some leaf j is such that $\Gamma_j \cap \Delta_j$ is the emptyset. In which case we can let $v(X) = 1$ for all $X \in \Gamma_j$ and $v(Y) = 0$ for all $Y \in \Delta_j$, giving that $v(\bigwedge \Gamma_j) = 1 > 0 = v(\bigvee \Delta_j)$.

By repeated application of Lemma 1.20 to the sequents $\Gamma \vdash \Delta$ appearing along the path from $\phi \vdash \emptyset$ to the leaf $\Gamma_j \vdash \Delta_j$, the inequality $v(\bigwedge \Gamma) > v(\bigvee \Delta)$ holds for all such sequents (given that along these paths we have only used LK-logical rules), hence $v(\phi) > v(\bigvee \emptyset) = 0$. v is a valuation witnessing the satisfiability of ϕ .

So let us use this strategy to check whether ϕ is satisfiable. The tentative construction of an LK-derivation of $\phi \vdash \emptyset$ gives us the following tree:

$$\frac{\frac{\frac{\frac{Q \vdash A, C \quad (D \rightarrow A) \vdash A, C}{(D \rightarrow A) \vee Q \vdash A, C}}{\neg C, (D \rightarrow A) \vee Q \vdash A}}{\neg A, \neg C, (D \rightarrow A) \vee Q \vdash}}{\neg A \wedge \neg C, (D \rightarrow A) \vee Q \vdash} \frac{}{[\neg A \wedge \neg C] \wedge [(D \rightarrow A) \vee Q] \vdash}$$

We can stop at this stage of the construction of a possible LK-derivation of $\phi \vdash \emptyset$: the topmost left sequent

$$Q \vdash A, C$$

consists just of propositional variables, and no such variable appears on both sides of the \vdash symbol. Hence a valuation v such that $v(Q) = 1, v(A) = v(C) = 0$ is such that $v(\phi) = 1$.

The direct computation of the two rows² of the truth table of ϕ induced by valuations satisfying the above constraint show that this is indeed the case.

²There at least two valuations witnessing the satisfiability of ϕ , since the above constraints leave a complete freedom on the choice of $v(D)$. Other leaves which cannot be obtained by weakenings of axioms may provide other valuations realizing ϕ .

In particular from the above tentative construction of an LK-derivation of $\phi \vdash \emptyset$, we have been guided to the definition of a valuation witnessing the satisfiability of ϕ .

To appreciate why this method is efficient, we invite the reader to solve this same satisfiability problem by means of truth tables.

1.5 Exercises on propositional logic and LK-calculus

Here is a list of suggestions for exercises on propositional calculus:

- The webpage <https://pythonism.wordpress.com/2010/09/13/propositional-logic-and-some-tautologies> contains a very rich list of propositional tautologies. Find an LK-derivation of at least five of them ($\sim P$ stands for $\neg P$, to deal with LK-derivations of formulae with \leftrightarrow among its connectives, replace $\phi \leftrightarrow \psi$ by the equivalent formula $\phi \rightarrow \psi \wedge \psi \rightarrow \phi$, or else look at the third item below).
- Take randomly four formulae of propositional calculus each one containing at least 4 propositional variables and 6 connectives so that all the connectives $\neg, \wedge, \vee, \rightarrow$ appear in any of these formulae. Check whether the formulae you chose are satisfiable, tautologies, or contradictions.
- Find LK-logical rules (\leftrightarrow -L) and (\leftrightarrow -R) satisfying items 3 or 4 of Lemma 1.20 for the propositional connective \leftrightarrow . (**HINT:** use that

$$A \leftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B) \equiv (A \rightarrow B) \wedge (B \rightarrow A)$$

and try to find an LK-derivation of $\Gamma, (A \wedge B) \vee (\neg A \wedge \neg B) \vdash \Delta$ by using LK-logical rules acting only on $(A \wedge B) \vee (\neg A \wedge \neg B)$ or its subformulae. Proceed this way until you reach a stage in which the sequents $\Sigma \vdash \Pi$ you are handling are such that $\Sigma \cup \Pi = \Gamma \cup \Delta \cup \{A, B\}$. These sequents together with the one you started with should suggest you what is the LK-logical rules (\leftrightarrow -L). To find (\leftrightarrow -R) proceed in the same way but starting with $\Gamma \vdash (A \rightarrow B) \wedge (B \rightarrow A), \Delta$. Prove that Lemma 1.20 holds for the rules you introduced for this connective.

- Choose your favourite formula ϕ in two propositional variables A, B . Define $v(A \times_{\phi} B) = v(\phi)$ for any valuation v . This gives you the truth table of a propositional connective \times_{ϕ} binding together two subformulae. Find LK-logical rules (\times_{ϕ} -L) and (\times_{ϕ} -R) satisfying items 3 or 4 of Lemma 1.20 for \times_{ϕ} and prove that Lemma 1.20 holds for the rules you introduced for this connective (note that your rules may have more than two premises).
- Show that the LK-rule

$$\frac{\Gamma \vdash \phi, \Delta \quad \Sigma, \phi \vdash \Pi}{\Gamma, \Sigma \vdash \Delta, \Pi}$$

can be obtained by means of the cut and weakening rules.

- Prove that Lemma 1.21 holds for the following rules (for some of these the proof is a self-evident variation of what has been already proved, for others it is more delicate):

$$\frac{\Gamma \vdash \Delta, \phi \wedge \psi}{\Gamma \vdash \Delta, \phi} \text{ (\wedge-elimination)}$$

$$\frac{\Gamma, \neg\phi \vdash \Delta}{\Gamma \vdash \Delta, \phi} \text{ (Proof by contradiction)}$$

$$\frac{\Gamma \vdash \Delta, \neg\phi \rightarrow \neg\psi}{\Gamma \vdash \Delta, \psi \rightarrow \phi} \text{ (Proof by contraposition)}$$

$$\frac{\Gamma \vdash \Delta, \phi \rightarrow \psi \quad \Gamma \vdash \Delta, \phi}{\Gamma \vdash \Delta, \psi} \text{ (Modus Ponens)}$$

$$\frac{\Gamma \vdash \Delta, \phi \vee \psi \quad \Gamma, \phi \vdash \Delta, \theta \quad \Gamma, \psi \vdash \Delta, \theta}{\Gamma \vdash \Delta, \theta} \text{ (\vee-elimination)}$$

In general it is worth to introduce a definition of what is a correct logical rule and a complete logical rule.

Definition 1.25. Let Form denote the set of all formulae and $\text{Seq} = \text{Form}^{<\mathbb{N}} \times \text{Form}^{<\mathbb{N}}$ denote the set of all sequents (i.e. ordered pairs of finite sets of formulae (Γ, Δ)).

- An n -ary LK-rule is a map $R : \text{Seq}^n \rightarrow \text{Seq}$.
- An n -ary LK-rule R is correct if the following holds:

For all valuations v and $\langle (\Gamma_1, \Delta_1), \dots, (\Gamma_n, \Delta_n) \rangle$, if $v(\bigwedge \Gamma_i) \leq v(\bigvee \Delta_i)$ for all $i = 1, \dots, n$, we also have that $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$, where $(\Gamma, \Delta) = R(\langle (\Gamma_1, \Delta_1), \dots, (\Gamma_n, \Delta_n) \rangle)$.

- An n -ary LK-rule R is complete if the following holds:

For all valuations v and $\langle (\Gamma_1, \Delta_1), \dots, (\Gamma_n, \Delta_n) \rangle$, letting $(\Gamma, \Delta) = R(\langle (\Gamma_1, \Delta_1), \dots, (\Gamma_n, \Delta_n) \rangle)$, $v(\bigwedge \Gamma_i) \leq v(\bigvee \Delta_i)$ for all $i = 1, \dots, n$, whenever $v(\bigwedge \Gamma) \leq v(\bigvee \Delta)$.

Lemma 1.20 states that the structural LK-rules are correct and that the LK-logical rules are correct and complete. The above exercises provide further examples of correct and/or complete LK-rules.

2 Basics of first order logic

We start to define formulae and semantics for one of the simplest first order languages, a language which is already suited to express the basic properties of groups. First of all we need a piece of notation. Let us stick to the following convention:

Notation 2.1. A vocabulary V is a certain set of symbols: for example the set $V = \{ (,), \wedge, \neg, A, B, \rightarrow \}$ is a vocabulary. A string on V is a finite sequence of elements of V : for example the propositional formulae $(\neg(A \wedge B))$ and $(A \rightarrow ((\neg A) \wedge (\neg B)))$ are strings on the vocabulary V . An occurrence of a symbol u of V in a string s is any appearance of the symbol in the string. For example A occurs once in the third position in the string $(\neg(A \wedge B))$, and twice in the second and seventh position in the string $(A \rightarrow ((\neg A) \wedge (\neg B)))$. A substring of a given string s is any consecutive list of symbols of s , for example $\neg(A \wedge$ and $(A \wedge B)$ are both substrings of $(\neg(A \wedge B))$.

Any propositional formula ϕ is a string of symbols taken from the vocabulary $\{A_n : n \in \omega\} \cup \{ (,), \neg, \vee, \wedge, \rightarrow \}$.

The notion of *string* and that of *set* diverge: the notion of string forces us to pay attention not just to which symbols occur in it, but also on the relative position these symbols occupy in it. On the other hand a set is uniquely defined by its elements, and the order and the number of occurrences of an element inside a set does not matter: $\{a, b, c\} = \{a, c, b\} = \{a, a, b, c, b\}$ are three different descriptions of the unique set whose three elements are a, b, c ; while the strings $abc, acb, aabcb$ are pairwise distinct, though the symbols occurring in them are the same (those in the vocabulary $\{a, b, c\}$). Another example is given by the propositional formulae $(\neg(A \wedge B))$ and $((\neg A) \wedge (\neg B))$ which are distinct strings containing the same set of symbols $\{A, B, (,), \neg, \wedge\}$, their difference is made explicit by the different positions and the different number of occurrences each of the symbols in the above set has in each of the two strings.

2.1 Examples of first order languages

First example of a first order language

Definition 2.2. Let $\mathcal{L}_0 = \{*, \doteq\}$, and $\{x_n : n \in \mathbb{N}\}$ be an infinite set of variables.

The \mathcal{L}_0 -terms and \mathcal{L}_0 -formulae are defined as strings over the vocabulary

$$\{\wedge, \neg, \vee, \rightarrow, \forall, \exists, (,)\} \cup \mathcal{L}_0 \cup \{x_n : n \in \mathbb{N}\}$$

according to the following rules:

Terms: an \mathcal{L}_0 -term is a string defined as follows:

- each variable x_n is an \mathcal{L}_0 -term,
- if t, s are \mathcal{L}_0 -terms, also $(t * s)$ is an \mathcal{L}_0 -term,
- strings which cannot be obtained by finitely many repeated applications of the above two rules are not \mathcal{L}_0 -terms.

Formulae: an \mathcal{L}_0 -formula is a string defined as follows:

- if t, s are \mathcal{L}_0 -terms, $(t \doteq s)$ is an \mathcal{L}_0 -formula,
- if ϕ, ψ are \mathcal{L}_0 -formulae and x_i is a variable, also $(\neg\phi)$, $(\phi \wedge \psi)$, $(\phi \rightarrow \psi)$, $(\phi \vee \psi)$, $(\forall x_i \phi)$, $(\exists x_i \phi)$ are \mathcal{L}_0 -formulae.
- strings which cannot be obtained by finitely many repeated applications of the above two rules are not \mathcal{L}_0 -formulae.

The basic idea behind the above definition is the following: $*$ is a symbol representing a given binary operation on some set M , and the variables range over elements of M , an \mathcal{L} -term will denote a certain element of M which can be exactly determined using the operation denoted by $*$, once a definite value is assigned to the variables occurring in this term.

The simplest formulae are equations stating that a certain term is equal to another term, certain assignment of the variables can make an equation true, others can make the equation false.

By means of propositional connectives and quantifiers more complicated statements (other than equations) expressing the relations subsisting between different terms can be expressed: propositional connective can say something like the given equation is false (with a formula of type $\neg(s \doteq t)$), both equations are true (with a formula of type $(s \doteq t) \wedge (u \doteq v)$), at least one equation is true (with a formula of type $(s \doteq t) \vee (u \doteq v)$), or more complicated such statements which can be obtained by means of repeated use of propositional connectives over simpler formulae.

For what concerns quantifiers, for example a formula of type $\exists x(s \doteq t)$ holds true in M for a given assignment of the variables different from x occurring in the equation, if some element of M satisfies the equation when assigned to x , a formula of type $\forall x\phi$ holds true in M if all elements of M satisfy the property ϕ .

We now want to give a precise mathematical meaning to these vague observations.

Definition 2.3. Let M be a set and $\cdot_M : M^2 \rightarrow M$ be a binary operation on M . Fix $v : \text{var} \rightarrow M$ be a function. Given an \mathcal{L}_0 -term t , we define $v(t)$ as follows:

- $v(t) = v(x)$ if t is the variable x ,
- $v((u * s)) = v(u) \cdot_M v(s)$ if t is the term $(u * s)$.

Given an \mathcal{L}_0 -formula ϕ we define $(M, \cdot_M) \models \phi[v]$ as follows:

- $(M, \cdot_M) \models \phi[v]$ iff $v(t) = v(s)$ and ϕ is the formula $(t \doteq s)$,
- $(M, \cdot_M) \models \psi \wedge \theta[v]$ iff $(M, \cdot_M) \models \psi[v]$ and $(M, \cdot_M) \models \theta[v]$,
- $(M, \cdot_M) \models \psi \vee \theta[v]$ iff $(M, \cdot_M) \models \psi[v]$ or $(M, \cdot_M) \models \theta[v]$,
- $(M, \cdot_M) \models \neg\psi[v]$ iff $(M, \cdot_M) \not\models \psi[v]$,
- $(M, \cdot_M) \models \exists x\psi[v]$ iff $(M, \cdot_M) \models \psi[v_{x/b}]$ for some $b \in M$,
- $(M, \cdot_M) \models \forall x\psi[v]$ iff $(M, \cdot_M) \models \psi[v_{x/b}]$ for all $b \in M$,

where $v_{x/b}$ denotes the function $v' : \text{var} \rightarrow M$ such that $v'(y) = v(y)$ for all variables $y \neq x$ and $v'(x) = b$.

Let $\mathcal{M} = (M, \cdot_M)$, we say that ϕ holds in the \mathcal{L}_0 -structure \mathcal{M} for a valuation v or that the \mathcal{L}_0 -structure \mathcal{M} models (satisfies) ϕ with valuation v when it is the case that $\mathcal{M} \models \phi[v]$.

Example 2.4. Consider the \mathcal{L}_0 -structure $(\mathbb{Z}, +)$ and the function $v : \text{var} \rightarrow \mathbb{Z}$ such that $v(x) = 2$, $v(y) = 5$, $v(z) = 8$.

Let t be the \mathcal{L}_0 -term $(x * z)$, s be the \mathcal{L}_0 -term $(y * y)$, u be the \mathcal{L}_0 -term $((z * y) * z)$. Then

- $v(t) = v(x) + v(z) = 2 + 8 = 10$,
- $v(s) = v(y) + v(y) = 5 + 5 = 10$,
- $v(u) = v((z * y)) + v(z) = (v(z) + v(y)) + v(z) = (8 + 5) + 8 = 21$.

Hence:

$$(\mathbb{Z}, +) \models (t \doteq s)[v]$$

given that $v(t) = 10 = v(s)$.

$$(\mathbb{Z}, +) \not\models (t \doteq u)[v]$$

given that $v(t) = 10 \neq 21 = v(u)$. For what concerns quantifiers:

$$(\mathbb{Z}, +) \models (\exists y((y * y) \doteq ((z * y) * z)))[v]$$

Since:

$$(\mathbb{Z}, +) \models (\exists y((y * y) \doteq ((z * y) * z)))[v]$$

if and only if

$$(\mathbb{Z}, +) \models ((y * y) \doteq ((z * y) * z))[v_{y/n}] \text{ for some } n \in \mathbb{Z}$$

if and only if

$$v_{y/n}((y * y) \doteq ((z * y) * z)) \text{ for some } n \in \mathbb{Z}$$

if and only if

$$2n = v_{y/n}((y * y)) = v_{y/n}((z * y) * z) = n + 16$$

for some $n \in \mathbb{Z}$.

The latter equation $2n = n + 16$ is satisfied uniquely by $n = 16$. Hence

$$(\mathbb{Z}, +) \models ((y * y) \doteq ((z * y) * z))[v_{y/16}]$$

and 16 is the natural number n witnessing that

$$(\mathbb{Z}, +) \models (\exists y((y * y) \doteq ((z * y) * z)))[v].$$

On the other hand:

$$(\mathbb{Z}, +) \not\models (\forall y((y * y) \doteq ((z * y) * z)))[v]$$

Since:

$$(\mathbb{Z}, +) \models (\forall y((y * y) \doteq ((z * y) * z)))[v]$$

if and only if

$$(\mathbb{Z}, +) \models ((y * y) \doteq ((z * y) * z))[v_{y/n}] \text{ for all } n \in \mathbb{Z}$$

if and only if

$$v_{y/n}((y * y) \doteq ((z * y) * z)) \text{ for all } n \in \mathbb{Z}$$

if and only if

$$2n = v_{y/n}((y * y)) = v_{y/n}((z * y) * z) = n + 16$$

for all $n \in \mathbb{Z}$.

But the latter equation is not satisfied for $n \neq 16$, hence any $n \neq 16$ (for example $n = 3$) witnesses that

$$(\mathbb{Z}, +) \not\models (\forall y((y * y) \doteq ((z * y) * z)))[v],$$

given that (for example)

$$(\mathbb{Z}, +) \not\models ((y * y) \doteq ((z * y) * z))[v_{y/3}].$$

We adopt the following conventions:

Notation 2.5. We drop parenthesis when this will not generate confusion, hence we will write $t * s$ rather than $(t * s)$, $t \doteq s$ rather than $(t \doteq s)$, $\exists x\phi$ rather than $(\exists x\phi)$ and so on so forth. Parentheses will be kept when confusion on the priority of the connectives may occur as in $\exists x\phi \wedge \psi$ which could stand either for $(\exists x\phi) \wedge \psi$ or for $\exists x(\phi \wedge \psi)$, expressions which can have a very distinct meaning. Moreover for the sake of readability of formulae, we will feel free to use at times the parentheses $[,]$ in the place of $(,)$.

Here are some examples to appreciate the expressive power of this language:

Exercise 2.6. Find for each natural number n a formula ϕ_n such that an \mathcal{L}_0 structure (M, \cdot_M) satisfies ϕ_n with any valuation $v : \text{var} \rightarrow M$ if and only if M has at least n elements. (*HINT:* $\phi_1 \equiv \exists x(x \doteq x)$, $\phi_2 \equiv \exists x\exists y\neg(x \doteq y), \dots$).

We introduce the group axioms as the following formulae of the language \mathcal{L}_0 :

Associativity law:	$\forall x\forall y\forall z((x * y) * z) = (x * (y * z))$
Neutral element:	$\exists e\forall y(e * y \doteq y \wedge y * e \doteq e)$
Inverse:	$\exists e[\forall y(e * y \doteq y \wedge y * e \doteq e) \wedge \forall x\exists z(x * z = e \wedge z * x = e)]$

Exercise 2.7. Show the following:

- Choose your favourite group (G, \cdot_G) (for example $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbf{GL}_{2,2}(\mathbb{R}), \cdot)$ — the latter is the group of 2×2 matrix with real coefficients and non-zero determinant, with \cdot the multiplication of matrices) and show that the three formulae above hold in (G, \cdot_G) .
- Show that the first two formulae hold in $(\mathbb{N}, +)$, but the third fails (*HINT: the inverse of a positive natural number with respect to the sum is a negative integer number, which does not belong to \mathbb{N}*).
- Show that the first two formulae hold in $(\mathbf{GL}_{2,2}(\mathbb{Z}), \cdot)$, but the third fails (where $\mathbf{GL}_{2,2}(\mathbb{Z})$ is the family of 2×2 matrix with integer coefficients and non-zero determinant, with \cdot being the multiplication of matrices).
- Show that the

Commutativity law:	$\forall x\forall y(x * y = y * x)$
---------------------------	-------------------------------------

holds in $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, and fails in $(\mathbf{GL}_{2,2}(\mathbb{R}), \cdot)$.

It should be transparent to the reader who has gained familiarity with the semantics of \mathcal{L}_0 -formulae that:

- A structure (G, \cdot_G) with G a set and $\cdot_G : G^2 \rightarrow G$ a binary operation is a *group* if for any valuation $v : \text{var} \rightarrow G$

$$(G, \cdot_G) \models \mathbf{Associativity\ law} \wedge \mathbf{Inverse}[v]$$

and it is not a group otherwise.

- A structure (G, \cdot_G) with G a set and $\cdot_G : G^2 \rightarrow G$ a binary operation is a *commutative group* if for any valuation $v : \text{var} \rightarrow G$

$$(G, \cdot_G) \models \mathbf{Associativity\ law} \wedge \mathbf{Inverse} \wedge \mathbf{Commutativity\ law}[v]$$

Second example of a first language

It is somewhat inconvenient to express the existence of the inverse and of the neutral element for the group operation in the language $\{*, \doteq\}$. This leads us to expand our notion of first order language by introducing constant symbols and unary operation symbols. The expansion of the language allows to express in a simpler fashion the existence of a neutral element and of an inverse for the group operation.

Definition 2.8. Let $\mathcal{L}_1 = \{*, \doteq, I, e\}$. A string t is a \mathcal{L}_1 -term if:

- t is a variable x ,
- t is the constant symbol e ,
- $t = (s * u)$ with s, u \mathcal{L}_1 -terms,
- $t = I(s)$ with s an \mathcal{L}_1 -term.
- Strings which cannot be obtained by a finite number of applications of the above rules are not \mathcal{L}_1 -terms.

\mathcal{L}_1 formulae are built over \mathcal{L}_1 -terms by the same rules we used to define \mathcal{L} -formulae, i.e. the simplest formulae are equations of the form $(t \doteq s)$ with t, s \mathcal{L}_1 -terms; more complex formulae are built over these equations by means of quantifiers and logical connectives.

Definition 2.9. (G, \cdot_G, I_G, e_G) is an \mathcal{L}_1 -structure if

- $e_G \in G$,
- $\cdot_G : G^2 \rightarrow G$ is a binary operation,
- $I_G : G \rightarrow G$ is a unary operation.

Let $v : \text{var} \rightarrow G$, and t an \mathcal{L}_1 -term. We define $v(t)$ as follows:

- $v(t) = v(x)$ if t is the variable x .
- $v(t) = e_G$ if t is the constant symbol e .
- $v(t) = I_G(v(s))$ if t is the term $I(s)$.

- $v(t) = v(s) \cdot_G v(u)$ if t is the term $(s * u)$.

We define $(G, \cdot_G, I_G, e_G) \models \phi[v]$ according to the same rules we gave for \mathcal{L} -formulae, for any given \mathcal{L}_1 -formula ϕ .

We introduce the group axioms as the following formulae of the language \mathcal{L}_1 :

$$\begin{array}{ll} \textbf{Associativity law:} & \forall x \forall y \forall z ((x * y) * z) = (x * (y * z)) \\ \textbf{e is the neutral element:} & \forall y (e * y \doteq y \wedge y * e \doteq e) \\ \textbf{Inverse:} & \forall x (x * I(x) = e \wedge I(x) * x = e) \end{array}$$

Exercise 2.10. Let (G, \cdot_G, I_G, e_G) stands for one of the following structures:

- $(\mathbb{Z}, +, I_{\mathbb{Z}}, 0)$ with $I_{\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $n \mapsto -n$,
- $(\mathbb{Q}, +, I_{\mathbb{Q}}, 0)$, with $I_{\mathbb{Q}} : \mathbb{Q} \rightarrow \mathbb{Q}$ given by $q \mapsto -q$,
- $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \cdot, I_{\mathbb{R}}, 1)$, with $I_{\mathbb{R}} : \mathbb{R}^* \rightarrow \mathbb{R}^*$ given by $r \mapsto 1/r$,
- $(\mathbf{GL}_{2,2}(\mathbb{R}), \cdot, I, Id)$ with $I : \mathbf{GL}_{2,2}(\mathbb{R}) \rightarrow \mathbf{GL}_{2,2}(\mathbb{R})$ given by $A \mapsto A^{-1}$, and Id the identity matrix.

Show that for all $v : \text{var} \rightarrow G$

$$(G, \cdot_G, I_G, e_G) \models \textbf{Associativity law} \wedge \textbf{e is the neutral element} \wedge \textbf{Inverse}[v].$$

Show that $(\mathbb{Q}, \cdot, I', 1)$ with $I'(a) = 1/a$ if $a \neq 0$ and $I'(0) = 0$ does not satisfy neither that 1 is the neutral element of \cdot nor the existence of multiplicative inverses for all $a \in \mathbb{Q}$. (*HINT: 0 witnesses the failure that 1 is the neutral element for multiplication, moreover $0 \cdot I'(0) = 0 \neq 1$, hence $I(0)$ is not the inverse of 0 for \cdot .*)

We can define a structure (G, \cdot_G, I_G, e_G) to be a group with neutral element e_G and inverse operation I_G if and only if

$$(G, \cdot_G, I_G, e_G) \models \textbf{Associativity law} \wedge \textbf{e is the neutral element} \wedge \textbf{Inverse}[v]$$

for all $v : \text{var} \rightarrow G$.

Third example of a first order language

We introduce the last natural example of a first order language, so to be able to express the properties of fields and rings with an ordering:

Definition 2.11. Let $\mathcal{L}_2 = \{*, \oplus, \doteq, \leq, \bar{0}, \bar{1}\}$ with $\oplus, *$ symbols for binary operations, \doteq, \leq symbols for binary relations, $\bar{0}, \bar{1}$ constant symbols.

A string t is a \mathcal{L}_2 -term if:

- t is a variable x ,
- t is the constant symbol $\bar{0}$ or the constant symbol $\bar{1}$,
- $t = (s * u)$ with s, u \mathcal{L}_2 -terms,
- $t = (s \oplus u)$ with s \mathcal{L}_2 -terms.

- Strings which cannot be obtained by a finite number of applications of the above rules are not \mathcal{L}_2 -terms.

The atomic \mathcal{L}_2 -formulae are the following:

- $(s \leq u)$ with s, u \mathcal{L}_2 -terms,
- $(s \doteq u)$ with s, u \mathcal{L}_2 -terms.

The other \mathcal{L}_2 -formulae are defined over \mathcal{L}_2 -atomic formulae using propositional connectives and quantifiers.

Definition 2.12. A structure $(M, <_M, +_M, \cdot_M, 0_M, 1_M)$ is an \mathcal{L}_2 -structure if $<_M \subseteq M^2$ is a binary relation, $\cdot_M, +_M : M^2 \rightarrow M$ are binary operations, $0_M, 1_M \in M$.

Given $v : \text{var} \rightarrow M$, we extend v to a function defined on all \mathcal{L}_2 -terms as follows:

- $v(s * u) = v(s) \cdot_M v(u)$ for s, u \mathcal{L}_2 -terms,
- $v(s \oplus u) = v(s) +_M v(u)$ for s, u \mathcal{L}_2 -terms,
- $v(\bar{0}) = 0_M$,
- $v(\bar{1}) = 1_M$.

The \mathcal{L}_2 -semantics is defined as follows:

- $(M, <_M, +_M, \cdot_M, 0_M, 1_M) \models (s \leq u)[v]$ if and only if $v(s) <_M v(u)$ (equivalently $(v(s), v(u)) \in <_M$),
- $(M, <_M, +_M, \cdot_M, 0_M, 1_M) \models (s \doteq u)[v]$ if and only if $v(s) = v(u)$.
- The semantics of other \mathcal{L}_2 -formulae obeys the usual definition given for propositional connectives and quantifiers.

Exercise 2.13. Consider the structure $\mathcal{R} = (\mathbb{R}, \cdot, +, 0, 1, <)$ and the assignment \oplus to $+$, $*$ to \cdot , \doteq to the equality relation, \leq to the strict order relation $\{(a, b) \in \mathbb{R}^2 : a < b\} \subseteq \mathbb{R}^2$, $\bar{0}$ to 0, $\bar{1}$ to 1. With this assignment \mathcal{R} is an \mathcal{L}_2 -structure.

- Find \mathcal{L}_2 -formulae which express that $(\mathbb{R}, +, \cdot, 0, 1)$ is a field with 0 neutral element for the sum and 1 neutral element for the product on \mathbb{R}^* . I.e. find the natural counterpart as \mathcal{L}_2 -formulae of the axioms expressing in the semi-formal mathematical language we are accustomed to work with that $(\mathbb{R}^*, \cdot, 1)$ and $(\mathbb{R}, +, 0)$ are commutative groups and the usual distributivity properties of sum and product. (*CAUTION: to express that $(\mathbb{R}^*, \cdot, 1)$ is a group one has to specify that all non-zero elements of \mathbb{R} are invertible, this can be expressed by means of the formula $\forall x (\neg(x \doteq \bar{0}) \rightarrow \exists y (x * y \doteq \bar{1}))$).*)
- Find also \mathcal{L}_2 -formulae expressing that $<$ is a strict order relation on \mathbb{R}^2 , i.e. \mathcal{L}_2 -formulae formalizing in \mathcal{L}_2 that $<$ is an antireflexive, antisymmetric, transitive binary relation on \mathbb{R}^2 . Recall that a binary relation $R \subseteq \mathbb{R}^2$ is:
 - *antireflexive* if $\Delta = \{(a, a) : a \in \mathbb{R}\} \cap R = \emptyset$,
 - *antisymmetric* if at most one among (a, b) and (b, a) belongs to R for all $a, b \in \mathbb{R}$,

- *transitive* if for all $a, b, c \in \mathbb{R}$ such that $(a, b), (b, c) \in R$ we also have that $(a, c) \in R$.

- Check also that the formula

$$\forall x \forall y [x < y \leftrightarrow \exists z ((-\bar{0} \doteq z) \wedge x \oplus (z * z) \doteq y)]$$

holds in \mathcal{R} for any valuation $v : \text{var} \rightarrow \mathbb{R}$.

We define an \mathcal{L}_2 -structure \mathcal{M} to be an *ordered field* if it satisfies all the \mathcal{L}_2 -formulae in the above list we asked you to find.

We remark how certain familiar type of linguistic expressions we use in mathematics can be rendered in first order logic.

“All positive real number are the square of some other real number”.

We can express it in \mathcal{L}_2 as:

$$\forall x (\bar{0} < x \rightarrow \exists y (y * y \doteq \bar{0}))$$

“There exists a positive solution for the polynomial $x^2 - 1 = 0$ ”.

We can express it in \mathcal{L}_2 as:

$$\exists x (\bar{0} < x \wedge x * x \doteq \bar{1})$$

Actually it is possible to formalize any mathematical reasoning in first order logic. We are going to explore this at length in the sequel.

2.2 Syntax and semantics for arbitrary first order languages

We are now ready to define what is an arbitrary first order language and what is its natural semantic. The three examples above will be just special instantiation of this general definition.

Definition 2.14. A set

$$\mathcal{L} = \{\doteq\} \cup \{R_i : i \in I\} \cup \{f_j : j \in J\} \cup \{c_k : k \in K\}$$

is a first order signature, where R_i denotes a relation symbol of arity $n_i \in \mathbb{N}$ for each $i \in I$, each f_j denotes a function symbol of arity $n_j \in \mathbb{N}$ for each $j \in J$, each c_k denotes a constant symbol for each $k \in K$.

Fix $\{x_n : n \in \mathbb{N}\}$ infinite set of variables (disjoint from \mathcal{L}).

The \mathcal{L} -terms and \mathcal{L} -formulae are defined as strings over the vocabulary

$$\{\wedge, \neg, \vee, \rightarrow, \leftrightarrow, \forall, \exists, (,)\} \cup \{, \} \cup \mathcal{L} \cup \{x_n : n \in \mathbb{N}\}$$

according to the following rules:

Terms: An \mathcal{L} -term is a string defined as follows:

- each variable x_n is an \mathcal{L} -term,
- each constant symbol c_k for $k \in K$ is an \mathcal{L} -term,

- if t_1, \dots, t_{n_j} are \mathcal{L} -terms, and f_j is a function symbol of arity n_j , also $f_j(t_1, \dots, t_{n_j})$ is an \mathcal{L} -term, for each $j \in J$.
- Strings which cannot be obtained by finitely many repeated applications of the above rules are not \mathcal{L} -terms.

Formulae: An \mathcal{L} -formula is a string defined as follows:

- if t, s are \mathcal{L} -terms, $(t \doteq s)$ is an (atomic) \mathcal{L} -formula,
- if t_1, \dots, t_{n_i} are \mathcal{L} -terms and R_i is a relation symbol of arity n_i , also $R_i(t_1, \dots, t_{n_i})$ is an (atomic) \mathcal{L} -formula for each $i \in I$.
- if ϕ, ψ are \mathcal{L} -formulae and x is a variable, also $(\neg\phi)$, $(\phi \wedge \psi)$, $(\phi \rightarrow \psi)$, $(\phi \leftrightarrow \psi)$, $(\phi \vee \psi)$, $(\forall x\phi)$, $(\exists x\phi)$ are \mathcal{L} -formulae.
- Strings which cannot be obtained by finitely many repeated applications of the above rules are not \mathcal{L} -formulae.

Notation 2.15. A caveat is in order: we are used to use the infix notation for binary operation and relations, i.e. we are accustomed to write $x + y$ rather than $+(x, y)$ to denote the sum of x and y , also we are used to write $x R y$ rather than $R(x, y)$ to denote that x, y are in the binary relation R . However we match a problem with this type of notation when we are dealing with functions and relations which are not binary. For example if we want to define a ternary function $f : M^3 \rightarrow M$ defined on some set M , we are used to write $f(x, y, z)$ to denote the output of f on the input (x, y, z) , in this latter case we use a *prefix*-notation to describe the function f and its action on its inputs. It turns out that the prefix notation is best suited to describe in general arbitrary terms of a first order language. In particular if we choose \mathcal{L} to be $\mathcal{L}_0 = \{*\}$, according to the above definition of \mathcal{L} -terms, we would get that the \mathcal{L} -term t obtained applying $*$ to previously defined \mathcal{L} -terms s, u is $*(s, u)$ rather than $(s * u)$. This is due to the fact that in the above definition of \mathcal{L} -terms and atomic formulae, we decided to conform all the times (except for \doteq) to the conventions imposed by the adoption of a *prefix* notation.

Definition 2.16. Let

$$\mathcal{L} = \{\doteq\} \cup \{R_i : i \in I\} \cup \{f_j : j \in J\} \cup \{c_k : k \in K\}$$

be a first order signature

$$\mathcal{M} = (M, R_i^M : i \in I, f_j^M : j \in J, c_k^M : k \in K)$$

is an \mathcal{L} structure with domain M if

- $c_k^M \in M$ for each $k \in K$ and each constant symbol c_k ,
- $R_i^M \subseteq M^{n_i}$ for each relation symbol $R_i \in \mathcal{L}$ of arity n_i for each $i \in I$,
- $f_j^M : M^{n_j} \rightarrow M$ is a function for each function symbol $f_j \in \mathcal{L}$ of arity n_j for each $j \in J$.

Fix $v : \text{var} \rightarrow M$ be a function. Given an \mathcal{L} -term t , we define $v(t)$ as follows:

- $v(t) = v(x)$ if t is the variable x ,

- $v(c_k) = c_k^M$ for each constant symbol c_k ,
- $v(f_j(t_1, \dots, t_{n_j})) = f_j^M(v(t_1), \dots, v(t_{n_j}))$ for each function symbol f_j of arity n_j .

Given an \mathcal{L} -formula ϕ we define $\mathcal{M} \models \phi[v]$ as follows:

- $\mathcal{M} \models (t \doteq s)[v]$ iff $v(t) = v(s)$,
- $\mathcal{M} \models R_i(t_1, \dots, t_{n_i})[v]$ iff $R_i^M(v(t_1), \dots, v(t_{n_i}))$ holds (i.e. the n_i -tuple $(v(t_1), \dots, v(t_{n_i}))$ is in the relation $R_i^M \subseteq M^{n_i}$),
- $\mathcal{M} \models \psi \wedge \theta[v]$ iff $\mathcal{M} \models \psi[v]$ and $\mathcal{M} \models \theta[v]$,
- $\mathcal{M} \models \psi \vee \theta[v]$ iff $\mathcal{M} \models \psi[v]$ or $\mathcal{M} \models \theta[v]$,
- $\mathcal{M} \models \neg\psi[v]$ iff $\mathcal{M} \not\models \psi[v]$,
- $\mathcal{M} \models \psi \rightarrow \theta[v]$ iff $\mathcal{M} \models \neg\psi[v]$ or $\mathcal{M} \models \theta[v]$,
- $\mathcal{M} \models \psi \leftrightarrow \theta[v]$ iff $\mathcal{M} \models \psi \rightarrow \theta[v]$ and $\mathcal{M} \models \theta \rightarrow \psi[v]$,
- $\mathcal{M} \models \exists x\psi[v]$ iff $\mathcal{M} \models \psi[v_{x/b}]$ for some $b \in M$,
- $\mathcal{M} \models \forall x\psi[v]$ iff $\mathcal{M} \models \psi[v_{x/b}]$ for all $b \in M$,

where $v_{x/b}$ denotes the function $v' : \text{var} \rightarrow M$ such that $v'(y) = v(y)$ for all variables $y \neq x$ and $v'(x) = b$.

Exercise 2.17. Check that:

- \mathcal{L}_0 is the \mathcal{L} -language given by just one function symbol $*$ of arity 2 and no constant symbols and no relation symbols other than \doteq (which is a relation symbol of arity 2 and the unique one for which we conform to the infix notation).
- \mathcal{L}_1 is the \mathcal{L} -language given by one function symbol $*$ of arity 2, one function symbol I of arity 1, one constant symbols e and no relation symbols other than \doteq .
- \mathcal{L}_2 is the \mathcal{L} -language given by two function symbols $*$, \oplus of arity 2, two constant symbols $0, 1$, one relation symbol \leq of arity 2, and the relation symbol \doteq of arity 2.

Check also that modulo the reframing of the notion of term and atomic formula determined by the switch from the infix notation to the prefix notation, the \mathcal{L} -semantic defined above is the \mathcal{L}_i -semantic we previously defined for each of the signatures \mathcal{L}_i for $i = 0, 1, 2$.

Remark 2.18. Given an \mathcal{L} -structure \mathcal{M} with domain M and $v : \text{Var} \rightarrow M$, set

$$\begin{aligned} \bar{v} : \mathcal{L}\text{-Form} &\rightarrow \{0, 1\} \\ \phi &\mapsto 1 \text{ if and only if } \mathcal{M} \models \phi[v] \end{aligned}$$

Then:

- $\bar{v}(\phi \wedge \psi) = \min \{\bar{v}(\phi), \bar{v}(\psi)\}$,

- $\bar{v}(\phi \vee \psi) = \max \{\bar{v}(\phi), \bar{v}(\psi)\},$
- $\bar{v}(\phi \rightarrow \psi) = \max \{\neg \bar{v}(\phi), \bar{v}(\psi)\},$
- $\bar{v}(\neg \phi) = 1 - \bar{v}(\phi),$
- $\bar{v}(\exists x \phi) = \max \{\bar{v}_{x/a}(\phi) : a \in M\},$
- $\bar{v}(\forall x \phi) = \min \{\bar{v}_{x/a}(\phi) : a \in M\}.$

Hence the semantics just defined is the natural generalization of the semantics for propositional formulae.

We can, as in the case of propositional logic, introduce the notion of tautology, contradiction, and satisfiable formula:

Definition 2.19. Let \mathcal{L} be a first order signature and ϕ an \mathcal{L} -formula.

- ϕ is a *tautology* if for all \mathcal{L} -structures \mathcal{M} with domain M and all $v : \text{var} \rightarrow M$ we have that

$$\mathcal{M} \models \phi[v].$$

- ϕ is a *contradiction* if for all \mathcal{L} -structures \mathcal{M} with domain M and all $v : \text{var} \rightarrow M$ we have that

$$\mathcal{M} \not\models \phi[v].$$

- ϕ is *satisfiable* if for some \mathcal{L} -structure \mathcal{M} with domain M and some $v : \text{var} \rightarrow M$, we have that

$$\mathcal{M} \models \phi[v].$$

A theory T over \mathcal{L} is a family of \mathcal{L} -formulae. T is satisfiable if for some \mathcal{L} -structure \mathcal{M} with domain M and some $v : \text{var} \rightarrow M$, we have that

$$\mathcal{M} \models \phi[v]$$

for all $\phi \in T$.

Finally we introduce a key notion in our analysis of first order logic: that of logical consequence. This notion gives a mathematically rigorous definition of what is a theorem of a mathematical theory T .

We say that

$$\mathcal{M} \models T[v]$$

if and only if for all formulae $\phi \in T$

$$\mathcal{M} \models \phi[v].$$

If T is a theory such that some $\mathcal{M} \models T[v]$, we say that T is a satisfiable theory. Otherwise we say it is a contradictory theory.

Definition 2.20. Let \mathcal{L} be a first order signature.

Given an \mathcal{L} -structure \mathcal{M} with domain M , a valuation $v : \text{var} \rightarrow M$, and a theory T , We say that ϕ is a logical consequence of T , and write $T \models \phi$, if for all \mathcal{L} -structures \mathcal{M} with domain M , and all valuations $v : \text{var} \rightarrow M$, if

$$\mathcal{M} \models T[v],$$

then

$$\mathcal{M} \models \phi[v].$$

We write $\phi \models \psi$ to signify that $T \models \psi$ where $T = \{\phi\}$.

We say that ϕ and ψ are logically equivalent and write $\phi \equiv \psi$ if $\phi \models \psi$ and $\psi \models \phi$.

We also write $\phi \models_T \psi$ if $\{\phi\} \cup T \models \psi$ and $\phi \equiv_T \psi$ (ϕ and ψ are logically equivalent over the theory T) if $\phi \models_T \psi$ and $\psi \models_T \phi$.

The above definition captures our concept that a certain mathematical statement ϕ is a consequence of the axioms of the theory T , i.e. that there is a mathematical theorem stating that under assumptions T , the thesis ϕ holds. Let's give a concrete example:

Example 2.21. Let T be the theory of groups and ϕ states that there exists a unique neutral element, we know that ϕ is a consequence of T exactly because we are able to show that in any group there is exactly one neutral element. Now let us translate this into our formalism using the language \mathcal{L}_0 . The \mathcal{L}_0 -formula

$$\phi \equiv \forall u \forall z [(\forall y (u * y = y \wedge z * y = y)) \rightarrow u = z]$$

formalizes that any two neutral element for multiplication on the right are equal, i.e. that there can be at most one neutral element for multiplication on the right. ϕ is a logical consequence of the axioms of the theory of groups as formalized in the language \mathcal{L}_0 , i.e. **Associativity law** \wedge **Inverse**.

Exercise 2.22. Prove that

$$\mathbf{Associativity\ law} \wedge \mathbf{Inverse} \models \forall u \forall z [(\forall y (u * y = y \wedge z * y = y)) \rightarrow u = z]$$

holds.

Exercise 2.23. Show that the \mathcal{L}_0 -formulae $x * y = z$ and $y * x = z$ are logically equivalent over the theory $T = \{\mathbf{Commutativity\ law}\}$ but are inequivalent otherwise. (*HINT: to show that they are inequivalent in general, take the group $\mathbf{GL}_{2,2}(\mathbb{R})$ and three 2×2 -matrices A, B, C such that $A \cdot B = C \neq B \cdot A$ and consider an assignment $v : x \mapsto A, y \mapsto B, z \mapsto C$.)*

Exercise 2.24. Show that \equiv and \equiv_T are equivalence relations on the set of \mathcal{L} -formulae, i.e. that for all \mathcal{L} -formulae ϕ, ψ, θ :

- $\phi \equiv \phi$,
- $\phi \equiv \psi$ entails that $\psi \equiv \phi$,
- $\phi \equiv \psi$ and $\psi \equiv \theta$ entail that $\phi \equiv \theta$,

and that the same holds replacing \equiv with \equiv_T for any theory T .

(*HINT: To this aim it suffices to show that \models is a reflexive and transitive relation, and that the same occurs for \models_T for any theory T . Since the symmetry of \equiv and \equiv_T comes for free from the fact that $\phi \equiv \psi$ iff $\phi \models \psi \models \phi$ ($\phi \equiv_T \psi$ iff $\phi \models_T \psi \models_T \phi$).*)

We are interested to analyze \mathcal{L} -formulae up to \equiv or \equiv_T . For example in commutative groups it is irrelevant for us to study the equations $x * y = z$ or the equation $y * x = z$, since the two are expressing the same concept (if we assume the commutativity of the operation $*$). In general, we will proceed as follows in the analysis of a mathematical theory T (for example T could be the theory of groups):

- We look for a first order language \mathcal{L} in which we are able to express the axioms of T as \mathcal{L} -formulae.
- We then try to analyze whether a certain property of the structures satisfying these axioms (in our case groups) can be expressed by means of a \mathcal{L} -formula ϕ .
- In the case this is possible, we can freely choose which among the many \mathcal{L} -formulae ψ which are logically equivalent to ϕ is more convenient to be used for our analysis of the property described by ϕ .

For this reason it is good to sort out the basic properties of the equivalence relation \equiv and \equiv_T and of the relation of logical consequence \models . This is what we propose to do in the sequel.

Exercise 2.25. Let \times be a binary connective and Q one among the symbols \exists, \forall . Prove that

$$\phi_0 \times \psi_0 \equiv \phi_1 \times \psi_1$$

if $\phi_0 \equiv \phi_1$ and $\psi_0 \equiv \psi_1$. Prove that $\phi \equiv \psi$ if and only if $\neg\phi \equiv \neg\psi$. Prove also that

$$Qx\phi \equiv Qx\psi$$

if $\phi \equiv \psi$.

Remark 2.26. The same does not hold for any theory T if in all the above expressions we replace \equiv by \equiv_T . The problem occurs for example in case $\phi \equiv_T \psi$ with $T = \{(x \doteq e)\}$ with a constant function symbol, ϕ being $(x \doteq e)$ and ψ being $(x \doteq x)$. Then any $\mathcal{L} = \{e\}$ -structure $\mathcal{M} \models \psi[v]$ and any structure \mathcal{M} with a valuation v of T such that $\mathcal{M} \models T[v]$ (i.e. v is such that $v(x) = e^{\mathcal{M}}$) is also such that $\mathcal{M} \models \phi[v]$. On the other hand if \mathcal{M} , the domain of \mathcal{M} , has at least two elements, we have that $\mathcal{M} \models \forall x(x \doteq x)[v]$ and $\mathcal{M} \not\models \forall x(x \doteq e)[v]$. The problem does not arise if T is made up just of sentences (i.e. formulae without free variables). But we need first to define what are these sentences, i.e. what are the free variables of a formula. This will be done in the next section.

Exercise 2.27. Show that there is some theory T such that $\phi \equiv_T \psi$ but $\exists x\phi \not\equiv_T \exists x\psi$.

2.3 Free and bounded variables and substitution of symbols inside formulae: what are the problems to match?

To proceed in our analysis of the semantic of first order logic and of the notion of logical consequence, we need to introduce some technical definition which will simplify some of our computations regarding formulae and their semantic.

The following basic examples based on our practice with integration outline all the kind of problems we can encounter in manipulating first order formulae. Consider the following function:

$$f(u) = \int_0^1 (y \cdot u) dy$$

Even though y appears in the expression of $f(u)$, in order to compute $f(u)$ we do not need to assign a value to y , i.e. y is a bounded variable in the above expression

and f is a function just of the variable u and not of the variable y . Exactly in the same way, y is bounded in $\exists y(y * y = x)$: in order to compute whether

$$(\mathbb{N}, +) \models \exists y(y * y = x)[v]$$

holds for some valuation $v : \text{var} \rightarrow \mathbb{N}$, we just need to see whether $v(x)$ is an even or an odd number.

$$(\mathbb{N}, +) \models \exists y(y * y = x)[v]$$

holds if and only if $v(x)$ is even. In particular the assignment of v to variables different from x (in particular to the quantified variable y) is irrelevant in the computation of the validity or not of the expression

$$(\mathbb{N}, +) \models \exists y(y * y = x)[v].$$

So our first observation is:

Observation (1): *The validity of an expression of type*

$$\mathcal{M} \models \phi[v]$$

depends only on the assignment v gives to the non-bounded variables occurring in the string ϕ .

Now let us come back to the expression

$$f(u) = \int_0^1 (y \cdot u) dy$$

We can change all occurrences of y with any other variable different from u without changing the meaning of $f(u)$:

$$f(u) = \int_0^1 (y \cdot u) dy = \int_0^1 (z \cdot u) dz.$$

But if we replace y with u we change the meaning of the expression:

$$f(u) = u/2 = \int_0^1 (y \cdot u) dy \neq \int_0^1 (u \cdot u) du = 1/3.$$

Similarly in the structure $(\mathbb{N}, +)$, the formulae $\exists y(y * y = x)$ and $\exists z(z * z = x)$ are two equivalent expressions which are true when x is assigned to an even number, but $\exists x(x * x = x)$ is a different kind of statement which is always true in $(\mathbb{N}, +)$ (for 0 is a number witnessing the truth of $\exists x(x * x = x)$ according to our semantic). So our second observation is:

Observation (2): *In a formula ϕ we can replace safely all occurrences of a variable y which are bounded by a quantifier of the form $\exists y$ or $\forall y$ by any other variable z , provided that z is a variable never occurring in ϕ .*

Finally it is often the case that in the expression

$$f(u) = \int_0^1 (y \cdot u) dy = \int_0^1 (z \cdot u) dz,$$

u is a shorthand for some other expression, for example u could be a function of x, z i.e. $u = g(x, z)$. In certain type of computation it is convenient for us to treat $g(x, z)$ as a variable u and manipulate the expression $\int_0^1 (y \cdot u) dy$, and at a certain point replace u with $g(x, z)$ in our expression. This is feasible and correct, provided that u is not a function of the variable y (which is bounded by the differential sign dy in the expression $\int_0^1 (y \cdot u) dy$). For example let $g(z, w) = \frac{1}{z \cdot w}$, then letting $u = g(z, w)$:

$$f(u) = \int_0^1 (y \cdot u) dy = \int_0^1 \frac{y}{z \cdot w} dy = \frac{1}{2(z \cdot w)}.$$

On the other hand if we used the expression

$$f(u) = \int_0^1 (z \cdot u) dz,$$

which we saw to represent equally well the function $f(u)$ as the expression

$$f(u) = \int_0^1 z u dz,$$

and we substitute $g(z, w)$ in the place of u , we would get

$$f(u) = \int_0^1 (z \cdot u) dz = \int_0^1 \frac{z}{z \cdot w} dz = \frac{1}{w} \neq \frac{1}{2(z \cdot w)}.$$

It is clear that we should consider this second expression the wrong one, since in the process of substituting u with $g(z, w)$ we transformed the free variable z in a bound variable: our final expression is not a function of two variables z, w as it should be, but just of one variable w . Similarly if we substitute $(z * w)$ to x in $\exists y(y * y = x)$, we get the expression $\exists y(y * y = z * w)$, which is true in $(\mathbb{N}, +)$ if $z * w$ is assigned to an even number, but if we replace $(z * w)$ to x in $\exists z(z * z = x)$, we get the expression $\exists z(z * z = z * w)$, which is true in $(\mathbb{N}, +)$ for any assignment of w to a natural number. In particular the first substitution shows that the formula $\exists y(y * y = z * w)$ predicates of the term $z * w$ the same properties the formula $\exists y(y * y = x)$ predicates of the variable x , while the formula $\exists z(z * z = z * w)$ has significantly changed the situation, and it is now a property just of the variable w , and not of the variables w, z . This leads to our third observation:

Observation (3): *In a formula ϕ we can safely replace a non-bounded variable of ϕ by some other term, provided the term we consider do not have variables which falls under the scope of a quantifier in ϕ .*

Finally observe that $\int_0^1 \int_0^1 (y * x) dy dz = \int_0^1 (y * x) dy$, i.e. the integral in dz does not affect at all the meaning of the expression $\int_0^1 (y * x) dy$. Similarly one can check that $\exists z(\exists y(y * y = x))$ and $\exists y(y * y = x)$ are logically equivalent. Hence our fourth observation is:

Observation (4): *Quantifying with a variable z never occurring in a formula ϕ , does not change the meaning of ϕ .*

We need to make these observations rigorous mathematical properties of first order logic. So we define the notion of free and bounded occurrence of a variable inside a formula and then formulate the relevant facts which express these observations in a rigorous mathematical form.

2.4 Syntactic complexity of terms and formulae

In the following we will make proofs by induction on the complexity of a term or of a formula, hence we must define a measure of complexity for such objects, and also give the right terminology to manipulate them.

Definition 2.28. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$ be a first order language.

- Let t be a \mathcal{L} -term; the tree $T(t)$ associated to t is defined as follows:
 - $T(t) = t$ if t is a variable x or a constant symbol c_k .
 - Assume $t = f_j(t_1, \dots, t_{n_j})$ and $T(t_i)$ has been defined for $i = 1, \dots, n_j$. Then $T(t)$ is the tree:

$$\frac{T(t_1) \quad \dots \quad T(t_{n_j})}{t}$$

- Let ϕ be a \mathcal{L} -formula; ϕ is atomic if it is of the form $(t \doteq s)$ with t, s \mathcal{L} -terms or of the form $R_i(t_1, \dots, t_{n_i})$, with $R_i \in I$ a relation symbol of \mathcal{L} of ariety n_i and t_1, \dots, t_{n_i} \mathcal{L} -terms.

The tree $T(\phi)$ associated to ϕ is defined as follows:

- $T(\phi) = \phi$ if ϕ is atomic.
- Assume ϕ is $(\theta \square \psi)$ with $\square \in \{\forall, \wedge, \rightarrow\}$ and $T(\theta), T(\psi)$ have been defined. Then $T(\phi)$ is the tree:

$$\frac{T(\theta) \quad T(\psi)}{\phi}$$

- Assume ϕ is $(\neg\psi)$ or $(\forall\psi)$ or $(\exists\psi)$. Then $T(\phi)$ is the tree:

$$\frac{T(\psi)}{\phi}$$

- The complexity of a formula ϕ or of a term t is the height of the associated tree.
- The subformulae of ϕ are all the formulae appearing in some node of $T(\phi)$. $\text{subfm}(\phi)$ is the set of subformulae of ϕ .

For example the \mathcal{L}_0 -formula ϕ :

$$(\exists x_3((\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_2(x_1 \doteq x_2)))))$$

has as $T(\phi)$ the tree

$$\frac{\frac{\frac{(x_1 * x_2) \doteq x_0}{(\forall x_1((x_1 * x_2) \doteq x_0))} \quad \frac{\frac{(x_1 \doteq x_2)}{(\exists x_2(x_1 \doteq x_2))} \quad (\neg(\exists x_2(x_1 \doteq x_2)))}{(\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_2(x_1 \doteq x_2)))}}{\phi}$$

The complexity of ϕ is 4, and its set of subformulae is the following set of substrings of ϕ :

$$\text{subfm}(\phi) = \{\phi, ((\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_0(x_1 \doteq x_2))))), \\ (\forall x_1((x_1 * x_2) \doteq x_0)), (\neg(\exists x_2(x_1 \doteq x_2))), ((x_1 * x_2) \doteq x_0), (\exists x_2(x_1 \doteq x_2)), (x_1 \doteq x_2)\}$$

Observe for example that the symbol x_1 occurs thrice in ϕ in the 6-th, 9-th, and 24-th positions (starting to count from 0 from left to right i.e. letting the 0-th symbol of the string ϕ being its leftmost symbol — the parenthesis (— and enumerating step by step from left to right, till we reach the rightmost symbol — the parenthesis) — placed in the 31-st position.

From now on along this section it will be convenient to be extremely cautious in our description of strings, hence we adopt the following terminology:

Notation 2.29. We identify a string ϕ with a function $s_\phi : n_\phi = \{0, \dots, n-1\} \rightarrow \mathcal{L}_0$ (where with \mathcal{L}_0 we intend in this context the set of possible symbols which can occur in some \mathcal{L}_0 -formula) and which associates to each the number $j < n$ the symbol occurring in the j -th position of ϕ (starting to count from 0 from left to right). Each element of a string ϕ can be uniquely identified by a pair $\langle k, S \rangle$ where S denotes the symbol occurring in position k along the string, i.e. $\langle k, S \rangle$ is the occurrence in position k of the symbol S in ϕ if and only if $s_\phi(k) = S$.

For example take the \mathcal{L}_0 -formula ϕ :

$$(\exists x_3((\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_2(x_1 \doteq x_2)))))$$

For this formula:

- $n_\phi = 32$
- $s_\phi : 32 \rightarrow \mathcal{L}_0$
- $s_\phi(0) = ($
- $s_\phi(31) =)$
- $s_\phi(6) = s_\phi(9) = s_\phi(24) = x_1$
- the occurrences of x_1 in ϕ are the pairs $\langle 6, x_1 \rangle, \langle 9, x_1 \rangle, \langle 24, x_1 \rangle$.

2.5 Free and bounded variables of a formula

We are now ready to define precisely what are the free and bounded variable in a formula.

Definition 2.30. Let \mathcal{L} be a first order signature.

- Let t be an \mathcal{L} -term. The variables occurring in t are the variables which occurs in at least some place in the string t . We write $t(x_1, \dots, x_n)$ to denote that the variables occurring in t are all among the set of variables $\{x_1, \dots, x_n\}$.
- Given a formula ϕ , let us identify ϕ with the sequence $s_\phi : n \rightarrow \mathcal{L}$ which enumerates the elements of the string ϕ . Let $Q = s_\phi(k)$ be a quantifier symbol (i.e. one among \forall, \exists) occurring in the string ϕ .

- A. The scope of the occurrence $\langle k, Q \rangle$ of the quantifier symbol Q is the unique substring $\psi_{k,Q} = s_\phi(k-1)Q \dots s_\phi(l)$ of ϕ such that $\psi_{k,Q}$ is a subformula of³ ϕ .
 - B. An occurrence $\langle j, x \rangle$ of the variable $x = s_\phi(j)$ in ϕ is *under the scope* of the occurrence $\langle k, Q \rangle$ of the quantifier symbol Q if it belongs to the string $\psi_{k,Q}$ and⁴ $s_\phi(k+1) = x$.
 - C. An occurrence of the variable x in ϕ is *bounded* by the occurrence of the quantifier symbol $Q = s_\phi(k)$ in ϕ if it is under the scope of $\langle k, Q \rangle$, and for no $j > m > k$ x is under the scope of the occurrence $\langle m, Q' \rangle$ of some quantifier symbol $Q' = s_\phi(m)$.
 - D. An occurrence of the variable x in ϕ is *free* if it is not under the scope of any occurrence of a quantifier symbol in ϕ .
- We will write $\phi(x_1, \dots, x_n)$ to denote that all occurrences of variables in the formula ϕ which are free belong to the set of variables $\{x_1, \dots, x_n\}$ (we do not exclude the case that there could be some variables among x_1, \dots, x_n which do not occur free in ϕ , or some occurrences of x_j which occur free in ϕ and some other occurrences of x_j which occur bounded in ϕ)
 - We say that ϕ is a closed formula or a sentence if (as a string) none of the variables occurring in it is free.

Example 2.31. In the formula

$$\phi \equiv (\exists x_3((\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_2(x_1 \doteq x_2))))) ,$$

the first occurrence of x_1 in the 6-th position of ϕ is bounded by $\langle 5, \forall \rangle$, the second occurrence of x_1 in the 9-th position is bounded by $\langle 5, \forall \rangle$ (in both cases $\psi_{5,\forall}$ is the subformula $(\forall x_1((x_1 * x_2) \doteq x_0))$ of ϕ); the third occurrence of x_1 in the 24-th position of ϕ is free. The first occurrence of x_2 in the 11-th position is free, while the second in the 22-nd position and the third in the 26-th position are bounded (this is witnessed by the subformula $\psi_{21,\exists}$ of ϕ given by $(\exists x_2(x_1 \doteq x_2))$).

The free variables of ϕ are $\{x_0, x_1, x_2\}$. Any set of variables $X \supseteq \{x_0, x_1, x_2\}$ is such that ϕ contains all occurrences of its free variables in the set X .

The requirement (C) in the definition of bounded occurrence of a variable is set up to rule which among the quantifier under whose scope the occurrence of

³In order to understand the scope of a quantifier in a formula ϕ , we must be able to pair a left-side parenthesis (occurring in ϕ with the corresponding rightside parenthesis) occurring in ϕ . For example if a quantifier symbol Q occurring in the formula ϕ is $s_\phi(k)$, we need to know which) symbol is paired to the parenthesis $s_\phi(k-1) = ($. Here is an algorithm to compute which $j > k$ is such that $s_\phi(j) =)$ is paired with $s_\phi(k-1)$: start a counter with 1 at $s_\phi(k-1) = ($ and, proceeding rightward on the string s_ϕ , increase the counter by 1 at position l if $s_\phi(l) = ($ and decrease it by 1 at position l whenever $s_\phi(l) =)$. When the counter reaches 0 in position j we get that $s_\phi(j) =)$ is the parenthesis coupled with $s_\phi(k-1) = ($. For example in

$$\phi := (\exists x_3((\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_2(x_1 \doteq x_2)))))$$

we want to know the scope of $s_\phi(6) = \forall$: we let the counter start with 1 at $s_\phi(5) = ($ and, proceeding rightward, the counter gets value 2 at position 8, value 3 at position 9, value 2 at position 13, value 1 at position 16 and value 0 at position 17. Hence the scope of $\langle 6, \forall \rangle$ is the substring of ϕ starting in $s_\phi(5)$ and finishing in $s_\phi(17)$ i.e. the sub-formula of ϕ given by $(\forall x_1((x_1 * x_2) \doteq x_0))$.

⁴Here $j > k+1$ is well possible and often the case, see the example below for clarifications!!

the variable falls is really binding the variable. For example consider the following formula:

$$(\exists x(\forall x(x * x \doteq y)))$$

In this case it is correct to argue that the most external quantifier $\exists x$ does not bound any occurrence of the variable x in the formula $(x * x \doteq y)$, since these occurrences of the variable x are already under the scope of the quantifier $\forall x$. (C) grants that this is indeed the case.

Remark 2.32. The semantics we have given to formulae has the property that any formula ϕ is logically equivalent to (i.e. it has the same meaning of) a formula ϕ' with the property that no variable can occur in some place of ϕ' as bounded and in some other place as free, for example:

$$\phi \equiv (\exists x_3((\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_0(x_1 \doteq x_2))))) ,$$

and

$$\phi' \equiv (\exists x_3((\forall x_4((x_4 * x_2) \doteq x_0)) \wedge (\neg(\exists x_5(x_1 \doteq x_2))))) ,$$

can be shown to be logically equivalent. Observe that in ϕ' no variable can occur in distinct places of the formula as free or bounded and there are no two occurrence of quantifier symbols which are followed by the same variable. We will come back on this point later on.

The following fact gives a rigorous mathematical formulation of our first observation:

Fact 2.33. *Let ϕ be an \mathcal{L} -formula with free variables among x_1, \dots, x_n , $\mathcal{M} = (M, \dots)$ be an \mathcal{L} -structure and $v, v' : \text{var} \rightarrow M$ be two distinct valuations. Assume $v(x_i) = v'(x_i)$ for all $i = 1, \dots, n$. Then*

$$\mathcal{M} \models \phi[v] \text{ if and only if } \mathcal{M} \models \phi[v'].$$

I.e. the validity of a formula ϕ under a valuation v in a structure \mathcal{M} depend just on the assignment v gives to the free variables of ϕ .

Proof. The proof is by induction on the logical complexity of ϕ . If ϕ is atomic, then the fact is almost self-evident. If ϕ is a boolean combination of ψ, θ by means of a propositional connective, than the fact is also easily established. The delicate case is when ϕ is of the form $Qx\psi$ with Q among \exists, \forall , but we won't enter the details of the argument in this case. \square

The following exercise should convince you that the above fact indeed is true:

Exercise 2.34. Check that the fact is easily proved for atomic formulae, for example check that

$$(M, \cdot) \models x * y \doteq z[v]$$

if and only if

$$(M, \cdot) \models x * y \doteq z[v']$$

whenever v, v' agree on x, y, z .

For more complex formulae, try to prove the fact for the formula

$$\phi = (\forall x_1(x_1 * x_2 \doteq x_0)) \wedge (\neg(\exists x_2(x_1 \doteq x_2))),$$

i.e. for any \mathcal{L}_0 -structure (M, \cdot) and valuations v, v' which agree on the values assigned to x_0, x_1, x_2 (which are the free variables occurring in ϕ)

$$(M, \cdot) \models \phi[v]$$

if and only if

$$(M, \cdot) \models \phi[v'].$$

The following fact gives a rigorous mathematical formulation of our fourth observation:

Fact 2.35. *Assume x does not occur free in ϕ . Then*

$$\exists x\phi \equiv \forall x\phi \equiv \phi.$$

Proof. Notice that $\exists x\phi$ and ϕ have the same free variables. Notice also that

$$\mathcal{M} = (M, \dots) \models \exists x\phi[v]$$

if and only if for some $b \in M$

$$\mathcal{M} \models \phi[v_{x/b}]$$

Since x does not occur free in ϕ we get that

$$\mathcal{M} \models \phi[v_{x/b}]$$

if and only if

$$\mathcal{M} \models \phi[v]$$

given that v and $v_{x/b}$ agree on all free variables of ϕ . Hence the thesis. \square

Exercise 2.36. Complete the proof of the above fact for the case $\forall x\phi$.

Notation 2.37. Given a string s on a vocabulary V and some $x, y \in V$, we denote by $s[x/y]$ the string t obtained from s systematically replacing the symbol x with the symbol y . For example let $s = abbbccmab$, $s[a/b] = bbbbccmbb$, $s[a/e] = ebbbccmab$. Given s a string and t a substring of s , we also let $s[a/b \upharpoonright t]$ denote the string obtained from s replacing a with b just on the occurrences of a which are in t .

For example if $s = abbbccmab$ and $t = bbccma$, $s[a/b \upharpoonright t] = abbbccmbb$.

The following fact gives a rigorous mathematical formulation of our second observation. We will not prove it, but we will use it in several occasions:

Fact 2.38. *Let ϕ be an \mathcal{L} -formula and y a variable never occurring in the string ϕ . Let $\theta = (\exists x\psi)$ be a subformula of ϕ . Then $\phi[x/y \upharpoonright \theta] \equiv \phi$.*

The following provides an example to convince you why the above fact is true:

Exercise 2.39. Prove that the string ϕ

$$(\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\exists x_2(x_1 \doteq x_2)))$$

is logically equivalent to the string ψ

$$(\forall y((y * x_2) \doteq x_0)) \wedge (\neg(\exists z(x_1 \doteq z))).$$

Notice that $\psi = \phi[x_1/y \upharpoonright (\forall x_1((x_1 * x_2) \doteq x_0))][x_2/z \upharpoonright (\exists x_2(x_1 \doteq x_2))]$.

Proof. It is enough to prove that $(\forall x_1((x_1 * x_2) \dot{=} x_0)) \equiv (\forall y((y * x_2) \dot{=} x_0))$ and that $(\neg(\exists x_2(x_1 \dot{=} x_2))) \equiv (\neg(\exists z(x_1 \dot{=} z)))$, and then appeal to the fact that $\phi_0 \equiv \psi_0$ and $\phi_1 \equiv \psi_1$ entail that $\phi_0 \wedge \phi_1 \equiv \psi_0 \wedge \psi_1$.

So let us prove that

$$(\forall x_1((x_1 * x_2) \dot{=} x_0)) \equiv (\forall y((y * x_2) \dot{=} x_0)).$$

For any structure $\mathcal{M} = (M, \cdot_M)$ and valuation $v : \text{var} \rightarrow M$, we have that

$$\mathcal{M} \models \forall x_1((x_1 * x_2) \dot{=} x_0)[v]$$

if and only if for all $a \in M$ we have that

$$\mathcal{M} \models (x_1 * x_2) \dot{=} x_0[v_{x_1/a}].$$

Now consider the formula $(y * x_2) \dot{=} x_0$. Take the valuation v' such that $v'(x_0) = v(x_0)$, $v'(x_2) = v(x_2)$ and $v'(y) = v(x_1)$.

Observe that $v'(y) \cdot v'(x_2) = v(x_1) \cdot v(x_2)$ and $v'(x_0) = v(x_0)$. Hence $v'(y) \cdot v'(x_2) = v'(x_0)$ if and only if $v(x_1) \cdot v(x_2) = v(x_0)$.

Assume

$$\mathcal{M} \models \forall x_1(x_1 * x_2 \dot{=} x_0)[v].$$

Then for all $a \in M$ we have that

$$\mathcal{M} \models x_1 * x_2 \dot{=} x_0[v_{x_1/a}].$$

Hence for all $a \in M$

$$\mathcal{M} \models y * x_2 \dot{=} x_0[v'_{y/a}].$$

We conclude that

$$\mathcal{M} \models \forall y(y * x_2 \dot{=} x_0)[v'].$$

But now observe that $v'(x_0) = v(x_0)$ and $v'(x_2) = v(x_2)$, and x_0, x_2 are the only free variables in $\forall y(y * x_2) \dot{=} x_0$. Hence we get that

$$\mathcal{M} \models \forall y(y * x_2 \dot{=} x_0)[v].$$

In particular we have shown that if

$$\mathcal{M} \models \forall x_1(x_1 * x_2 \dot{=} x_0)[v],$$

then

$$\mathcal{M} \models \forall y(y * x_2 \dot{=} x_0)[v].$$

We can repeat verbatim the same argument switching in all places y with x_1 and x_1 with y to get that if

$$\mathcal{M} \models \forall y(y * x_2 \dot{=} x_0)[v],$$

then

$$\mathcal{M} \models \forall x_1(x_1 * x_2 \dot{=} x_0)[v].$$

Since the above argument is independent of the choice of \mathcal{M} and v , we proved that

$$(\forall x_1((x_1 * x_2) \dot{=} x_0)) \equiv (\forall y((y * x_2) \dot{=} x_0)).$$

We leave to the reader to prove that $(\neg(\exists x_2(x_1 \dot{=} x_2))) \equiv (\neg(\exists z(x_1 \dot{=} z)))$ along the same lines, so to complete the exercise. \square

Definition 2.40. Given an \mathcal{L} -formula $\phi(x_1, \dots, x_n)$ with free variables x_1, \dots, x_n its universal closure is $\forall x_1 \dots \forall x_n \phi(x_1, \dots, x_n)$ and its existential closure is $\exists x_1 \dots \exists x_n \phi(x_1, \dots, x_n)$.

We denote by $\forall\phi$ (respectively $\exists\phi$) the universal (existential) closure of ϕ .

Fact 2.41. An \mathcal{L} -formula $\phi(x_1, \dots, x_n)$ is a tautology if and only if its universal closure is and is satisfiable if and only if its existential closure is.

Exercise 2.42. Prove the fact.

Exercise 2.43. Let ϕ be an \mathcal{L} -formula and T an \mathcal{L} theory made up just of sentences. Prove the following:

1. $\mathcal{M} \models T[v]$ if and only if $\mathcal{M} \models T[v']$ for all valuations v, v' with target the domain of \mathcal{M} .
2. $T \models \phi$ if and only if $T \models \forall\phi$.
3. $T \cup \{\phi\}$ is satisfiable if and only if $T \cup \{\exists\phi\}$ is.
4. Prove exercise 2.25 for \equiv_T .

2.6 Basic rules for logic equivalence and prenex normal forms of formulae

We are now ready to prove the basic logical equivalences:

Fact 2.44. We have the following for all formulae ϕ, ψ :

- $\exists x(\phi \vee \psi) \equiv (\exists x\phi) \vee (\exists x\psi)$,
- $\forall x(\phi \wedge \psi) \equiv (\forall x\phi) \wedge (\forall x\psi)$,
- $\forall x\neg\phi \equiv \neg\exists x\phi$,
- $\exists x\neg\phi \equiv \neg\forall x\phi$,
- $\exists x(\phi \wedge \psi) \equiv \phi \wedge (\exists x\psi)$ if x does not occur free in ϕ .
- $\forall x(\phi \vee \psi) \equiv \phi \vee (\forall x\psi)$ if x does not occur free in ϕ .
- $\exists x(\phi \rightarrow \psi) \equiv \phi \rightarrow (\exists x\psi)$ if x does not occur free in ϕ .
- $\forall x(\phi \rightarrow \psi) \equiv \phi \rightarrow (\forall x\psi)$ if x does not occur free in ϕ .
- $\forall x(\phi \rightarrow \psi) \equiv (\exists x\phi) \rightarrow \psi$ if x does not occur free in ψ .
- $\exists x(\phi \rightarrow \psi) \equiv (\forall x\phi) \rightarrow \psi$ if x does not occur free in ψ .

Proof. The first four are left completely to the reader. We prove in detail the fifth and leave the remaining as an exercise to the reader. To prove the first four use the same strategy based on an analysis of the definition of \equiv of the fifth below, for the remaining it is worth to use what has already been proved about \equiv in the first five items above, in combination with the results of exercise 2.25, the logical equivalence $\phi \rightarrow \psi \equiv \neg\phi \vee \psi$, and the De Morgan laws $\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi$, $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$.

We must show that

$$\exists x(\phi \wedge \psi) \equiv \phi \wedge (\exists x\psi)$$

if x does not occur free in ϕ . Choose a structure $\mathcal{M} = (M, \cdot)$ and a valuation $v : \text{var} \rightarrow M$ such that

$$\mathcal{M} \models \exists x(\phi \wedge \psi)[v].$$

This occurs if for some $a \in M$

$$\mathcal{M} \models \phi \wedge \psi[v_{x/a}]$$

which is the case if and only if

$$\mathcal{M} \models \phi[v_{x/a}]$$

and

$$\mathcal{M} \models \psi[v_{x/a}].$$

This gives that

$$\mathcal{M} \models \phi[v_{x/a}]$$

and

$$\mathcal{M} \models \exists x\psi[v].$$

Since x does not occur free in ϕ we have that

$$\mathcal{M} \models \phi[v_{x/a}]$$

if and only if

$$\mathcal{M} \models \phi[v]$$

since v and $v_{x/a}$ differ just on the value assigned to x which is not free in ϕ . Hence we get that

$$\mathcal{M} \models \phi[v]$$

and also that

$$\mathcal{M} \models \exists x\psi[v],$$

from which we can infer

$$\mathcal{M} \models \phi \wedge \exists x\psi[v].$$

Since this argument is independent of the choice of \mathcal{M}, v , we proved that

$$\exists x(\phi \wedge \psi) \models \phi \wedge \exists x\psi.$$

For the converse assume

$$\mathcal{M} \models \phi \wedge \exists x\psi[v].$$

Then

$$\mathcal{M} \models \phi[v]$$

and

$$\mathcal{M} \models \exists x\psi[v].$$

This gives that for some $a \in M$

$$\mathcal{M} \models \psi[v_{x/a}]$$

and

$$\mathcal{M} \models \phi[v].$$

Since x does not occurs free in ϕ we have that

$$\mathcal{M} \models \phi[v_{x/a}]$$

if and only if

$$\mathcal{M} \models \phi[v]$$

since v and $v_{x/a}$ differ just on the value assigned to x which is not free in ϕ . Hence we get that

$$\mathcal{M} \models \phi[v_{x/a}]$$

and also that

$$\mathcal{M} \models \psi[v_{x/a}],$$

from which we can infer

$$\mathcal{M} \models \phi \wedge \psi[v_{x/a}].$$

This a thus witnesses that

$$\mathcal{M} \models \exists x(\phi \wedge \psi)[v].$$

Since this argument is independent of the choice of \mathcal{M}, v we proved that

$$\phi \wedge \exists x\psi \models \exists x(\phi \wedge \psi).$$

□

With these equivalences at hand, we can now prove the existence of canonical representative in the equivalence class of a formula:

Definition 2.45. An \mathcal{L} -formula ϕ is in prenex normal form if ϕ is of the form $Q_1x_1 \dots Q_nx_n\psi$ with each Q_i a symbol among \forall, \exists and ψ a quantifier free formula.

Theorem 2.46. Every formula ϕ is equivalent to a formula ψ in prenex normal form.

Proof. SKETCH: We use the above equivalence to systematically pull quantifiers out of subformulae of ϕ . For example if ϕ is $\theta \wedge \exists x\psi$ we pick y variable never occurring neither in θ nor in ψ . Then $\phi \equiv \theta \wedge \exists y(\psi[x/y])$ and by the above equivalences (since y does not occur free in θ), we get that $\phi \equiv \exists y(\theta \wedge \psi[x/y])$. Repeating this procedure for all binary connectives occurring in ϕ and using the equivalences $\neg\exists x\psi \equiv \forall x\neg\psi$, $\neg\forall x\psi \equiv \exists x\neg\psi$, after finitely many steps we find a formula $\psi \equiv \phi$ in prenex normal form. □

Exercise 2.47. Choose an \mathcal{L}_0 -formula ϕ with at least four quantifiers and six logical connectives and find a $\psi \equiv \phi$ in prenex normal form.

Fact 2.48. Every formula ϕ is logically equivalent to a formula in which only the boolean connectives \wedge, \neg and the quantifier \exists appear.

Proof. Proceed by induction on the logical complexity of ϕ to remove the occurrences of $\vee, \forall, \rightarrow, \leftrightarrow$ using the De Morgan laws $\psi \vee \theta \equiv \neg(\neg\psi \wedge \neg\theta)$ and $\forall x\phi \equiv \neg\exists x\neg\phi$. □

2.7 Substitution of terms inside formulae

We now want to define a general procedure to substitute a free variable by a term inside a formula and thus give a rigorous mathematical form to our third observation.

Definition 2.49. Let \mathcal{L} be a first order signature and $\phi(x_1, \dots, x_n)$ a formula with free variables among $\{x_1, \dots, x_n\}$ $t_j(y_1, \dots, y_{k_j})$ terms with free variables among $\{y_1, \dots, y_{k_j}\}$ for $j = 1, \dots, n$.

We define $\phi[x_1/t_1, \dots, x_n/t_n]$ by the following procedure:

- By means of repeated applications of Fact 2.38 we replace all the occurrences of bounded variables inside ϕ with new variables never in the set

$$X = \{x_1, \dots, x_n\} \cup \bigcup_{j=1, \dots, n} \{y_1, \dots, y_{k_j}\}.$$

By Fact 2.38, we obtain a formula $\phi' \equiv \phi$ with the same free variables and such that all the quantifiers of ϕ' quantify on distinct variables which are not in X .

- We let $\phi[x_1/t_1, \dots, x_n/t_n]$ be the string obtained replacing each occurrence of x_i in ϕ' with the string t_i .

Example 2.50. Let us consider the following example: $\phi(x_0, x_1, x_2)$ is the formula

$$(\exists x_3((\forall x_1((x_1 * x_2) \doteq x_0)) \wedge (\neg(\forall x_2(x_1 \doteq x_2)))))$$

$t_0 = x_1 * x_2$, $t_1 = (x_0 * x_0) * x_1$, $t_2 = x_3 * (x_2 * x_1)$. We choose variables y, z, w and we change ϕ to the formula

$$\psi = \phi[x_3/y][x_1/z \upharpoonright (\forall x_1((x_1 * x_2) \doteq x_0))][x_2/w \upharpoonright (\forall x_2(x_1 \doteq x_2))].$$

We get that ψ is the formula

$$(\exists y((\forall z((z * x_2) \doteq x_0)) \wedge (\neg(\forall w(x_1 \doteq w)))))$$

Now we substitute the terms t_i in the occurrences of the variables x_i in ψ (which are all free) to get $\phi[x_0/t_0, x_1/t_1, x_2/t_2]$:

$$(\exists y((\forall z((z * (x_3 * (x_2 * x_1))) \doteq x_1 * x_2)) \wedge (\neg(\forall w((x_0 * x_0) * x_1 \doteq w)))))$$

Fact 2.51. Let \mathcal{L} be a first order signature and $\phi(x_1, \dots, x_n)$ a formula with free variables among $\{x_1, \dots, x_n\}$, $t_j(y_1, \dots, y_{k_j})$ terms with free variables among $\{y_1, \dots, y_{k_j}\}$ for $j = 1, \dots, n$. Let \mathcal{M} be an \mathcal{L} -structure with domain M , and $v, v' : \text{var} \rightarrow M$ be valuations.

Assume $v(x_j) = v'(t_j)$ for all $j = 1, \dots, n$. Then

$$\mathcal{M} \models \phi(x_1, \dots, x_n)[v]$$

if and only if

$$\mathcal{M} \models \phi[x_1/t_1, \dots, x_n/t_n][v'].$$

We don't prove the fact but we give an example to explain why this holds:

Example 2.52. Consider again the formula $\phi(x_0, x_1, x_2)$ of the previous example and the substitution of its free variables by the same terms. Let $\mathcal{M} = (\mathbb{N}, +)$ and $v(x_0) = v(x_2) = 0, v(x_1) = 9$. We leave to the reader to check that

$$(\mathbb{N}, +) \models (\exists x_3((\forall x_1((x_1 * x_2) \dot{=} x_0)) \wedge (\neg(\forall x_2(x_1 \dot{=} x_2)))))[v],$$

This is the case since the outer quantifier $\exists x_3$ is irrelevant, and of the two conjuncts $(\forall x_1((x_1 * x_2) \dot{=} x_0))$, $\neg(\forall x_2(x_1 \dot{=} x_2))$, the first is true since $n \cdot 0 = 0$ for all natural numbers n , and the second is true because any number different from 9 can be used to witness that

$$(\mathbb{N}, +) \models \forall x_2(x_1 \dot{=} x_2)[v]$$

does not hold.

After the substitution of x_i with t_i inside ϕ we have the formula

$$(\exists y((\forall z((z * (x_3 * (x_2 * x_1))) \dot{=} x_1 * x_2)) \wedge (\neg(\forall w((x_0 * x_0) * x_1 \dot{=} w)))))).$$

Let $v'(x_0) = v'(x_1) = 3, v'(x_3) = 2$, and $v'(x_2) = 0$. Then:

- $v'(t_0) = v'(x_1 * x_2) = 3 \cdot 0 = 0 = v(x_0)$,
- $v'(t_1) = v'((x_0 * x_0) * x_1) = 9 = v(x_1)$,
- $v'(t_2) = v'(x_3 * (x_2 * x_1)) = 0 = v(x_2)$.

We leave to the reader to check that

$$(\mathbb{N}, +) \models (\exists y((\forall z((z * (x_3 * (x_2 * x_1))) \dot{=} x_1 * x_2)) \wedge (\neg(\forall w((x_0 * x_0) * x_1 \dot{=} w)))))[v'].$$

This witnesses the truth of the fact in this particular instance.

2.8 Geometric interpretation of formulae

Much in the same fashion as one draws the set of solutions of a (dis)equation in two variables as a subset of the plane, one can do the same kind of representations for the set of tuples satisfying some first order formulae with some valuation. Here is how:

Definition 2.53. Let \mathcal{L} be a first order signature, \mathcal{M} an \mathcal{L} -structure with domain M , $\phi(x_1, \dots, x_n)$ an \mathcal{L} -formula with all the free variables occurring in ϕ among x_1, \dots, x_n . We define the following subset of M^n :

$$T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}} = \{(a_1, \dots, a_n) \in M^n : \mathcal{M} \models \phi[v_{x_1/a_1, \dots, x_n/a_n}]\}.$$

Example 2.54. Take the language \mathcal{L}_2 and the structure $\mathcal{R} = (\mathbb{R}, \cdot, *, <, 0, 1)$. The curve $y = 1/x$ in the plane \mathbb{R}^2 can be described as

$$T_{\phi(x, y)}^{\mathcal{R}} = \{(a_1, a_2) \in \mathbb{R}^2 : \mathcal{R} \models \phi[v_{x/a_1, y/a_2}]\}$$

where $\phi(x, y) = (y * x) \dot{=} x\bar{1}$.

More generally one can prove that every polynomial with coefficients in \mathbb{N} can be described by an \mathcal{L}_2 -term (see the exercise below). Sets of solutions of equations and disequations in rational coefficients can also be described by means of \mathcal{L}_2 -formulae. The above example for the equation $y = 1/x$ is a simple illustration of this fact.

Remark 2.55. It is crucial when defining the sets $T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}}$ to specify, not only the formula and the structure, but also the set (or more importantly the number) of distinct free variables x_1, \dots, x_n one aims to consider. This last information specifies the dimension of the space M^n of whom $T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}}$ is going to be a subset. For example for ϕ being $\exists z(z \oplus \bar{1} \doteq x\bar{0} \wedge (y * x) \oplus z \doteq x\bar{0})$

$$T_{\phi(x,y)}^{\mathcal{R}} = \{(a_1, a_2) \in \mathbb{R}^2 : \mathcal{R} \models \phi[v_{x/a_1, y/a_2}]\}$$

is a subset of the plane \mathbb{R}^2 (of dimension one as an algebraic variety), but

$$T_{\phi(x,y,z)}^{\mathcal{R}} = \{(a_1, a_2, a_3) \in \mathbb{R}^3 : \mathcal{R} \models \phi[v_{x/a_1, y/a_2, z/a_3}]\}$$

is a (two dimensional) subset of \mathbb{R}^3 (obtained by a translation along the z -axis of the curve $y = 1/x$).

Exercise 2.56. Show that for any polynomial $p(x)$ with coefficients in \mathbb{N} , there is an \mathcal{L}_2 -term $t(x)$ such that $v_{x/a}(t) = p(a)$ for all real numbers a and valuations $v : \text{var} \rightarrow \mathbb{R}$, and conversely. (*HINT: proceed by induction on the degree n of the polynomial. Let $p(x) = \sum_{i=0}^{n+1} a_i x^i$, and assume that for all polynomial of degree n one can find the required term $t(x)$. Let $q(x) = \sum_{i=0}^n a_i x^i$ and $s(x)$ the term such that $v_{x/a}(s) = q(a)$ for all real numbers a and all valuations v . Now let $t(x) = s(x) \oplus (\bar{1} \oplus \dots \oplus \bar{1})(x * \dots * x)$ with the appropriate numbers of repetitions of the strings $\bar{1} \oplus$ and $x *$. Check that this works. For the converse assume that $t(x) = (s * u)$ and that there are such polynomials $q(x)$ for $s(x)$ and $r(x)$ for $u(x)$. Let $p(x) = s(x) \cdot r(x)$ and check that it works).*

More generally show that for any polynomial $p(x_1, \dots, x_n)$ with coefficients in \mathbb{N} , there is an \mathcal{L}_2 -term $t(x_1, \dots, x_n)$ such that for all real numbers a_1, \dots, a_n $v_{x_1/a_1, \dots, x_n/a_n}(t) = p(a_1, \dots, a_n)$ and conversely.

Even more generally prove that for any polynomial in integer or even rational coefficients $p(x_1, \dots, x_n)$ there are terms $t_1(x_1, \dots, x_n), t_2(x_1, \dots, x_n)$ such that for every n -tuple of real numbers (a_1, \dots, a_n) and real number a we have that $p(a_1, \dots, a_n) = a$ if and only if $v_{x_1/a_1, \dots, x_n/a_n}(t_1) = v_{x_1/a_1, \dots, x_n/a_n}(t_2) + a$ (*HINT: start with the case $n = 1$ and $a = 0$ and look at the example of the hyperbole given above and to what has been done to handle the case of polynomial with coefficients in the natural numbers*).

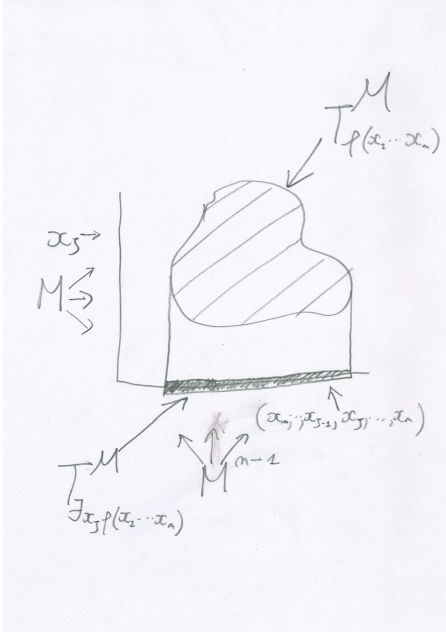
Fact 2.57. *The following holds for any \mathcal{L} -structure \mathcal{M} with domain M and any \mathcal{M} -formula ϕ, ψ with free variables among x_1, \dots, x_n :*

- $T_{\phi \wedge \psi(x_1, \dots, x_n)}^{\mathcal{M}} = T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}} \cap T_{\psi(x_1, \dots, x_n)}^{\mathcal{M}}$,
- $T_{\phi \vee \psi(x_1, \dots, x_n)}^{\mathcal{M}} = T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}} \cup T_{\psi(x_1, \dots, x_n)}^{\mathcal{M}}$,
- $T_{\neg \phi(x_1, \dots, x_n)}^{\mathcal{M}} = M^n \setminus T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}}$,
- $T_{\exists x_j \phi(x_1, \dots, x_n)}^{\mathcal{M}} = \pi_j[T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}}]$ where $\pi_j : M^n \rightarrow M^{n-1}$ is defined by $(a_1, \dots, a_n) \mapsto (a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n)$.

Proof. The proof of all but the last item are left to the reader. For the last item: Assume $(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) \in T_{\exists x_j \phi(x_1, \dots, x_n)}^{\mathcal{M}}$, then

$$\mathcal{M} \models \exists x_j \phi[v_{x_1/a_1, \dots, x_{j-1}/a_{j-1}, x_{j+1}/a_{j+1}, \dots, x_n/a_n}]$$

Figure 1: Existential quantification and projection maps



which occurs if and only if for some $a \in M$

$$\mathcal{M} \models \phi[v_{x_1/a_1, \dots, x_{j-1}/a_{j-1}, x_j/a, x_{j+1}/a_{j+1}, \dots, x_n/a_n]$$

giving that

$$(a_1, \dots, a_{j-1}, a, a_{j+1}, \dots, a_n) \in T^{\mathcal{M}}_{\phi(x_1, \dots, x_n)}.$$

Now observe that

$$\pi_j(a_1, \dots, a_{j-1}, a, a_{j+1}, \dots, a_n) = (a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n),$$

hence

$$(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) \in \pi_j[T^{\mathcal{M}}_{\phi(x_1, \dots, x_n)}].$$

Since $(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n)$ was chosen arbitrarily in $T^{\mathcal{M}}_{\exists x_j \phi(x_1, \dots, x_n)}$, we conclude that

$$T^{\mathcal{M}}_{\exists x_j \phi(x_1, \dots, x_n)} \subseteq \pi_j[T^{\mathcal{M}}_{\phi(x_1, \dots, x_n)}].$$

We leave the proof of the converse inclusion to the reader. \square

Exercise 2.58. Express $T^{\mathcal{M}}_{\forall x_j \phi(x_1, \dots, x_n)}$ in terms of $T^{\mathcal{M}}_{\phi(x_1, \dots, x_n)}$ using the projection maps, and the set theoretic operation of complementation.

Exercise 2.59. Fix a first order signature \mathcal{L} . Show that

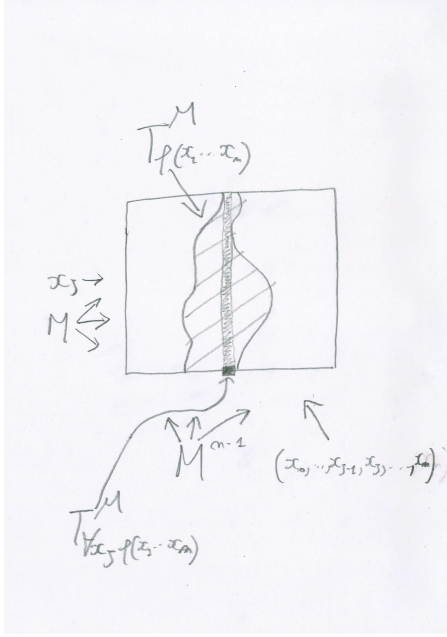
- ϕ is satisfiable if and only if we can find some $n > 0$, some set x_1, \dots, x_n containing the free variables of ϕ , and an \mathcal{L} -structure \mathcal{M} such that

$$T^{\mathcal{M}}_{\phi(x_1, \dots, x_n)} \neq \emptyset.$$

- ϕ is a tautology if and only if we can find some $n > 0$, and some set x_1, \dots, x_n containing the free variables of ϕ such that for all \mathcal{L} -structures \mathcal{M} with domain M we have that

$$T^{\mathcal{M}}_{\phi(x_1, \dots, x_n)} = M^n.$$

Figure 2: Universal quantification and its sections



- ϕ is a contradiction if and only if we can find some $n > 0$, and some set x_1, \dots, x_n containing the free variables of ϕ such that for all \mathcal{L} -structures \mathcal{M} we have that

$$T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}} = \emptyset.$$

Exercise 2.60. Fix a first order signature \mathcal{L} . Show that for all \mathcal{L} -formulae ϕ, ψ we have that $\phi \models \psi$ if and only if we can find some $n > 0$ and some set x_1, \dots, x_n containing the free variables of ϕ, ψ such that for all \mathcal{L} -structure \mathcal{M}

$$T_{\phi(x_1, \dots, x_n)}^{\mathcal{M}} \subseteq T_{\psi(x_1, \dots, x_n)}^{\mathcal{M}}.$$

2.9 Definable sets with and without parameters

In many cases we are interested in sets which needs some arguments not expressible in a first order language to be defined. For example we want to study the set of solutions of equations and disequations on real numbers for which the coefficients of the relevant polynomials are neither rational, nor even solutions of polynomial equations. It is hard to imagine how to express these coefficients by means of closed terms, or even of formulae in the language $\mathcal{L} = \{\cdot, +, 0, 1, <, =\}$. In most cases it is even impossible to talk about them (for example it can be proved that the number π is such that for no formula $\phi(x)$ in one free variable in the language $\mathcal{L} = \{\cdot, +, 0, 1, <, =\}$ $\langle \mathbb{R}, \cdot, +, 0, 1, <, = \rangle \models \phi(x)[x/a]$ if and only if $a = \pi$; the same holds for e). Nonetheless we want to be able to freely use all real numbers in our analysis of the structure $\langle \mathbb{R}, \cdot, +, 0, 1, <, = \rangle$, not just the ones obtained as the interpretation of some closed term v or as the unique number c such that for some $\phi(x)$ in free variable x , $\langle \mathbb{R}, \cdot, +, 0, 1, <, = \rangle \models \phi(x)[x/a]$ if and only if $a = c$.

This leads us to the notion of parameter and of subset of a structure $\mathcal{M} = \langle M, \dots \rangle$ definable with parameters.

Definition 2.61. Let \mathcal{L} be a first order signature, \mathcal{M} be an \mathcal{L} -structure with domain M , $b_1, \dots, b_n \in M$, and $\phi(x_1, \dots, x_k, y_1, \dots, y_n)$ be an \mathcal{L} -formula with displayed free variables.

$$T_{\phi(x_1, \dots, x_k, y_1, \dots, y_n), \langle b_1, \dots, b_n \rangle}^{\mathcal{M}} = \{ \langle a_1, \dots, a_k \rangle \in M^k : \mathcal{M} \models \phi(x_1, \dots, x_k, y_1, \dots, y_n)[x_i/a_i, y_j/b_j] \}.$$

- $A \subseteq M^k$ is \mathcal{M} -definable with parameters $b_1, \dots, b_n \in M$ if for some $\phi(x_1, \dots, x_k, y_1, \dots, y_n)$ \mathcal{L} -formula with displayed free variables we have that

$$A = T_{\phi(x_1, \dots, x_k, y_1, \dots, y_n), \langle b_1, \dots, b_n \rangle}^{\mathcal{M}}.$$

- $A \subseteq M^k$ is \mathcal{M} -definable without parameters if for some $\phi(x_1, \dots, x_k)$ \mathcal{L} -formula with displayed free variables we have that

$$A = T_{\phi(x_1, \dots, x_k)}^{\mathcal{M}}.$$

- $a \in M$ is \mathcal{M} -definable (with parameters $b_1, \dots, b_n \in M$) if $\{a\}$ is definable (with parameters $b_1, \dots, b_n \in M$).

Example 2.62. Here are a few examples:

- The interval $(-\pi; e)$ is \mathcal{R} -definable in parameters π, e where $\mathcal{R} = \langle \mathbb{R}, <, +, 0 \rangle$ by the formula $\phi := (0 < y_0 + x) \wedge (x < y_1)$.
- Each natural number n is definable in the structure $(\mathbb{N}, +, \cdot)$ (without parameters): 0 is definable using the formula $\forall z(z + x = z)$; 1 using the formula $\phi_1(x) := \forall z(z \cdot x = z)$; given the formula $\phi_n(x)$ defining n we let

$$\phi_{n+1}(x) := \exists z \exists w (\phi_n(x) \llbracket x/z \rrbracket \wedge \phi_1(x) \llbracket x/w \rrbracket \wedge x = z + w).$$

Exercise 2.63. Show the following:

- For any structure \mathcal{M} with domain M all finite and cofinite (i.e. of the form $M \setminus X$ with X finite subset of M) subsets of M are \mathcal{M} -definable with parameters.
- All finite and cofinite sets $A \subseteq \mathbb{N}$ are $(\mathbb{N}, +, \cdot)$ -definable without parameters.
- The set of solutions of any finite set of polynomial equations and disequations with real coefficients is $(\mathbb{R}, +, \cdot, 0, 1, <)$ -definable with parameters.

Predicates, functions, and constants definable in a structure

Given an \mathcal{L} -structure \mathcal{M} with domain M , it is often the case that certain functions $f : M^k \rightarrow M$, elements $c \in M$, and predicates $R \subseteq M^n$ are \mathcal{M} -definable with (or without) parameters from M . To increase the readability of formulae which talks about properties of these \mathcal{M} -definable objects, it is often convenient to expand \mathcal{L} with symbols which can denote these objects (i.e. a new function symbol \bar{f} of arity k to denote the definable function $f : M^k \rightarrow M$, a new relation constant symbol \bar{c} to denote the definable element $c \in M$, a new relation symbol \bar{R} of arity n to denote the definable relation $R \subseteq M^n$). In this case we enrich the relevant theory of which \mathcal{M} is a model by sentences in the new language which explain the meaning of the new symbols added to the language by means of their defining properties in the original language. The following example should clarify what we mean:

Example 2.64. Consider the \mathcal{L} -model $(\mathbb{R}, +, \cdot)$ for the language $\mathcal{L} = \{\oplus, \otimes\}$. Then 0 is definable by the formula $\phi_0(x) := \forall y(y \otimes x \dot{=} x)$, 1 is definable by the formula $\phi_1(x) := \forall y(y \otimes x \dot{=} y)$, the order relation $a \leq b$ is definable by the formula $\phi_{\leq}(x, y) := \exists z[x \oplus (z \otimes z) \dot{=} y]$, the successor operation $a \mapsto a + 1$ is definable by the formula $\phi_S(x, y) := \exists z[\phi_1(x) \llbracket x/z \rrbracket \wedge y \dot{=} x \oplus z]$.

We expand the language \mathcal{L} adding the binary relation symbol \prec , the function symbol \bar{S} and the constant symbols $\bar{0}, \bar{1}$. The axioms

- $\psi_0 := \phi_0(x) \llbracket x/\bar{0} \rrbracket$,
- $\psi_1 := \phi_1(x) \llbracket x/\bar{1} \rrbracket$,
- $\psi_2 := \forall x \forall y[(x \prec y) \leftrightarrow \phi_{\leq}(x, y)]$,
- $\psi_3 := \forall x \phi_S(x, \bar{S}(x))$.

provide the definitions of these properties and force their interpretation to be the desired one in \mathbb{R} , i.e. if we ask that $(\mathbb{R}, +, \cdot, c_0, c_1, \leq^*, S^*)$ is a model of ψ_j for $j = 0, \dots, 3$, it must be the case that S^* is the successor operation $a \mapsto a + 1$, $c_0 = 0$, $c_1 = 1$, \leq^* is the usual order relation on \mathbb{R} .

One advantage of doing so is that many properties of \mathbb{R} which required complex formulae to be formalized in \mathcal{L} are now simply expressible in $\langle \mathbb{R}, +, \cdot, 0, 1, \leq \rangle$; consider for example the property that holds of $a, b \in \mathbb{R}$ if and only if $b = a + 3$. Write down an \mathcal{L} -formula $\phi(x, y)$ which holds for a, b if and only if $a + 3 = b$ and compare it with the \mathcal{L}' -formula $y = \bar{S}(\bar{S}(\bar{S}(x)))$.

The following fact is trivial but must be checked, the proof goes by induction on the complexity of formulae and is left to the reader:

Fact 2.65. *Let*

$$\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$$

and

$$\mathcal{L}' = \mathcal{L} \cup \{S_i : i \in I', h_j : j \in J', d_k : k \in K'\}$$

be two first order languages.

Assume ϕ is an \mathcal{L} -sentence and

$$\mathcal{M}' = \langle M, R_i^{\mathcal{M}'} : i \in I, f_j^{\mathcal{M}'} : j \in J, c_k^{\mathcal{M}'} : k \in K, S_i^{\mathcal{M}'} : i \in I', h_j^{\mathcal{M}'} : j \in J', d_k^{\mathcal{M}'} : k \in K' \rangle$$

is an \mathcal{L}' -structure such that $\mathcal{M}' \models \phi$. Let

$$\mathcal{M} = \langle M, R_i^{\mathcal{M}'} : i \in I, f_j^{\mathcal{M}'} : j \in J, c_k^{\mathcal{M}'} : k \in K \rangle.$$

Then \mathcal{M} is an \mathcal{L} -structure and models ϕ as well.

2.10 Exercises on first order logic

Here is a list of exercises on first order logic:

- Consider the following LK-rule for the elimination of the universal quantifier:

$$\frac{\Gamma \vdash \forall x \phi(x, x_1, \dots, x_n), \Delta}{\Gamma \vdash \phi(x, x_1, \dots, x_n) \llbracket x/t \rrbracket, \Delta} \text{ (\forall-elimination)}$$

for a term t .

Show that Lemma 1.21 holds for the above rule.

More generally: take the logical rules of Section 15.5, Definition 15.21 of the notes of Berarducci linked on the Moodle page of the course, and prove that Lemma 1.21 holds for all these rules.

- Take the set of notes on logic of prof. Andretta available on the Moodle page of this course and do some among the exercises: 3.55, 3.56, 3.57, 3.58, 3.59, 3.63, 3.64, 3.65, 3.66 ((i)*, (iii)**), 3.67 ((vi)*), 3.68 ((ii)*), 3.69, 3.70, 3.71 ((ii)*, (iii)**). (* means the exercise is difficult, ** means the exercise is even more difficult....)

3 More on first order logic

We now start a deeper analysis of what can be done by means of first order logic. In particular we outline how first order logic provides:

- a fully satisfactory mathematical formulation of the notion of theorem and of proof (by means of the completeness theorem);
- the right framework to generalize the notions of algebraic structures and morphism between them, while tying their algebraic properties to syntactic properties of the first order axioms used to define them;
- a variety of “exotic” algebraic structures (by means of the compactness theorem).

3.1 First order LK-calculus

We add to the LK-rules for propositional logic rules which reflect in our calculus the logical meaning of quantifiers and axioms which incorporate the properties of the symbol \doteq for equality:

Definition 3.1. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$ be a first order signature with R_i a relation symbol of arity n_i for $i \in I$ and f_j a function symbol of arity n_j for $j \in J$.

The axioms of the LK-calculus for \mathcal{L} are:

- $\phi \vdash \phi$ for ϕ an \mathcal{L} -formula,
- $\vdash t \doteq t$ for all \mathcal{L} -terms t ,
- $t \doteq s \vdash s \doteq t$ for all \mathcal{L} -terms s, t ,
- $s \doteq t, t \doteq u \vdash s \doteq u$ for all \mathcal{L} -terms s, t, u ,
- $x_1 \doteq t_1, \dots, x_{n_j} \doteq t_{n_j} \vdash f_j(x_1, \dots, x_{n_j}) \doteq f_j(t_1, \dots, t_{n_j})$ for all variables x_1, \dots, x_{n_j} and \mathcal{L} -terms t_1, \dots, t_{n_j} ,

- $x_1 \doteq t_1, \dots, x_n \doteq t_n, \phi \vdash \phi[x_1/t_1, \dots, x_n/t_n]$ for all variables x_1, \dots, x_n , \mathcal{L} -terms t_1, \dots, t_n , \mathcal{L} -formulae ϕ .

Let Γ, Δ be finite sets of \mathcal{L} -formulae. The rules of LK-calcul for \mathcal{L} are the ones already introduced for propositional logic (see Def.1.15) and the following rules for quantifiers:

$$\frac{\Gamma \vdash \phi[x/t], \Delta}{\Gamma \vdash \exists x\phi, \Delta} (\exists\text{-R})$$

$$\frac{\Gamma, \phi[x/t] \vdash \Delta}{\Gamma, \forall x\phi \vdash \Delta} (\forall\text{-L})$$

$$\frac{\Gamma, \phi \vdash \Delta}{\Gamma, \exists x\phi \vdash \Delta} (\exists\text{-L})$$

$$\frac{\Gamma \vdash \phi, \Delta}{\Gamma \vdash \forall x\phi, \Delta} (\forall\text{-R})$$

where in the last two rules it is required that x is not free in any formula belonging to $\Gamma \cup \Delta$.

Definition 3.2. Let \mathcal{L} be a first order signature, T a theory in the language \mathcal{L} , ϕ an \mathcal{L} -formula. $T \vdash \phi$ if there is a finite set $\Gamma \subseteq T$ such that $\Gamma \vdash \phi$ is LK-derivable, i.e. it is the root of an LK-derivation tree.

More generally for finite or infinite sets of \mathcal{L} -formulae Γ, Δ we let $\Gamma \vdash \Delta$ if there are finite sets of formulae $\Gamma_0 \subseteq \Gamma$ and $\Delta_0 \subseteq \Delta$ such that $\Gamma_0 \vdash \Delta_0$ is LK-derivable.

Example 3.3. We give an LK-derivation of $\exists y\forall x\phi \vdash \forall x\exists y\phi$ and argue why the above restriction is necessary in the two latter deduction rules.

$$\begin{array}{c} \frac{\phi \vdash \phi}{\phi \vdash \exists y\phi} (\exists\text{-R}) \\ \frac{\phi \vdash \exists y\phi}{\forall x\phi \vdash \exists y\phi} (\forall\text{-L}) \\ \frac{\forall x\phi \vdash \exists y\phi}{\exists y\forall x\phi \vdash \exists y\phi} (\exists\text{-L}) \\ \frac{\exists y\forall x\phi \vdash \exists y\phi}{\exists y\forall x\phi \vdash \forall x\exists y\phi} (\forall\text{-R}) \end{array}$$

The last two applications of $(\exists\text{-L})$ and $(\forall\text{-R})$ are correct because y is not anymore free in $\exists y\phi$, and x is not anymore free in $\exists y\forall x\phi$.

On the other hand assume x, y occurs as free variables in ϕ . Then the following derivation of $\forall x\exists y\phi \vdash \exists y\forall x\phi$ is flawed:

$$\begin{array}{c} \frac{\phi \vdash \phi}{\exists y\phi \vdash \phi} (\exists\text{-L}) \\ \frac{\exists y\phi \vdash \phi}{\forall x\exists y\phi \vdash \phi} (\forall\text{-L}) \\ \frac{\forall x\exists y\phi \vdash \phi}{\forall x\exists y\phi \vdash \forall x\phi} (\forall\text{-R}) \\ \frac{\forall x\exists y\phi \vdash \forall x\phi}{\forall x\exists y\phi \vdash \exists y\forall x\phi} (\exists\text{-R}) \end{array}$$

The use of $(\exists\text{-L})$ in the first step of the above tree is not allowed by the LK -rules, since y occurs free in ϕ (which belongs to $\Delta = \{\phi\}$).

Exercise 3.4. Show by means of a counterexample that $\forall x \exists y \phi \not\models \exists y \forall x \phi$.

Show also that $\exists y \forall x \phi \models \forall x \exists y \phi$.

The above calculus works as expected (though the proof of the theorem below is significantly more intricate than the corresponding proof for propositional logic).

Theorem 3.5 (Gödel's Completeness Theorem, 1930). *Let \mathcal{L} be a first order signature, T a theory in the language \mathcal{L} , ϕ an \mathcal{L} -formula. The following are equivalent:*

- $T \vdash \phi$,
- $T \models \phi$.

3.2 Satisfiable theories and compactness

Fix all over a first order signature \mathcal{L} . From now on unless otherwise specified we will assume our theories T consist of \mathcal{L} -sentences i.e. of formulae with no free variables. Recall that if ϕ is an \mathcal{L} -sentence and \mathcal{M} is an \mathcal{L} -structure with domain M the truth value of ϕ is independent of the valuation $v : \text{var} \rightarrow M$ chosen (all valuations coincide on the empty set, which is the set of free variables of ϕ , hence we can apply Fact 2.33 to ϕ). Thus for \mathcal{L} -sentences ϕ we will write

$$\mathcal{M} \models \phi,$$

rather than

$$\mathcal{M} \models \phi[v] \text{ for some (equivalently all) valuations } v : \text{var} \rightarrow M.$$

We also remark that for all \mathcal{L} -sentences ϕ and \mathcal{L} -structure \mathcal{M} either

$$\mathcal{M} \models \phi,$$

or

$$\mathcal{M} \models \neg \phi.$$

We will assume our theories consist of \mathcal{L} -sentences also in view of the following observations:

Exercise 3.6. Let T be a theory and \mathcal{M} an \mathcal{L} -structure let us denote by $\exists T$ ($\forall T$) the theory obtained by taking the existential (universal) closure of all formulae in T . $\forall T$ and $\exists T$ are \mathcal{L} -theory consisting of sentences. Prove the following:

1. $\mathcal{M} \models \forall T$ if and only if for all valuations v and formulae $\phi \in T$ $\mathcal{M} \models \phi[v]$.
2. $\mathcal{M} \models \exists T$ if and only if there exists a valuation v such that for all formulae $\phi \in T$ $\mathcal{M} \models \phi[v]$.

Therefore if we want to study whether T holds in some structure for some valuation, it suffices to prove that $\exists T$ holds in some structure. Moreover the usual mathematical practice considers just theories consisting of sentences (such is the case for example for the theories we introduced so far in our examples), hence it is natural to focus our attention on this type of theories.

Definition 3.7. Let \mathcal{L} be a first order theory.

A theory T consisting of \mathcal{L} -sentences is:

- satisfiable if there exists a \mathcal{L} -structure \mathcal{M} such that

$$\mathcal{M} \models \phi$$

for all $\phi \in T$;

- closed under logical consequences, if for all \mathcal{L} -sentences ϕ such that $T \models \phi$, we have that $\phi \in T$;
- complete, if for all \mathcal{L} -sentences ϕ , we either have that $T \models \phi$ or that $T \models \neg\phi$.

Given a set of \mathcal{L} -sentences S , its closure under logical consequences $\text{CCL}(S)$ is the least theory T which contains all \mathcal{L} -sentences ϕ such that $S \models \phi$.

Σ is a set of axioms for T , if $\text{CCL}(T) = \text{CCL}(\Sigma)$.

T is finitely axiomatizable if there exists a finite set of sentences Σ such that $\text{CCL}(T) = \text{CCL}(\Sigma)$.

An immediate corollary of the completeness theorem is the following fundamental result:

Theorem 3.8 (Compactness Theorem). *Assume T is a finitely satisfiable theory in the language \mathcal{L} (i.e. for every finite set $\Gamma \subseteq T$ there is an \mathcal{L} -structure \mathcal{M} satisfying all formulae in Γ). Then T is satisfiable.*

Proof. If T is satisfiable it is clearly finitely satisfiable, hence only one direction is non trivial. We prove it: If T is not satisfiable it does not hold in any model, hence $T \models \psi$ for any ψ , in particular $T \models \phi \wedge \neg\phi$. By the completeness theorem, we get that $T \vdash \phi \wedge \neg\phi$. This holds if and only if there is a finite set $\Gamma_0 \subseteq T$ such that $\Gamma_0 \vdash \phi \wedge \neg\phi$ is the root of an LK derivation tree. The completeness theorem gives that $\Gamma_0 \models \phi \wedge \neg\phi$, i.e. Γ_0 is not satisfiable. Hence T is not finitely satisfiable as witnessed by Γ_0 . \square

A second equivalent formulation of compactness is the following:

Theorem 3.9 (Compactness II). *Assume $T \models \phi$. Then there exists a finite $\Sigma \subseteq T$ such that $\Sigma \models \phi$.*

Proof. An immediate byproduct of the definitions and of the completeness theorem. \square

We will give a self-contained proof of the compactness theorem in the last part of these notes. Before then we will outline some of its applications.

Proposition 3.10. *Assume T is finitely axiomatizable. Then there exists a finite set $\Sigma \subseteq T$ which is a set of axioms for T .*

Proof. Assume $\Sigma_0 \not\subseteq T$ is a finite set such that $\text{CCL}(\Sigma_0) = \text{CCL}(T)$. Then $T \models \bigwedge \Sigma_0$ and for all formulae $\phi \in T$ we have that $\Sigma_0 \models \phi$. By the compactness theorem we get that some finite $\Sigma \subseteq T$ is such that $\Sigma \models \bigwedge \Sigma_0$. On the other hand we also get that $\Sigma_0 \models \bigwedge \Sigma$ since $\Sigma_0 \models \phi$ for all $\phi \in \Sigma$. Therefore $\bigwedge \Sigma \equiv \bigwedge \Sigma_0$. We conclude that $\Sigma \subseteq T$ is a finite set of axioms for T , since for any $\psi \in \text{CCL}(T)$ $\Sigma \models \bigwedge \Sigma_0$ and $\bigwedge \Sigma_0 \models \psi$. \square

3.3 Classes of \mathcal{L} -structures

Definition 3.11. Let \mathcal{L} be a first order signature. We denote by $\text{Mod}_{\mathcal{L}}$ the class of all \mathcal{L} -structures.

Given a theory T in the language \mathcal{L}

$$\text{Mod}_{\mathcal{L}}(T) = \{\mathcal{M} \in \text{Mod}_{\mathcal{L}} : \mathcal{M} \models T\}.$$

A family C of \mathcal{L} -structures is axiomatizable if $C = \text{Mod}_{\mathcal{L}}(T)$ for some \mathcal{L} -theory T , and finitely axiomatizable if $C = \text{Mod}_{\mathcal{L}}(T)$ for some theory T given by a finite set of axioms.

Example 3.12. Groups, rings, fields are all examples of finitely axiomatizable classes of \mathcal{L} -structures over the appropriate language. An example of a theory which is axiomatizable but not finitely axiomatizable is that of fields of characteristic 0. We will prove this as an application of the compactness theorem.

Exercise 3.13. Prove that groups, rings, and fields are finitely axiomatizable, and also that fields of characteristic 0 are axiomatizable.

Fact 3.14. Let \mathcal{L} be a first order signature and T_0, T_1 be theories in the language \mathcal{L} . Then:

1. $\text{Mod}_{\mathcal{L}} = \text{Mod}_{\mathcal{L}}(\emptyset)$,
2. $\text{Mod}_{\mathcal{L}}(T_0) \cap \text{Mod}_{\mathcal{L}}(T_1) = \text{Mod}_{\mathcal{L}}(T_0 \cup T_1)$.
3. Assume T_0 is finitely axiomatizable. Then $\text{Mod}_{\mathcal{L}} \setminus \text{Mod}_{\mathcal{L}}(T_0)$ is finitely axiomatizable.
4. Assume $\text{Mod}_{\mathcal{L}} \setminus \text{Mod}_{\mathcal{L}}(T_0)$ is axiomatizable. Then $\text{Mod}_{\mathcal{L}}(T_0)$ and $\text{Mod}_{\mathcal{L}} \setminus \text{Mod}_{\mathcal{L}}(T_0)$ are both finitely axiomatizable. Hence a partition of $\text{Mod}_{\mathcal{L}}$ in two pieces is such that either both pieces are finitely axiomatizable or none of the pieces is axiomatizable.

Proof. 1, 2, 3 are useful exercises for the reader. We prove 4: If one of the two is finitely axiomatizable, by 3 so is the other. So assume both of them are axiomatizable but not finitely axiomatizable. Let T_1 be such that $\text{Mod}_{\mathcal{L}}(T_1) = \text{Mod}_{\mathcal{L}} \setminus \text{Mod}_{\mathcal{L}}(T_0)$. Then for any finite $\Sigma \subseteq T_1$ there is an \mathcal{L} -structure \mathcal{M} which models Σ but not T_1 . Since $\text{Mod}_{\mathcal{L}}(T_0) = \text{Mod}_{\mathcal{L}} \setminus \text{Mod}_{\mathcal{L}}(T_1)$, we get that \mathcal{M} is a model of $\Sigma \cup T_0$. This gives that the theory $T_0 \cup T_1$ is finitely consistent. Therefore it has a model \mathcal{N} . Then

$$\mathcal{N} \in \text{Mod}_{\mathcal{L}}(T_0 \cup T_1) = \text{Mod}_{\mathcal{L}}(T_0) \cap \text{Mod}_{\mathcal{L}}(T_1) = \emptyset.$$

□

We can also relativize the above properties to axiomatizable classes:

Definition 3.15. Let \mathcal{L} be a first order signature. Given a theory T in the language \mathcal{L} , we say that $C \subseteq \text{Mod}(T)$ is (finitely) axiomatizable modulo T if $C = \text{Mod}(T \cup T_0)$ with T_0 a (finite) set of \mathcal{L} -sentences.

Fact 3.16. Assume $C \subseteq \text{Mod}_{\mathcal{L}}(T)$ is axiomatizable modulo T . Then C is finitely axiomatizable modulo T if and only if so is $\text{Mod}_{\mathcal{L}}(T) \setminus C$. Hence a partition of $\text{Mod}_{\mathcal{L}}(T)$ in two pieces is such that either both pieces are finitely axiomatizable modulo T or none of the pieces is axiomatizable.

Exercise 3.17. Prove the fact.

Example 3.18. As a further application of compactness let us prove that the class of fields of characteristic 0 is \mathcal{L} -axiomatizable, but it is not finitely axiomatizable where $\mathcal{L} = \{0, 1, +, \cdot\}$. This will also give that class of fields of non-zero characteristic is not axiomatizable by Fact 3.16. The theory of fields is finitely axiomatizable in \mathcal{L} by a finite set of axioms T_0 (prove it). We can isolate the fields of characteristic 0 in $\text{Mod}_{\mathcal{L}}(T_0)$ as those fields which moreover satisfy the sentences $\neg(\underline{n} = 0)$ for all $n \in \mathbb{N}$, where \underline{n} is the term obtained by the string $1 + 1 + 1 + \dots$ repeated n -times. Let $T_1 = T_0 \cup \{\neg(\underline{n} = 0) : n \in \mathbb{N}\}$.

Now assume that $\text{Mod}_{\mathcal{L}}(T_1)$ is finitely axiomatizable as witnessed by the finite set Σ . By proposition 3.10 we can assume $\Sigma \subseteq T$. Find p a prime number large enough so that no sentence of type $\neg(\underline{n} = 0)$ appearing in Σ is such that $n \geq p$. Then \mathbb{Z}_p is a model of Σ and is a field with non-zero characteristic, a contradiction.

3.4 Substructures, morphisms, and products

We now generalize to arbitrary \mathcal{L} -structures the usual notion of homomorphism, product, and substructure we have already encountered in algebra. We will show that many algebraic properties can be characterized in terms of syntactic properties of the formulae satisfied by the relevant algebraic structures.

First of all we need to define two special subclasses of formulae: the positive ones and the quantifier free ones.

Definition 3.19. A formula is *positive* if the unique boolean connectives occurring in it are \vee, \wedge . It is *quantifier free* if no quantifier symbol occurs in it.

Fact 3.20. Let \mathcal{L} be a first order signature. Every quantifier free \mathcal{L} -formula ψ is logically equivalent to one of the form

$$\bigvee_{i \in I} \left(\bigwedge \Gamma_i \right)$$

with I a finite set and Γ_i a finite set of atomic formulae or negation of atomic formulae.

Proof. SKETCH: Run the proof of Theorem 1.13 with atomic formulae taking the role of propositional variables. \square

Substructures

Definition 3.21. Let M be a set and $f : M^n \rightarrow M$. Given $B \subseteq M$, B is f -closed if $f(a_1, \dots, a_n) \in B$ for all $a_1, \dots, a_n \in B$.

Assume \mathcal{F} is a family of finitary operations on M , $B \subseteq M$ is \mathcal{F} -closed if $f(a_1, \dots, a_n) \in B$ for all $a_1, \dots, a_n \in B$ and $f \in \mathcal{F}$.

For any $A \subseteq M$, $\text{Cl}_{\mathcal{F}}(A)$ (the closure of A under \mathcal{F}) is the intersection of all \mathcal{F} -closed sets $B \supseteq A$.

Definition 3.22. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$ be a first order signature and $\mathcal{M} = \langle M, R_i^M : i \in I, f_j^M : j \in J, c_k^M : k \in K \rangle$ be an \mathcal{L} -structure with domain M .

$N \subseteq M$ is an \mathcal{L} -substructure of M if it contains $\{c_k^M : k \in K\}$ and is $\{f_j^M : j \in J\}$ -closed.

The \mathcal{L} -substructure of M generated by $X \subseteq M$ is the intersection of all \mathcal{L} -substructures of M containing X , i.e. the $\{f_j^M : j \in J\}$ -closure of $X \cup \{c_k^M : k \in K\}$.

An \mathcal{L} -substructure N of M is generated by a subset X if $N = \text{Cl}_{\{f_j^M : j \in J\}}(X \cup \{c_k^M : k \in K\})$, and is finitely generated if it can be generated by a finite subset X .

Example 3.23. A substructure of the \mathcal{L}_2 -structure $\langle \mathbb{R}, <, +, \cdot, -, 0, 1 \rangle$ is any ring $A \subseteq \mathbb{R}$, and the smallest such substructure is \mathbb{Z} . \mathbb{Z} is finitely generated inside \mathbb{R} , since $\mathbb{Z} = \text{Cl}_{\{+, -, \cdot\}}(\{0, 1\})$.

Proposition 3.24. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$ be a first order signature and $\mathcal{M} = \langle M, R_i^M : i \in I, f_j^M : j \in J, c_k^M : k \in K \rangle$ be an \mathcal{L} -structure with domain M . Assume \mathcal{N} is an \mathcal{L} -substructure of \mathcal{M} generated by X . Then

$$\mathcal{N} = \{v(t(x_1, \dots, x_n)) : t(x_1, \dots, x_n) \text{ an } \mathcal{L}\text{-term and } v : \text{var} \rightarrow X \text{ a valuation}\}.$$

(in case $X = \emptyset$, $\mathcal{N} = \{v(t) : t \text{ a } \mathcal{L}\text{-term with no free variables}\}$).

Proof. We have that $\mathcal{N} = \text{Cl}_{\{f_j^M : j \in J\}}(X \cup \{c_k^M : k \in K\})$.

It is enough to show that $D = \{v(t(x_1, \dots, x_n)) : v : \text{var} \rightarrow X\} \subseteq \text{Cl}_{\{f_j^M : j \in J\}}(X \cup \{c_k^M : k \in K\})$ is $\{f_j^M : j \in J\}$ -closed. First of all, $c_k^M = v(c_k) \in D$ and $a = v(x) \in D$ for all $a \in X$, choosing a valuation v which maps all variables to a . Now let t_1, \dots, t_n be \mathcal{L} -terms and $v : \text{var} \rightarrow X$ be a valuation. Assume that $v(t_l) \in \text{Cl}_{\{f_j^M : j \in J\}}(X \cup \{c_k^M : k \in K\})$ for all $l = 1, \dots, n$. Then for any t of the form $f_j(t_1, \dots, t_n)$ we have that

$$v(t) = v(f_j(t_1, \dots, t_n)) = f_j^M(v(t_1), \dots, v(t_n)) \in \text{Cl}_{\{f_j^M : j \in J\}}(X \cup \{c_k^M : k \in K\}).$$

An induction on the complexity of a term t shows at the same time that $D \subseteq \text{Cl}_{\{f_j^M : j \in J\}}(X \cup \{c_k^M : k \in K\})$ is $\{f_j^M : j \in J\}$ -closed, giving the desired thesis. \square

Exercise 3.25.

- Prove that the substructure generated by $\{-1\}$ inside $(\mathbb{Z}, +, 0)$ is the family of negative or null integers (HINT: prove by induction: (a) for any negative or null integer number n there is a term $t(x)$ such that $v(t(x)) = n$ for any (the unique) valuation $v : \text{var} \rightarrow \{-1\}$, (b) for any term t , $v(t) \leq 0$).
- What is the substructure generated by $\{n\}$ for some fixed non null $n \in \mathbb{Z}$?
- What is the substructure generated by a finite set $\{n_1, \dots, n_k\}$ of elements of \mathbb{Z} ? (HINT: it is the substructure given by numbers of type $\sum_{i=1}^l k_i \cdot n_i$ with each $k_i \in \mathbb{N}$. How would you prove that this is the correct answer?)
- What is the substructure generated by an arbitrary subset of \mathbb{Z} ?

Fact 3.26. A substructure of \mathcal{M} preserves the truth of all quantifier free formulae.

Proof. Every quantifier free formula is logically equivalent to formula ϕ of type

$$\bigvee \left\{ \bigwedge \Gamma_i : i \in I \right\}$$

with each Γ_i a finite set consisting either of atomic formulae or of their negation. Now it is easy to check that the fact holds for an atomic formula or for its negation and also that if it holds for ϕ, ψ , it also holds for $\phi \vee \psi$ and $\phi \wedge \psi$, hence the thesis. \square

Remark 3.27. A substructure may not preserve existential formulae or universal formulae. For example: consider the partial order \mathbb{Z}^2 with ordering defined component wise $((a, b) < (c, d)$ if and only if $a < c$ and $b < d$). Then $\langle \mathbb{Z}^2, < \rangle \models \exists x \exists y \neg(x \leq y \vee y \leq x)$. On the other hand the substructure with domain $\{(n, 0) : n \in \mathbb{Z}\}$ satisfies its opposite $\forall x \forall y (x \leq y \vee y \leq x)$.

Products

Recall that for a family of non-empty sets $\langle M_l : l \in L \rangle$, its product is the set $\prod_{l \in L} M_l$ given by functions $h : L \rightarrow \bigcup_{l \in L} M_l$ such that $h(l) \in M_l$ for all $l \in L$.

Definition 3.28. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$ be a first order language and $(\mathcal{M}_l = \langle M_l, R_i^{M_l} : i \in I, f_j^{M_l} : j \in J, c_k^{M_l} : k \in K \rangle : l \in L)$ be a family of \mathcal{L} -structures. The product of this family $\mathcal{M} = \prod_{l \in L} \mathcal{M}_l$ is the \mathcal{L} -structure defined as follows:

- its domain is the set $\prod_{l \in L} M_l$;
- $R_i^{\mathcal{M}}(h_1, \dots, h_n)$ holds if and only if $R_i^{M_l}(h_1(l), \dots, h_n(l))$ holds for all $l \in L$ and $i \in I$;
- $f_j^{\mathcal{M}}(h_1, \dots, h_n)(l) = f_j^{M_l}(h_1(l), \dots, h_n(l))$ for all $l \in L$ and $j \in J$;
- $c_k^{\mathcal{M}}(l) = c_k^{M_l}$ for all $l \in L$ and $k \in K$.

Example 3.29. The product of two copies of the structure $\langle \mathbb{C}, +, \cdot, -, ^{-1}, 0, 1 \rangle$ is the structure \mathbb{C}^2 endowed with the operations defined pointwise and $-, ^{-1}$ denoting the inverse operations of the additive and multiplicative group structure on \mathbb{C} . Notice that the product does not preserves the truth of disjunctions:

For example let $\mathcal{L} = \{\oplus, \otimes, I_{\oplus}, I_{\otimes}, \bar{0}, \bar{1}\}$ be the language to interpret the above symbols as the operations $+, \cdot, -, ^{-1}, 0, 1$ in \mathbb{C} . Then

$$\mathcal{C} = \langle \mathbb{C}, +, \cdot, -, ^{-1}, 0, 1 \rangle \models x \doteq \bar{0} \vee x \otimes I_{\otimes}(x) = \bar{1}[v]$$

for any $v : \text{var} \rightarrow \mathbb{C}$, while

$$\mathcal{C} \times \mathcal{C} \not\models x \doteq \bar{0} \vee x \otimes I_{\otimes}(x) = \bar{1}[v]$$

for $v(x) = (0, 1)$.

Fact 3.30. Assume ϕ is positive with no symbol of disjunction \vee occurring in it. Let $(\mathcal{M}_l = \langle M_l, R_i^{M_l} : i \in I, f_j^{M_l} : j \in J, c_k^{M_l} : k \in K \rangle : l \in L)$ be a family of \mathcal{L} -structures. Then the product $\mathcal{M} = \prod_{l \in L} \mathcal{M}_l$ satisfies ϕ with a valuation $v : \text{var} \rightarrow \prod_{l \in L} M_l$ if and only if

$$\mathcal{M}_l \models \phi[v_l]$$

(where $v_l(x) = v(x)(l)$) for all $l \in L$.

Proof. The fact holds for atomic formulae by definition. We prove the clause for existential formulae and leave the remaining to the reader. Assume $\mathcal{M} \models \phi[v]$ if and only if $(\mathcal{M}_l \models \phi[v_l])$ for all $l \in L$. Then

$$\mathcal{M} \models \exists x \phi[v]$$

if and only if there is $h \in \prod_{l \in L} M_l$ such that

$$\mathcal{M} \models \phi[v_{x/h}]$$

if and only if (by inductive assumption) for all $l \in L$

$$\mathcal{M}_l \models \phi[(v_l)_{x/h(l)} = (v_{x/h})_l],$$

giving that

$$\mathcal{M}_l \models \exists x \phi[v_l]$$

for all $l \in L$ as witnessed by $h(l)$.

Conversely assume that

$$\mathcal{M}_l \models \exists x \phi[v_l]$$

for all $l \in L$. Then for all $l \in L$ there is some $a_l \in L$ such that

$$\mathcal{M}_l \models \phi[(v_l)_{x/a_l}];$$

let $h \in \prod_{l \in L} M_l$ be defined by $h(l) = a_l$, then (by inductive assumption on ϕ)

$$\mathcal{M} \models \phi[v_{x/h}]$$

giving that

$$\mathcal{M} \models \exists x \phi[v].$$

□

Remark 3.31. The above fact fails for negations of positive formulae, for example: Let $\phi \equiv \neg x = y$. Then

$$\mathbb{Z}^2 \models \neg x = y[x/(2, 3), y/(4, 3)],$$

but it is not the case that

$$\mathbb{Z} \models \neg x = y[x/3, y/3].$$

Exercise 3.32. In the language $\mathcal{L} = \{+, \cdot, 0, 1\}$ give axioms for the theory of integral domains. Prove that the product of two integral domains is never an integral domain. Which axiom is never preserved?

Morphisms

The examples we gave of \mathcal{L} -structures were all drawn from familiar algebraic structures. It is the case that first order logic is a good setting in which the notion of morphism can be generalized to a much wider class of structures.

Definition 3.33. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$ be a first order language and $\mathcal{M} = \langle M, R_i^M : i \in I, f_j^M : j \in J, c_k^M : k \in K \rangle, \mathcal{N} = \langle N, R_i^N : i \in I, f_j^N : j \in J, c_k^N : k \in K \rangle$ be first order structures $h : M \rightarrow N$ is a:

- morphism if

$$h(c_k^M) = c_k^N,$$

$$R_i^M(a_1, \dots, a_n) \Rightarrow R_i^N(h(a_1), \dots, h(a_n)),$$

$$f_j^N(h(a_1), \dots, h(a_n)) = h(f_j^M(a_1, \dots, a_n)),$$

for all $i \in I$, $j \in J$, $k \in K$ and $a_1, \dots, a_n \in M$;

- an embedding if

$$R_i^M(a_1, \dots, a_n) \Leftrightarrow R_i^N(h(a_1), \dots, h(a_n)),$$

holds for all $i \in I$ and $a_1, \dots, a_n \in M$;

- an elementary embedding if for all formulae $\phi(x_1, \dots, x_n)$ with displayed free variables and all $v : \text{var} \rightarrow M$, letting

$$v_h(x) = h(v(x)), \tag{1}$$

we get that

$$\mathcal{M} \models \phi(x_1, \dots, x_n)[v] \Leftrightarrow \mathcal{N} \models \phi(x_1, \dots, x_n)[v_h];$$

- an isomorphism if it is a surjective embedding.

We say that $h : M \rightarrow N$ preserves a formula $\phi(x_1, \dots, x_n)$ if for all valuations $v : \text{var} \rightarrow M$ we have that

$$\mathcal{M} \models \phi(x_1, \dots, x_n)[v] \Rightarrow \mathcal{N} \models \phi(x_1, \dots, x_n)[v_h];$$

Example 3.34. The inclusion map of \mathbb{N} into \mathbb{Z} is an \mathcal{L}_0 -embedding for the language $\mathcal{L}_0 = \{*\}$ and the structures $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$. It is not an elementary embedding since the first structure does not satisfy the group axioms, while the second does.

The inclusion map of \mathbb{Z} into \mathbb{R} is an \mathcal{L}_2 -embedding for the language $\mathcal{L}_0 = \{+, \cdot, 0, 1, <\}$ and the structures $(\mathbb{Z}, +, \cdot, 0, 1, <)$, $(\mathbb{R}, +, \cdot, 0, 1, <)$. It is not elementary since $(\mathbb{R}, +, \cdot, 0, 1)$ is a field and $(\mathbb{Z}, +, \cdot, 0, 1)$ is not.

It can be shown (but it is a rather deep result) that the inclusion map of $(\mathbb{Q}, <)$ into $(\mathbb{R}, <)$ is an elementary embedding for the language $\{<\}$.

Exercise 3.35. Show that the inclusion map of the structure $(\mathbb{Q}, +, \cdot, 0, 1, <)$ into $(\mathbb{R}, +, \cdot, 0, 1, <)$ is an embedding but not an elementary embedding (HINT: there are polynomials in integer coefficients whose roots are not rational).

The following exercise gives some of the basic properties of homomorphisms.

Exercise 3.36. Prove the following facts:

- For the language $\mathcal{L}_\infty = \{*, \doteq\}$ introduced before, the notion of morphism introduced above correspond to the notion of group homomorphism whenever \mathcal{M}, \mathcal{N} are groups.
- The notion of ring homomorphism correspond to the notion of morphism in the language $\mathcal{L} = \{*, \oplus, \doteq, \bar{0}, \bar{1}\}$ whenever \mathcal{M}, \mathcal{N} are rings.

- An embedding is always an injective morphism (apply the definition of embedding to the equality relation symbol).
- The inclusion map of a substructure into a structure is always an embedding.
- An elementary embedding is also an embedding (apply the definition of elementary embedding to the atomic formulae of type $R(x_1, \dots, x_n)$ and their negation).

The following can be proved by induction on the complexity of the terms:

Fact 3.37. *Let \mathcal{L} be a first order language. Let \mathcal{M}, \mathcal{N} be \mathcal{L} -structures with domain M, N respectively. Assume $h : M \rightarrow N$ is a morphism between \mathcal{M} and \mathcal{N} . Then⁵ $h(v(t)) = v_h(t)$ for all \mathcal{L} -terms t .*

Proof. If t is a constant or a variable, the thesis trivially holds; next assume the thesis holds for t_1, \dots, t_m and $t = f_j(t_1, \dots, t_m)$. Then

$$\begin{aligned}
 h(v(t)) &= h(v(f_j(t_1, \dots, t_m))) = \\
 &= h(f_j^M(v(t_1), \dots, v(t_m))) = \\
 &= f_j^N(h(v(t_1)), \dots, h(v(t_m))) = \\
 &= f_j^N(v_h(t_1), \dots, v_h(t_m)) = \\
 &= v_h(t),
 \end{aligned}$$

where in the before last equality we used the inductive assumptions on t_1, \dots, t_m . \square

There are several conclusions that can be drawn from Fact 3.37:

Fact 3.38. *Let $h : M \rightarrow N$ be a morphism between the \mathcal{L} -structures \mathcal{M}, \mathcal{N} with domain respectively M, N .*

1. *Assume h preserves ϕ, ψ . Then h preserves $\exists x\phi, \phi \vee \psi, \phi \wedge \psi$.*
2. *Assume h is surjective and preserves ϕ . Then h preserves also $\forall x\phi$.*
3. *Assume h preserves ϕ , then it preserves any formula ψ logically equivalent to ϕ .*

Proof. We leave everything as a useful exercise for the reader, except the proof that whenever ϕ is preserved by h so is $\exists x\phi$: assume $\mathcal{M} \models \exists x\phi(x, x_1, \dots, x_n)[v]$. By definition there is $a \in M$ such that

$$\mathcal{M} \models \phi(x, x_1, \dots, x_n)[v_{x/a}].$$

By inductive assumptions (letting $v^* = v_{x/a}$) applied to $\phi(x, x_1, \dots, x_n), v^*$ we conclude that

$$\mathcal{N} \models \phi(x, x_1, \dots, x_n)[v_h^*];$$

by definition we get that

$$\mathcal{N} \models \exists x\phi(x, x_1, \dots, x_n)[v_h^*].$$

⁵Recall 1 for the definition of v_h .

Since v_h^* and v_h agree on all free variables of $\exists x\phi(x, x_1, \dots, x_n)$, we conclude that

$$\mathcal{N} \models \exists x\phi(x, x_1, \dots, x_n)[v_h].$$

□

Proposition 3.39. *Let $h : M \rightarrow N$ be a morphism between the \mathcal{L} -structures \mathcal{M}, \mathcal{N} with domain respectively M, N . The following holds:*

1. *h preserves all positive formulae in which no universal quantifier symbol \forall appears.*
2. *If h is a surjective morphism, it preserves all positive formulae.*
3. *If h is an embedding it preserves all quantifier free formulae.*
4. *If h is an isomorphism, it is also an elementary embedding.*

Proof.

1. By the previous fact (using that h is a morphism) we obtain that for any $v : \text{var} \rightarrow M$

$$R_i^M(v(t_1), \dots, v(t_m)) \Rightarrow R_i^N(v_h(t_1), \dots, v_h(t_m))$$

Hence

$$\mathcal{M} \models R_i(t_1, \dots, t_m)[v]$$

if and only if

$$R_i^M(v(t_1), \dots, v(t_m))$$

only if

$$R_i^N(v_h(t_1), \dots, v_h(t_m))$$

if and only if

$$\mathcal{N} \models R_i(t_1, \dots, t_m)[v_h].$$

Now a simple inductive argument handles the cases of formulae built up over atomic formulae just by means of \vee, \wedge, \exists .

2. If $h : M \rightarrow N$ is surjective we can handle also the inductive argument for the universal quantifier \forall .
3. If $h : M \rightarrow N$ is an embedding for any⁶ $v : \text{var} \rightarrow M$

$$R_i^M(v(t_1), \dots, v(t_m)) \Leftrightarrow R_i^N(v_h(t_1), \dots, v_h(t_m))$$

Hence

$$\mathcal{M} \models R_i(t_1, \dots, t_m)[v]$$

if and only if

$$R_i^M(v(t_1), \dots, v(t_m))$$

if and only if

$$R_i^N(v_h(t_1), \dots, v_h(t_m))$$

⁶Recall 1 for the definition of v_h .

if and only if

$$\mathcal{N} \models R_i(t_1, \dots, t_m)[v_h].$$

Therefore h preserves the negation of atomic formulae. Now any quantifier free \mathcal{L} -formula ϕ is logically equivalent to a formula ψ of the form $\bigvee_{i \in I} \left\{ \bigwedge_{j \in J_i} \Gamma_j \right\}$, where each Γ_j is a set consisting just of atomic formulae or negation of atomic formulae. By the first item of this proposition and the last item of the previous fact we obtain that h must preserve all quantifier free formulae.

4. Assume $h : M \rightarrow N$ is an isomorphism between \mathcal{L} -structures \mathcal{M}, \mathcal{N} with domain M, N . Since h is an embedding the above argument applies for atomic formulae. The same argument of the previous item handles the inductive cases for formulae whose principal connective is boolean. We are left with the treatment of quantifiers, which can be handled by means of Fact 3.38.

□

The above results link algebraic properties of morphisms to their logical properties. There is a celebrated theorem of Birkhoff which gives a nice algebraic characterization of which theories can be axiomatized by sentences of type

$$\forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_m t(x_1, \dots, x_n) = s(y_1, \dots, y_m).$$

Notation 3.40. Theories which can be axiomatized by this type of axioms are called equational theories.

This is the case for example for the theory of groups in the language $\mathcal{L}_1 = \{*, I, e\}$ and for the theory of rings in the language $\mathcal{L} = \{\oplus, \otimes, \underline{0}, \underline{1}, I_{\oplus}\}$ (I_{\oplus} is a unary relation symbol which can be used to define the inverse of the group operation given by the sum).

Exercise 3.41. Show that the theory of groups and the theory of rings are equational.

Exercise 3.42. Show that the class of groups and the class of rings are closed under:

- homomorphic images (i.e. if $(G, \cdot_G, I_G, e_G), (H, \cdot_H, I_H, e_H)$ are $\mathcal{L}_1 = \{*, I, e\}$ -structures, G is a group, and $h : G \rightarrow H$ is a surjective \mathcal{L}_1 -morphism, then H is a group as well, and similarly for rings);
- substructures;
- products.

Exercise 3.43. Show that the class of fields is not closed under products.

In general it is not too hard to see that whenever a theory T in a language \mathcal{L} is equational, the class C_T of \mathcal{L} -structures which are models of T is closed under products, homomorphic images, and substructures. The converse is Birkhoff's theorem:

Theorem 3.44 (Birkhoff). *Let \mathcal{L} be a first order language with no relation symbols and C a class of \mathcal{L} -structures. The following are equivalent:*

- C is closed under products, substructures, and homomorphic images.

- There is a language $\mathcal{L}_1 \supseteq \mathcal{L}$ such that C is the family of \mathcal{L}_1 -structures satisfying an equational theory T^7 .

By Birkhoff's theorem we get that the class of fields is not an equational theory.

3.5 Elementary equivalence and completeness

Definition 3.45. Let \mathcal{M}, \mathcal{N} be \mathcal{L} -structures.

\mathcal{M}, \mathcal{N} are elementarily equivalent ($\mathcal{M} \equiv \mathcal{N}$) if for all \mathcal{L} -sentences ϕ

$$\mathcal{M} \models \phi \text{ if and only if } \mathcal{N} \models \phi.$$

Lemma 3.46. Assume $h : M \rightarrow N$ is an elementary embedding between \mathcal{L} -structures \mathcal{M}, \mathcal{N} with domain M, N . Then \mathcal{M} and \mathcal{N} are elementarily equivalent.

Proof. Exercise for the reader. □

Remark 3.47. The converse does not hold: for example it can be shown that $\langle [0, 1] \cup (\mathbb{Q} \cap (1, 2]), < \rangle$ and $\langle (\mathbb{Q} \cap [0, 1]) \cup (1, 2], < \rangle$ are elementarily equivalent in the language $\{<\}$ but there is no elementary embedding of one of them into the other.

Fact 3.48. Let Σ be a satisfiable set of \mathcal{L} -sentences, and ϕ an \mathcal{L} -sentence. The following are equivalent:

1. $\Sigma \models \phi$,
2. $\Sigma \cup \{\neg\phi\}$ is not satisfiable.

Proof. (1) implies (2): By contraposition. Assume (2) fails and find \mathcal{M} model of $\Sigma \cup \{\neg\phi\}$. Then \mathcal{M} witnesses that $\Sigma \not\models \phi$, i.e. (1) fails.

Conversely assume (1) fails. Then we can find \mathcal{M} model of Σ such that $\mathcal{M} \not\models \phi$. Then $\mathcal{M} \models \neg\phi$, hence $\Sigma \cup \{\neg\phi\}$ is satisfiable as witnessed by \mathcal{M} , i.e. (2) fails. □

Notation 3.49. Let \mathcal{M} be an \mathcal{L} -structure for some first order signature \mathcal{L} . The theory of \mathcal{M} is the set

$$T_{\mathcal{M}} = \{\phi : \phi \text{ is an } \mathcal{L}\text{-sentence and } \mathcal{M} \models \phi\}$$

Remark 3.50. $T_{\mathcal{M}}$ is a satisfiable, complete theory, closed under logical consequence as witnessed by \mathcal{M} .

Proposition 3.51. Let T be a satisfiable \mathcal{L} -theory made up of \mathcal{L} -sentences and closed under logical consequence. The following are equivalent:

1. T is complete.
2. Every two \mathcal{L} -structures \mathcal{M}, \mathcal{N} which are models of T are elementarily equivalent.
3. $T = T_{\mathcal{M}}$ for some \mathcal{M} which satisfies T .

⁷More precisely we can expand each $\mathcal{M} \in C$ to an \mathcal{L}_1 -structure \mathcal{M}_1 with the same domain, the same interpretation of the symbols in \mathcal{L} , and such that $\mathcal{M}_1 \models T$.

Proof. We prove these equivalences as follows:

- (1) **implies (2):** Assume $\mathcal{M} \models \phi$. Then $T \not\models \neg\phi$ as witnessed by \mathcal{M} , since T is complete $T \models \phi$. Hence $\mathcal{N} \models \phi$ as well being a model of T . (This implication does not need that T is closed under logical consequences).
- (2) **implies (3):** Notice that $T \subseteq T_{\mathcal{M}}$ for any \mathcal{M} model of T . By (2) all models of T satisfy exactly the same set of sentences, i.e. $T_{\mathcal{M}} = T_{\mathcal{N}}$ for all \mathcal{M}, \mathcal{N} which model T . Assume $T \neq T_{\mathcal{M}}$ for some \mathcal{M} which models T . Then there exists $\phi \in T_{\mathcal{M}} \setminus T$. Since T is closed under logical consequences $T \not\models \phi$, otherwise $\phi \in T$. This gives that some $\mathcal{N} \models T \cup \{\neg\phi\}$. But this contradicts (2), since $T_{\mathcal{M}}$ and $T_{\mathcal{N}}$ disagree on ϕ .
- (3) **implies (1):** For any sentence ϕ and any structure \mathcal{M} , either $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$. Hence $T_{\mathcal{M}}$ is complete (and closed under logical consequences).

□

3.6 More exercises on first order logic

Take the set of notes on logic of prof. Andretta available on the Moodle page of this course and do some among the exercises: 3.72(**) (ignore the request to prove elementary equivalence, but —if you think the two models are not elementarily equivalent — try to prove it), 3.73(**) (ignore the request to prove elementary equivalence, but —if you think the two models are not elementarily equivalent — try to prove it), 3.74 ((i)*, (ii)**, (iii)**), 3.75, 3.76 (** — a structure is rigid if it does not admit non-trivial automorphisms), 3.77(* — use 3.76), 3.78 (*), 3.79 (*), 3.80(*), 3.81(*), 3.84 (** — an independent set of axioms Δ for a theory Σ is a set of axioms for Σ such that $\text{CCL}(\Delta \setminus \{\phi\}) \neq \text{CCL}(\Delta)$ for all $\phi \in \Delta$). (* means the exercise is difficult, ** means the exercise is even more difficult....)

4 Compactness

All over this section the first order theories we consider consist just of sentences. Recall the compactness theorem:

Theorem. *Let \mathcal{L} be a first order signature and T an \mathcal{L} -theory. Then T is finitely satisfiable if and only if it is satisfiable.*

4.1 Proof of the compactness theorem

The proof is based on two Lemmas and two Definitions.

Definition 4.1. Let \mathcal{L} be a first order signature and T be an \mathcal{L} -theory. T has existential witnesses (or the *Henkin property*) if for all \mathcal{L} -formulae ϕ such that $T \models \exists x\phi$, there is some constant symbol $c \in \mathcal{L}$ such that $T \models \phi[x/c]$.

In most cases theories do not have existential witnesses simply because there are not enough constants.

Example 4.2. Let $\mathcal{L} = \{\oplus, \otimes, c_0, c_1\}$ with c_0, c_1 constant symbols and \oplus, \otimes binary function symbols. Consider $T_{\mathcal{N}}$ where

$$\mathcal{N} = \langle \mathbb{N}, +, \cdot, 0, 1 \rangle.$$

Then $T_{\mathcal{N}} \models \exists x(x = c_1 \oplus c_1)$ but there is no constant symbol e such that $T_{\mathcal{N}} \models e = c_1 \oplus c_1$.

In this example we still have a closed term t such that $T_{\mathcal{N}} \models \exists x(x = c_1 \oplus c_1)$ if and only if $T_{\mathcal{N}} \models (t = c_1 \oplus c_1)$; it suffices to take $t = c_1 \oplus c_1$.

On the other hand in more complicated structures this is not anymore the case.

Example 4.3. Consider the $\mathcal{L} = \{\oplus, \otimes, c_0, c_1\}$ -structure $\mathcal{R} = \langle \mathbb{R}, +, \cdot, 0, 1 \rangle$ and the \mathcal{L} -sentence $\exists x(x \otimes x = c_1 \oplus c_1)$. This sentence holds in \mathcal{R} as witnessed by any assignment α satisfying $\alpha(x) = \sqrt{2}$, but there is no closed \mathcal{L} -term t such that $\mathcal{R} \models t \otimes t = c_1 \oplus c_1$.

Let us expand $\mathcal{L} = \{\oplus, \otimes, c_0, c_1\}$ to $\mathcal{L}' = \{\oplus, \otimes, c_n : n \in \mathbb{N}\}$. Let

$$\mathcal{N}' = \langle \mathbb{N}, +, \cdot, n : n \in \mathbb{N} \rangle$$

(where each $n \in \mathbb{N}$ is the interpretation in \mathcal{N}' of the constant symbol c_n).

Then $T_{\mathcal{N}'}$ clearly has existential witnesses and for all \mathcal{L} -sentences ϕ , $\phi \in T_{\mathcal{N}'}$ if and only if $\phi \in T_{\mathcal{N}}$.

Similarly we can expand $\mathcal{L} = \{\oplus, \otimes, c_0, c_1\}$ to $\mathcal{L}^* = \{\oplus, \otimes, c_r : r \in \mathbb{R}\}$, let $\mathcal{R}^* = \langle \mathbb{R}, +, \cdot, r : r \in \mathbb{R} \rangle$ (where each $r \in \mathbb{R}$ is the interpretation in \mathcal{R}^* of the constant symbol c_r), and conclude that $T_{\mathcal{R}^*}$ has existential witnesses and $\phi \in T_{\mathcal{R}^*}$ if and only if $\phi \in T_{\mathcal{R}}$ for all \mathcal{L} -sentences ϕ .

Exercise 4.4. Prove that $T_{\mathcal{N}'}$ has the Henkin property and $\phi \in T_{\mathcal{N}'}$ if and only if $\phi \in T_{\mathcal{N}}$ for all \mathcal{L} -sentences ϕ .

Prove that the same holds for $T_{\mathcal{R}^*}$ with respect to $T_{\mathcal{R}}$.

More generally we can perform the same construction over any \mathcal{L} -theory T :

Proposition 4.5. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$ be a first order signature and T be an \mathcal{L} -theory. Assume $\mathcal{M} \models T$ with

$$\mathcal{M} = \langle M, R_i^{\mathcal{M}} : i \in I, f_j^{\mathcal{M}} : j \in J, c_k^{\mathcal{M}} : k \in K \rangle$$

an \mathcal{L} -structure with domain M . Let $\mathcal{L}' = \mathcal{L} \cup \{e_m : m \in M\}$ and

$$T' = T \cup \{\exists x \phi \rightarrow \phi[x/e_m] : \mathcal{M} \models \phi[x/m], \quad \exists x \phi \text{ an } \mathcal{L}'\text{-sentence}\}.$$

Then T' has the Henkin property. Moreover the \mathcal{L}' -structure $\mathcal{M}' \models T'$, where

$$\mathcal{M}' = \langle M, R_i^{\mathcal{M}} : i \in I, f_j^{\mathcal{M}} : j \in J, c_k^{\mathcal{M}} : k \in K, e_m^{\mathcal{M}} : m \in M \rangle$$

with $e_m^{\mathcal{M}} = m$ for all $m \in M$.

Definition 4.6. Let \mathcal{L} be a first order signature, and T be an \mathcal{L} -theory consisting of sentences. Let $\mathcal{L}' \supseteq \mathcal{L}$ be another first order signature, and T' be an \mathcal{L}' -theory also consisting of \mathcal{L}' -sentences.

- T' is a *consistent* extension of T over \mathcal{L} if $\phi \in T$ entails $\phi \in T'$ for all \mathcal{L} -sentences ϕ .
- T' is a *conservative* extension of T over \mathcal{L} if $\phi \in T$ if and only if $\phi \in T'$ for all \mathcal{L} -sentences ϕ .

Exercise 4.4 shows that $T_{\mathcal{N}'}$ is a conservative extension of $T_{\mathcal{N}}$ with the Henkin property. Proposition 4.5 generalizes this result to the theory of any \mathcal{L} -structure.

One of the main ingredients in the proof of the compactness theorem essentially amounts to prove a converse of 4.5, i.e. to show that complete finitely satisfiable theories with the Henkin property have a model.

Towards this aim it is important to give a different characterization of complete theories which is based on a maximality property with respect to finite satisfiability.

Definition 4.7. A theory T is *maximally satisfiable* if it is finitely satisfiable and there is no finitely satisfiable S properly containing T .

Fact 4.8. Assume T is maximally satisfiable, then:

- (a) for all sentences ϕ exactly one among ϕ and $\neg\phi$ is in T ,
- (b) for all $\phi_1, \dots, \phi_n \in T$ and ϕ such that $\phi_1 \dots \phi_n \models \phi$ we have that $\phi \in T$.

Proof.

- (a) If for some ϕ both ϕ and $\neg\phi$ are in T , T is not finitely satisfiable. Assume none of them is in T . Since T is maximally satisfiable we get that $T \cup \{\phi\}$ and $T \cup \{\neg\phi\}$ are both not finitely satisfiable. Hence there are $\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m$ all in T such that $\{\phi_1, \dots, \phi_n, \phi\}$, $\{\psi_1, \dots, \psi_m, \neg\phi\}$ are both not satisfiable. Hence also $\{\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m, \phi\}$ and $\{\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m, \neg\phi\}$ are both not satisfiable.

Now $\{\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m\} \subseteq T$, hence it is finitely satisfiable. Find a model \mathcal{M} of $\bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j$. Then

$$\begin{aligned} \bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j &\equiv \left(\bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j \right) \wedge (\phi \vee \neg\phi) \equiv \\ &\equiv \left(\bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j \wedge \phi \right) \vee \left(\bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j \wedge \neg\phi \right). \end{aligned}$$

Therefore

$$\mathcal{M} \models \left(\bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j \wedge \phi \right) \vee \left(\bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j \wedge \neg\phi \right)$$

This gives that either

$$\mathcal{M} \models \bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j \wedge \phi,$$

or

$$\mathcal{M} \models \bigwedge_{i=1}^n \phi_i \wedge \bigwedge_{j=1}^m \psi_j \wedge \neg\phi.$$

In one case we contradict the unsatisfiability of

$$\{\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m, \phi\},$$

in the other that of

$$\{\phi_1, \dots, \phi_n, \psi_1, \dots, \psi_m, \neg\phi\}.$$

- (b) Assume $\phi_1, \dots, \phi_n \in T$ and ϕ are such that $\phi_1 \dots \phi_n \models \phi$. If $\phi \notin T$, $\neg\phi \in T$, but $\phi_1 \dots \phi_n \models \phi$ if and only if $\{\phi_1 \dots \phi_n, \neg\phi\}$ is not satisfiable (see Fact 3.48). Then T is not finitely satisfiable, a contradiction.

□

We will not need the following remark in the remainder of the proof, but it is worth stating it.

Remark 4.9. Assume T is a maximally satisfiable \mathcal{L} -theory consisting of \mathcal{L} -sentences. Then any finitely satisfiable consistent extension of T over \mathcal{L} is also a finitely satisfiable conservative extension.

The first key Lemma is the following:

Lemma 4.10 (Henkin's lemma). *Let \mathcal{L} be a first order signature and T be a finitely satisfiable \mathcal{L} -theory.*

There is a language $\mathcal{L}' = \mathcal{L} \cup \{e_l : l \in L\}$ containing just new constant symbols, and a maximally satisfiable \mathcal{L}' -theory T' which has the Henkin property, and is a coherent extension of T over \mathcal{L} .

The second key Lemma is the following characterization of the theory of a \mathcal{M} -structure:

Lemma 4.11. *Assume T is a finitely satisfiable \mathcal{L} -theory which has the Henkin property.*

The following are equivalent:

- T is maximally satisfiable.
- $T = T_{\mathcal{M}}$ for some \mathcal{L} -structure \mathcal{M} .

Assume the two lemmas have been proved. The proof of the compactness theorem is given by the following argument:

Proof. Let T be a finitely satisfiable \mathcal{L} -theory with $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$.

By Lemma 4.10 there is a signature $\mathcal{L}' = \mathcal{L} \cup \{e_l : l \in L\}$ containing the new constant symbols $\{e_l : l \in L\}$ and a maximally satisfiable \mathcal{L}' -theory T' which is a coherent extension of T and has the Henkin property.

By Lemma 4.11 T' is satisfiable by a \mathcal{L}' -model

$$\mathcal{N} = \langle M, R_i^{\mathcal{N}} : i \in I, f_j^{\mathcal{N}} : j \in J, c_k^{\mathcal{N}} : k \in K, e_l^{\mathcal{N}} : l \in L \rangle.$$

It is clear that (see Fact 2.65)

$$\mathcal{M} = \langle M, R_i^{\mathcal{N}} : i \in I, f_j^{\mathcal{N}} : j \in J, c_k^{\mathcal{N}} : k \in K \rangle \models T.$$

□

We are left with the proof of the two key lemmas.

Proof of Lemma 4.11

Proof. Let $\mathcal{L} = \{R_i : i \in I, f_j : j \in J, c_k : k \in K\}$. If $T = T_{\mathcal{M}}$ for some \mathcal{L} -structure \mathcal{M} , we easily get that T is maximally satisfiable (useful exercise for the reader). Therefore we are left with the converse implication. We prove it.

Let $CT_{\mathcal{L}}$ be the set of closed \mathcal{L} -terms t (i.e. those \mathcal{L} -terms which do not have variable symbols occurring in them and whose interpretation does not depend on the assignment of a value to free variables). Define the relation \approx_T on $CT_{\mathcal{L}}$ by $t \approx_T s$ if and only if $(t = s) \in T$.

Claim 4.11.1. \approx_T has the following properties:

- (a) it is an equivalence relation on $CT_{\mathcal{L}}$;
- (b) for all terms $t \in CT_{\mathcal{L}}$ there is some constant symbol c such that $c \approx_T t$;
- (c) for all $t_1, \dots, t_n \in CT_{\mathcal{L}}$ and any R relation symbol in \mathcal{L} either $R(t_1, \dots, t_n) \in T$, or $\neg R(t_1, \dots, t_n) \in T$;
- (d) for any relation symbol R in \mathcal{L} of arity n , and all $t_1, \dots, t_n, s_1, \dots, s_n \in CT_{\mathcal{L}}$ such that $s_i \approx_T t_i$ for all $i = 1, \dots, n$,

$$R(t_1, \dots, t_n) \in T \quad \text{if and only if} \quad R(s_1, \dots, s_n) \in T;$$

- (e) for any function symbol f in \mathcal{L} of arity n , and all $t_1, \dots, t_n, s_1, \dots, s_n \in CT_{\mathcal{L}}$ such that $s_i \approx_T t_i$ for all $i = 1, \dots, n$,

$$(f(t_1, \dots, t_n) = f(s_1, \dots, s_n)) \in T.$$

Proof.

- (a) Assume $(t_1 = t_2), (t_2 = t_3) \in T$, since $t_1 = t_2, t_2 = t_3 \models t_1 = t_3$, by Fact 4.8(b), we get that $t_1 = t_3 \in T$ as well. Similarly we can check also the reflexivity and symmetry of \approx_T .
- (b) Let t be any \mathcal{L} -closed term. Remark that $t = t \models \exists x(x = t)$ for any closed term $t \in CT_{\mathcal{L}}$. Hence $\exists x(x = t) \in T$ (being $t = t$ a logical truth). By the Henkin property of T , we get that there is some constant symbol c such that $(c = t) \in T$, hence $c \approx_T t$.
- (c) by Fact 4.8(a), at least one among $R(t_1, \dots, t_n)$, or $\neg R(t_1, \dots, t_n)$ is in T .
- (d) By Fact 4.8(b), since

$$t_1 = s_1, \dots, t_n = s_n, R(t_1, \dots, t_n) \models R(s_1, \dots, s_n),$$

$$R(t_1, \dots, t_n) \in T \text{ implies } R(s_1, \dots, s_n) \in T.$$

Similarly we can prove the converse implication.

- (e) By Fact 4.8(b), since $t_1 = s_1, \dots, t_n = s_n \models f(t_1, \dots, t_n) = f(s_1, \dots, s_n)$,

$$f(t_1, \dots, t_n) = f(s_1, \dots, s_n) \in T.$$

□

Let $M_T = \text{CT}_{\mathcal{L}}/\approx_T$ and $[t]$ denote the equivalence class in M_T of $t \in \text{CT}_{\mathcal{L}}$. Set for any function symbol f of ariety n

$$f^* : M_T^n \rightarrow M_T \\ \langle [t_1], \dots, [t_n] \rangle \mapsto [f(t_1, \dots, t_n)],$$

and for any relation symbol R of ariety n

$$\langle [t_1], \dots, [t_n] \rangle \in R^* \quad \text{if and only if} \quad R(t_1, \dots, t_n) \in T.$$

Claim 4.11.2. $\langle M_T, R_i^* : i \in I, f_j^* : j \in J, [c_k] : k \in K \rangle$ is an \mathcal{L} -structure.

Proof. By Claim 4.11.1, the functions f_j^* are well defined for all $j \in J$, and R_i^* is a well defined relation on $M_T^{n_i}$ for all $i \in I$. □

Claim 4.11.3. *Let*

$$\mathcal{M} = \langle M, R_i^* : i \in I, f_j^* : j \in J, [c_k] : k \in K \rangle.$$

Then

$$\mathcal{M} \models \phi(x_1, \dots, x_n)[x_1/[c_1], \dots, x_n/[c_n]]$$

if and only if

$$\phi[x_1/c_1, \dots, x_n/c_n] \in T.$$

By the Claim we get that $T = T_{\mathcal{M}}$, concluding the proof. We prove the Claim.

Proof. Let ϕ be an atomic formula of type $R(t_1(x_1, \dots, x_m), \dots, t_n(x_1, \dots, x_m))$. Then

$$\mathcal{M} \models R(t_1(x_1, \dots, x_m), \dots, t_n(x_1, \dots, x_m))[x_i/[c_i] : i = 1, \dots, m]$$

if and only if (since the closed terms $t_1[x_1/c_1, \dots, x_n/c_m], \dots, t_n[x_1/c_1, \dots, x_n/c_m]$ gets the same evaluation of the terms $t_1(x_1, \dots, x_m), \dots, t_n(x_1, \dots, x_m)$ when x_i is assigned to $[c_i]$ for $i = 1, \dots, m$, see Fact 2.51).

$$\mathcal{M} \models R(t_1[x_1/c_1, \dots, x_n/c_m], \dots, t_n[x_1/c_1, \dots, x_n/c_m])$$

if and only if

$$\langle [t_1[x_1/c_1, \dots, x_n/c_m]], \dots, [t_n[x_1/c_1, \dots, x_n/c_m]] \rangle \in R^*$$

if and only if

$$R(t_1[x_1/c_1, \dots, x_n/c_m], \dots, t_n[x_1/c_1, \dots, x_n/c_m]) \in T.$$

Hence the Claim holds for atomic formulae.

Now we proceed by induction on the logical complexity of ϕ . Assume the Claim holds for ϕ, ψ . We handle each logical operator as follows:

Case for $\phi \wedge \psi$:

$$\mathcal{M} \models \phi \wedge \psi[x_i/[c_i] : i = 1 \dots, m]$$

if and only if

$$(\mathcal{M} \models \phi[x_i/[c_i] : i = 1 \dots, m] \text{ and } \mathcal{M} \models \psi[x_i/[c_i] : i = 1 \dots, m])$$

if and only if (by inductive assumptions on ϕ, ψ)

$$(\phi \llbracket x_1/c_1, \dots, x_m/c_m \rrbracket \in T \text{ and } \psi \llbracket x_1/c_1, \dots, x_m/c_m \rrbracket \in T)$$

if and only if (by Fact 4.8(b))

$$\phi \wedge \psi \llbracket x_1/c_1, \dots, x_n/c_n \rrbracket \in T.$$

Case for $\neg\phi$:

$$\mathcal{M} \models \neg\phi[x_i/[c_i] : i = 1 \dots, m]$$

if and only if

$$\mathcal{M} \not\models \phi[x_i/[c_i] : i = 1 \dots, m]$$

if and only if (by inductive assumptions on ϕ)

$$\phi \llbracket x_1/c_1, \dots, x_m/c_m \rrbracket \notin T$$

if and only if (by Fact 4.8(a))

$$\neg\phi \llbracket x_1/c_1, \dots, x_n/c_n \rrbracket \in T.$$

Case for $\exists x\phi$:

$$\mathcal{M} \models \exists x\phi[x_i/[c_i] : i = 1 \dots, m]$$

if and only if

$$\text{For some } [c] \in M_T \mathcal{M} \models \phi[x/[c], x_i/[c_i] : i = 1 \dots, m]$$

if and only if (by inductive assumptions on ϕ)

$$\text{For some } [c] \in M_T \phi \llbracket x/c, x_1/c_1, \dots, x_n/c_n \rrbracket \in T$$

if and only if (for \Leftarrow use the Henkin property of T , for \Rightarrow use Fact 4.8(b))

$$\exists x\phi \llbracket x_1/c_1, \dots, x_n/c_n \rrbracket \in T.$$

By Fact 2.48 this suffices. □

The Lemma is proved in all its parts. □

Proof of Lemma 4.10

The proof of this Lemma uses a recursive procedure to define theories T_n and languages \mathcal{L}_n such that:

- $T_0 = T$.
- $\mathcal{L}_0 = \mathcal{L}$.
- At odd stages $2n + 1$ we extend the \mathcal{L}_n -theory T_{2n} to a *maximally satisfiable* \mathcal{L}_n -theory T_{2n+1} .
- At even stages $2n + 2$ we extend \mathcal{L}_n to

$$\mathcal{L}_{n+1} = \mathcal{L}_n \cup \{e_\phi^n : \phi \text{ a } \mathcal{L}_n\text{-formula in at most one free variable}\},$$

and the maximally satisfiable \mathcal{L}_n -theory T_{2n+1} to a \mathcal{L}_{n+1} -theory $T_{2n+2} \supseteq T_{2n+1}$ which:

- has the Henkin property with respect to all existential formulae in T_{2n+1} (i.e. for all \mathcal{L}_n -formulae ϕ in at most one free variable x such that $T_{2n+1} \models \exists x \phi$, there is e_ϕ^n such that $\phi \llbracket x/e_\phi^n \rrbracket \in T_{2n+2}$),
- is finitely satisfiable,
- is a coherent extension of T_{2n+1} .

Assume this construction can be carried. Then the following holds:

Claim 4.11.4. *Let $\mathcal{L}' = \bigcup_{n \in \mathbb{N}} \mathcal{L}_n$ and $T' = \bigcup_{n \in \mathbb{N}} T_n$. Then T' is a maximally satisfiable \mathcal{L}' -theory which is a coherent extension of T .*

Proof.

T' is a coherent extension of T : clear since $T = T_0 \subseteq T'$.

T' is finitely satisfiable: Any finite set of formulae Γ in T' appears in some T_{2n} which is finitely satisfiable in some \mathcal{L}_n -structure \mathcal{M} with domain M . We can interpret the remaining constants of $\mathcal{L}' \setminus \mathcal{L}_n$ in M as we like, so to extend \mathcal{M} to an \mathcal{L}' -structure which is still a model of Γ .

T' has the Henkin property: Any sentence in T' appears in some T_n , hence at stages $2n + 2$ existential witnesses for it have been added.

T' is maximally satisfiable: If $S \supseteq T'$ find $\psi \in S \setminus T'$. Then ψ is an \mathcal{L}_n -sentence for some odd n , hence $\neg\psi \in T_{n+1} \subseteq T$ (since $\psi \notin T \supseteq T_{n+1}$ and T_{n+1} is maximally consistent). This gives that $\psi, \neg\psi \in S$, therefore S is not finitely satisfiable.

□

To complete the proof of Lemma 4.10 we must show that the above construction can be performed.

The following proposition handles the odd stages of the construction:

Proposition 4.12. *Let \mathcal{L} be a first order signature and T be a finitely satisfiable \mathcal{L} -theory.*

Then T can be extended to a maximally satisfiable, \mathcal{L} -theory T' .

We give two proofs of this proposition:

First proof.

Proof. Let

$$\mathcal{A} = \{S \supseteq T : S \text{ is a finitely satisfiable } \mathcal{L}\text{-theory}\}$$

Exercise 4.13. Show that whenever $F \subseteq \mathcal{A}$ is such that (F, \subseteq) is a linear order, $\bigcup F \in \mathcal{A}$.

By Zorn's lemma \mathcal{A} has a maximal element T' . Clearly $T' \supseteq T$ is maximally satisfiable. \square

Second proof.

Proof. Let T be a finitely satisfiable theory over the language \mathcal{L} . Consider the equivalence relation on the set of \mathcal{L} -sentences given by logical equivalence. Let $[\phi]$ denote the equivalence class of an \mathcal{L} -sentence ϕ . Let $\mathbf{B}_{\mathcal{L}}$ be the boolean algebra

$$\{[\phi] : \phi \text{ an } \mathcal{L}\text{-sentence}\}$$

with boolean operations $[\phi] \wedge [\psi] = [\phi \wedge \psi]$, $[\phi] \vee [\psi] = [\phi \vee \psi]$, $\neg[\phi] = [\neg\phi]$.

Exercise 4.14. Check that $\mathbf{B}_{\mathcal{L}}$ with boolean operations defined above is a boolean algebra with top element $[\phi \vee \neg\phi]$ and bottom element $[\phi \wedge \neg\phi]$ for some (any) ϕ . Check also that $[\phi] \leq_{\mathbf{B}_{\mathcal{L}}} [\psi]$ if and only if $\phi \models \psi$.

Exercise 4.15. For any set S of \mathcal{L} -sentences, let $I_S = \{[\phi] : S \models \neg\phi\}$. Prove that I_S is a proper ideal on $\mathbf{B}_{\mathcal{L}}$ if and only if S is finitely satisfiable.

By the Prime Ideal Theorem [2, Thm 2.2.30], let $I \supseteq I_T$ be a prime ideal on $\mathbf{B}_{\mathcal{L}}$. Let $T' = \{\phi : [\neg\phi] \in I\}$.

Claim 4.15.1. $T' \supseteq T$ is a maximally satisfiable theory.

Proof. Clearly $T' \supseteq T$.

T' is finitely satisfiable: If not there are $\phi_1, \dots, \phi_n \in T'$ such that $\phi_1, \dots, \phi_n \models \phi \wedge \neg\phi$. This gives that $[\neg(\phi \wedge \neg\phi)] \in I$, contradicting that I is a proper ideal.

T' is maximally satisfiable: Assume $S \supset T'$ is finitely satisfiable with $\phi \in S \setminus T'$. Then $I_S = \{[\psi] : S \models \neg\psi\}$ is a proper ideal strictly containing I , since $[\neg\phi] \in I_S \setminus I$. This contradicts the maximality of I .

The Claim is proved. \square

The Proposition is proved. \square

The following proposition handles the even stages of the recursive construction.

Proposition 4.16. *Let \mathcal{L} be a first order signature and T be a finitely satisfiable \mathcal{L} -theory.*

Let

$$\mathcal{L}' = \mathcal{L} \cup \{e_\phi : \phi \text{ an } \mathcal{L}\text{-formula in at most one free variable } x\},$$

with

$$C' = \{e_\phi : \phi \text{ an } \mathcal{L}\text{-formula in at most one free variable } x\}$$

a new set of constant symbols disjoint from \mathcal{L} . Define

$$T' = T \cup \{(\exists x\phi) \rightarrow (\phi[x/e_\phi]) : e_\phi \in C'\}.$$

Then:

- *T' has the Henkin property with respect to all existential sentences in T (i.e. for all \mathcal{L} -sentences $\exists x\phi$ such that $T \models \exists x\phi$, $T' \models \phi[x/e_\phi]$),*
- *T' is finitely satisfiable,*
- *T' is a coherent extension of T .*

Proof. The unique delicate point is to check that T' is finitely satisfiable. Given a finite subset Γ of T' , find \mathcal{M} model of

$$\Delta = (\Gamma \cap T)$$

with domain M (\mathcal{M} exists by the finite satisfiability of T).

For each \mathcal{L} -formula ϕ in at most one free variable x such that $\mathcal{M} \models \exists x\phi$, let $a_\phi \in M$ be such that

$$\mathcal{M} \models \phi[x/a_\phi].$$

Consider the \mathcal{L}' -structure \mathcal{M}^* for \mathcal{L}' , with domain M and interpretation of all symbols in \mathcal{L} equal to the interpretation of these symbols in \mathcal{M} , and evaluation of the new constant symbols $e_\phi \in C'$ by the requirement that

- $e_\phi^{\mathcal{M}^*} = a_\phi$ if $\mathcal{M} \models \exists x\phi$,
- $e_\phi^{\mathcal{M}^*} = a$ for some fixed $a \in M$ otherwise.

Then $\mathcal{M}^* \models \Gamma$: On the one hand it models Δ . On the other hand \mathcal{M}^* models all sentences $(\exists x\phi) \rightarrow (\phi[x/e_\phi])$ for all $e_\phi \in C'$, since :

- either $\mathcal{M}^* \not\models \exists x\phi$ (since $\mathcal{M} \not\models \exists x\phi$),
- or $\mathcal{M}^* \models \phi[x/e_\phi]$ (since $\mathcal{M} \models \phi[x/a_\phi]$ and $e_\phi^{\mathcal{M}^*} = a_\phi$).

Since Γ was chosen arbitrarily among the finite subsets of T' , we get that T' is finitely satisfiable. \square

By these two propositions we can perform the construction sketched at the beginning of this section and complete the proof of Lemma 4.10.

Sketch of proof for the completeness theorem

A proof of the completeness theorem can go as follows:

- A \mathcal{L} -theory T is *consistent* if $T \not\vdash \phi \wedge \neg\phi$.
- A \mathcal{L} -theory T is *maximally consistent* if no $S \supsetneq T$ is consistent.

In all the results and definitions of the previous section replace *finitely satisfiable* with *consistent* and *maximally satisfiable* with *maximally consistent*, in most arguments the semantic notion of logical consequence \models must be replaced with the syntactic notion of derivability \vdash . Check that all proofs of the relevant claims go through mutatis-mutandis. This gives that T is satisfiable if T is consistent i.e. the completeness theorem.

5 First order logic and set theory

We give some brief comments on how first order logic can be developed inside set theory. First of all \mathcal{L} -formulae and \mathcal{L} -terms are strings over the alphabet $\mathcal{L} \cup \text{Symb}$ where

$$\text{Symb} = \{\wedge, \vee, \rightarrow, (,), \forall, \exists, \neg\} \cup \{, \} \cup \{x_n : n \in \mathbb{N}\}.$$

All over these notes (with the exception of the preceding section) we just focused on countable (or even finite) languages. We may assume that a first order signature \mathcal{L} is identified with a subset of $\mathbb{N} \times \{0, 1, 2, 3\} \times \mathbb{N}$, with the convention that a triple of type $(n, 0, m)$ is a relation symbol of arity m , a triple of type $(n, 1, m)$ is a function symbol of arity m , a triple of type $(n, 2, m)$ is a constant symbol, a triple of type $(n, 3, m)$ is a symbol in Symb .

- Strings over \mathcal{L} corresponds to the set $(\mathcal{L} \cup \text{Symb})^{<\mathbb{N}}$.
- \mathcal{L} -formulae and \mathcal{L} -terms can be recognized inside $(\mathcal{L} \cup \text{Symb})^{<\mathbb{N}}$ using suitable instances of the separation axiom.
- Finitely satisfiable theories form a proper subset of $\mathcal{P}((\mathcal{L} \cup \text{Symb})^{<\mathbb{N}})$ defined by a suitable instance of the separation axiom.
- \mathcal{L} -structures can be seen as functions $\mathcal{M} : (\{*\} \cup \mathcal{L}) \rightarrow (\mathcal{P}(M^{<\mathbb{N}}) \cup M)$ which assign to $*$ the domain M of the structure, to each relation and function symbol in \mathcal{L} the appropriate subset of $\mathcal{P}(M^{<\mathbb{N}})$, and to each constant symbol of \mathcal{L} an element of M .
- Over any set M one can define an \mathcal{L} -structure having that set as domain. Hence it is easy to check that the family of \mathcal{L} -structures is always a proper class.

All the results presented in the previous sections can be formulated as set theoretical statements asserting that certain sets and classes exist and have certain properties.

References

- [1] Alessandro Andretta, *Elementi di logica matematica*, 2014.
- [2] Matteo Viale, *Notes on forcing*, 2017.