LOGICS
lecture notes

Géraud Sénizergues

Year 2013-2014 [1]

[1] last update: September 5, 2013

Contents

Introduction

This part of the course mainly focuses on "proof-theory": it consists in studying proofs within formal systems.

Historical origins .
Let us try to give a (very) short and sketchy historical account on the evolution of logics and mathematics (we refer the reader to [Gui78] for an historical overview of mathematical logics and [Dow07] for some reflexion about the interconnections between the deductive and the computational aspects of mathematics).

For a long period (-300–1850) logics and mathematics were two different areas of knowledge:
- logics was the study of *reasoning*; it focused on the correct forms of reasoning i.e. thoses which, surely, allowed to move from true assumptions to true conclusions.
- mathematics was the study of *numbers and space*, viewed as modelizations of some aspects of the physical world.

At the end of the 19th century (1850–1900), several new ideas created strong links between logics and mathematics:
- after the works of G.Boole and others, it appeared that the correct ways of reasoning could be described by some adapted algebraic structures (nowadays named "Boolean" algebras); it was later remarked (by H.Stone) that it could be achieved by means of the classical notion of ring, a structure

which was already used in number theory and geometry. Pushing further the mathematical treatment of logics, G.Frege created a precise mathematical notion of "correct reasoning", strong enough to express all mathematics. This is what we nowadays call formal mathematics.
- mathematicians got progressively convinced that their discoveries were less concerning some parts of the physical world than *deduction* by itself: a theorem is nothing else than a statement that must be true, as soon as the *axioms* are true. The questions of defining exactly what are numbers, points, straight lines became irrelevant; accordingly, the question whether numbers, points, straight-lines were really fulfilling the axioms, did not make sense any more.
- this change of thought about the nature of mathematical statements was contemporary with a development of precise systems of axioms for geometry, number theory, analysis by G.Peano, M.Pieri, D.Hilbert and others.
- at this time also appeared *set theory*, created by G.Cantor, which became a unified framework in which one could express all of mathematics; set theory itself was founded on an axiomatic ground by E.Zermelo and others.

Recently, after the appearance of computers, it became possible to compute effectively formal proofs for non-trivial theorems. Some pratical achievements in this direction were obtained in the 1970ś by N.De Bruijn (he converted a full analysis treatise by Landau into formal mathematics). Such formal proofs can be obtained by the interaction of a human-being (with strong mathematical culture) with a program, the *proof-assistant*.

One of the major proof-assistant which is now available is *COQ*. With the help of such a program formal proofs of theorems that could not be achieved by human beings, even within usual non-formal mathematics, were realized: this is the case of the "four color theorem", stating that every planar map can be coloured with only four different colors in such a way that every pair of regions with a non-trivial common frontier have different colors.

Questions After having modelized mathematical proofs by derivations in a formal system (we shall consider in this course 4 formal systems called $\mathsf{NJ}, \mathsf{NK}, \mathrm{LJ}, \mathrm{LK}$) we can then handle mathematically, questions about mathematical reasoning. Some (metamathematical) natural questions are:

Q1: Are the above formal systems *consistent*? i.e. are they able to prove the false constant ? (i.e. the most obviously false statement that we can imagine). We expect they do not allow such a stupid derivation. But we would like to demonstrate this property just by examining the combinatorial properties of the systems i.e. by forgetting its relation with reasoning and considering it, merely, as a special kind of formal grammar; the question then becomes "does this grammar generate the word $\bot$?

Q2: What is the relation between "truth" and "provability"? We of course expect that every provable statement is true (though to make sure of this is not easy and is what Q1 asks for). But does a converse hold ?

Q3: Can we decide whether a formal statement (i.e. a formula) is true ?

Q4: Can we decide whether a formal statement is provable ? The reader might already have a pratical experience of searching formal proofs with the help of some proof-assistant. But is there an *algorithm* able to tell whether a formal proof exists ?

Q5: Does provability of the statement $\forall x \exists y \ \Phi(x,y)$ ensure that "y is computable from x" ? We guess that, if a proof of the existence of y is abstract enough, we shall not be able to extract from it even a single example of y fulfilling $\Phi(x,y)$. Since the *intuitionism* was developed (historically) as an opposition to the abuse of abstraction in proofs, it is natural to examine to what extent an intuitionistic proof of a statement of the form $\forall x \exists y \ \Phi(x,y)$ is enough to guaranty that from every concrete x we can effectively produce a corresponding y such that $\Phi(x,y)$.

Answers This course brings several (partial) answers to these questions.

In chapter 1 we describe carefully the basic ingredients of mathematical proofs: terms, formulas, bindings, substitutions. We then define a formal

system called *natural deduction* (NK) as well as its intuitionistic variant (NJ).

In chapter 2, we define an alternative formal system called *sequent calculus* (LK) and its intuitionistic variant (LJ). We show that, up to some simple translations, natural deduction as well as sequent calculus generate the same set of judgments.

In chapter 3 we show a major property of derivations in system LK called the *cut elimination theorem*. We then deduce from this property that LK is consistent (which answers Q1) and that LJ is constructive, which answers Q5 in the case of predicate calculus i.e. of mathematics without any axioms. We then examine to which kinds of axiomatic theories this constructivity property can be extended.

In chapter 4 we define a notion of "truth" for the judgments of our formal systems. We are then in a position to compare (from the outside) the set of true judgments with the set of provable judgments. We state the *accuracy theorem* for predicate calculus which is a first answer to Q2. We then define a notion of "intuitionistic truth" and state that the accuracy theorem remains valid for the intuitionistic versions of natural deduction or sequent calculus (on the side of proofs) and this intuitionistic notion of truth. It will be seen through exercises that, when we focus on truth in a given mathematical structure (typically the set of integers $\mathbb{N}$ endowed with sum, product and equality), there must exist some judgments which are true but not provable. This is another answer to Q2. By the same kind of considerations we shall see that, in general, provability, as well as truth, are not decidable (this answers Q3,Q4 in some "bad" cases).

In chapter 5, we study a "good" case, i.e. a mathematical structure (namely the integers endowed with sum and equality) where it is possible to "decide thruth" for statements (this is another partial answer to Q3) by a reduction to finite automata theory.

Chapter 1

Natural Deduction

1.1 Formulas

Let us call *signature* a sequence of predicate symbols followed by a sequence of function symbols together with an aruty for every symbol:

$$\mathcal{S} := \langle R_1, R_2, \ldots, R_n; f_1, f_2, \ldots, f_m \rangle$$

with the arities

$$\langle r_1, r_2, \ldots, r_n; a_1, a_2, \ldots, a_m \rangle$$

Let

$$\mathcal{V} := \{v_0, v_1, \ldots, v_n, \ldots\}$$

be a denumerable set. We call variables the elements of $\mathcal{V}$. Every variable has an arity 0. Let

$$\mathcal{C} := \{\wedge, \vee, \rightarrow, \neg, \bot\}$$

be the set of *connectors*, and

$$\mathcal{Q} := \{\forall, \exists\}$$

be the set of *quantifiers*.

Definition 1.1.1 *The set of* terms *over the signature $\mathcal{S}$ and the set of variables $\mathcal{V}$, is the set of words generated by the grammar:*

$$\begin{array}{lcl} T \to & v & \text{for } v \in \mathcal{V} \\ T \to & f_j(T, \ldots, T) & \text{for } 1 \leq j \leq m \end{array}$$

We denote by $\mathcal{T}(\mathcal{S}, \mathcal{V})$ the set of these terms.

Definition 1.1.2 *The set of* formulas *over the signature $\mathcal{S}$ and the set of variables $\mathcal{V}$ is the set of words generated by the following grammar $\mathcal{G}_1$, over the terminal alphabet $\mathcal{S} \cup \mathcal{V} \cup \mathcal{C} \cup \mathcal{Q} \cup \{(,), \underline{,}\}$ and the non-terminal alphabet $\{T, F\}$:*

$$\begin{array}{lcl} T \to & v & \text{for } v \in \mathcal{V} \\ T \to & f_j(T \underline{,} \ldots \underline{,} T) & \text{for } 1 \leq j \leq m \\ F \to & R_i(T \underline{,} \ldots \underline{,} T) & \text{for } 1 \leq i \leq n \\ F \to & (F \diamond F) & \text{for } \diamond \in \{\wedge, \vee, \to\} \\ F \to & \neg F & \\ F \to & \bot & \\ F \to & Qv \ F & \text{for } Q \in \mathcal{Q}, v \in \mathcal{V} \end{array}$$

Example 1.1.3 *Let $\mathcal{S} := \langle EG; S, P\rangle$ with arities $\langle 2; 2, 2\rangle$. Then*

$$\Phi := \forall x \ \exists y_1 \ \exists y_2 \ \exists y_3 \ \exists y_4 \ \ EG(x, S(P(y_1, y_1), S(P(y_2, y_2), S(P(y_3, y_3), P(y_4, y_4)))))$$

is a formula; if we think of EG as denoting the equality predicate and of S (resp. P) as denoting the sum (resp. the product) of integers, this formula expresses, intuitively, the fact that every natural integer is the sum of four squares of integers.

(In the sequel we often replace the terminal letter $\underline{,}$ by the symbol , when no confusion with the meta-character is possible). We denote by $\mathcal{L}_1(\mathcal{S}, \mathcal{V})$ the

set of these formulas. They are called first-order formulas over the signature $\mathcal{S}$ and the set of variables $\mathcal{V}$.
Every formula Φ is mapped to a planar tree $P(\Phi)$, labeled over $\mathcal{S} \cup \mathcal{V}$ in the following way:
- the grammar $\mathcal{G}_1$ is unambiguous
- therefore , every formula Φ is generated through a unique construction term $CT(\Phi)$ i.e. planar tree, where the nodes are labeled by the rules of $\mathcal{G}_1$ and such that, if the rule $N \to w$ is the rule labelling a node u, then the arity of this node is equal to $|w|_{\{T,F\}}$ and the label of the i-th son of u is a rule with lhs the i-th occurrence of a non-terminal in the word w.
- we define the tree $P(\Phi)$ by: $\mathrm{Dom}(P(\Phi)) := \mathrm{Dom}(CT(\Phi))$ and, for every $u \in \mathrm{Dom}(P(\Phi))$

$$
\begin{array}{rcll}
\text{if } CT(\Phi)(u) = & T \to v & \text{and } v \in \mathcal{V} \\
\text{then } P(\Phi)(u) := & v & \\
\text{if } CT(\Phi)(u) = & T \to f_j(\underset{\_}{T}, \ldots, \underset{\_}{T}) & \text{and } 1 \leq j \leq m \\
\text{then } P(\Phi)(u) := & f_j & \\
\text{if } CT(\Phi)(u) = & F \to R_i(\underset{\_}{T}, \ldots, \underset{\_}{T}) & \text{and } 1 \leq i \leq n \\
\text{then } P(\Phi)(u) := & R_i & \\
\text{if } CT(\Phi)(u) = & F \to (F \diamond F) & \text{and } \diamond \in \{\wedge, \vee, \to\} \\
\text{then } P(\Phi)(u) := & \diamond & \\
\text{if } CT(\Phi)(u) = & F \to \neg F & \\
\text{then } P(\Phi)(u) := & \neg & \\
\text{if } CT(\Phi)(u) = & F \to \bot & \\
\text{then } P(\Phi)(u) := & \bot & \\
\text{if } CT(\Phi)(u) = & F \to Qv \;\; F & \text{for } Q \in \mathcal{Q}, v \in \mathcal{V} \\
\text{then } P(\Phi)(u) := & Qv & .
\end{array}
$$

For the formula Φ of Example 1.1.3, the tree $P(\Phi)$ is depicted on figure 1.1.

1.2 Bindings

We describe in this section the notion of *bindings* between positions in a formula. The general idea is that an occurrence of a variable v in a formula

Φ can be bound by some position, more on the left, where the factor $\forall v$ or $\exists v$ appears. We shall examine in details how these bindings can be defined, in some algorithmic way, and how the names of the bound variables can be changed, if necessary , in order to avoid some unexpected effects of substitutions. We thus prepare the ground for a definition of *substitution* that behaves correctly w.r.t truth.

Let $\Phi \in \mathcal{L}_1(\mathcal{S}, \mathcal{V})$and $P(\Phi)$ its associated planar tree. Let p be a *position* of the formula Φ i.e. and element p of the domain of $P(\Phi)$. We call p an *occurrence* of the variable $v \in \mathcal{V}$ if

$$P(\Phi)(p) = v.$$

This occurrence of v is *free* iff

$$\forall q \in \mathrm{Dom}(P(\Phi)), \;\; q \preceq p \Rightarrow P(\Phi(q)) \notin \{\forall v, \exists v\}.$$

In words: p is free if there is not ancestor of this node p which is labelled by a qiuantification of v. This occurrence of v is *bound* by the quantification in position $q \in \mathrm{Dom}(P(\Phi))$ iff

$$q \preceq p \quad \text{and} \quad P(\Phi(q)) \in \{\forall v, \exists v\} \quad \text{and}$$

$$\forall r \in \mathrm{Dom}(P(\Phi)), \;\; q \prec r \prec p \Rightarrow P(\Phi(q)) \notin \{\forall v, \exists v\}.$$

In words: p is bound by position q, if the label of q is a quantification of the variable v and, there is no other such quantification strictly between p and q. We denote by $\mathrm{FV}(\Phi)$ the set of variables v that have at least one free occurrence in Φ.
N.B. A given variable v may have both a free occurrence p in Φ and a bound occurrence p' in Φ.

Example 1.2.1 *Let*

$$\Phi_1 := \forall v_1 \;\; (I(v_1, v_1) \vee (\exists v_1 \;\; EG(v_1, 0))).$$

(see its associated planar tree on figure 1.2). The set of occurrences of v_1 *is* $\{000, 001, 0100\}$. *The occurrences* $000, 001$ *are bound by the quantification* $\forall v_1$ *at position* ε. *The occurrence* 0100 *is bound by the quantification* $\exists v_1$ *at position* 01. *Thus* $FVar(\Phi_1) = \emptyset$

$$\Phi_2 := \forall v_2 \;\; (I(v_1, v_1) \vee (\exists v_1 \;\; EG(v_1, v_2))).$$

(see its associated planar tree on figure 1.3).

The set of occurrences of v_1 *is still* $\{000, 001, 0100\}$. *The occurrences* $000, 001$ *are free. The occurrence* 0100 *is bound by the quantification* $\exists v_1$ *at position* 01. *The set of occurrences of* v_2 *is* $\emptyset$. *Thus* $FVar(\Phi_2) = \{v_1\}$.

Let us define a partition of the set of positions of a formula, according to its status concerning variables. Let Φ be some formula. let us abbreviate $\mathrm{Dom}(P(\Phi))$ as $\mathrm{D}(\Phi)$ and $P(\Phi)(p)$ as $\Phi(p)$. The set $\mathrm{D}(\Phi)$ is partitionned into three subsets:

$$\begin{array}{rcl} \mathrm{D}_c(\Phi) & := & \{p \in \mathrm{Dom}(P(\Phi)) \mid P(\Phi)(p) \in \mathcal{S} \cup Con\} \\ \mathrm{D}_{vl}(\Phi) & := & \{p \in \mathrm{Dom}(P(\Phi)) \mid P(\Phi)(p) \in \mathcal{V} \text{ and this position is free}\} \\ \mathrm{D}_q(\Phi) & := & \{p \in \mathrm{Dom}(P(\Phi)) \mid (P(\Phi)(p) \in \mathcal{V} \text{ and this position is bound}) \\ & & \text{or } (P(\Phi)(p) \in \mathcal{QV}\} \end{array}$$

We the define the binary relation $\mathcal{L}(\Phi)$ over $\mathrm{D}_q(\Phi)$ by:

$$\mathcal{L}(\Phi) := \{(p, p') \in \mathrm{D}_q(\Phi) \times \mathrm{D}_q(\Phi) \mid \Phi(p) \in \mathcal{V} \text{ and this occurrence is bound by } \Phi(p') \in \mathcal{QV}\}$$

(Every ordered pair $(p, p') \in \mathcal{L}(\Phi)$ is a link, hence the letter $\mathcal{L}$ for designating this relation).

It is intuitively clear, for anybody aquainted with mathematical language, that a statement like:

$$\forall x \ \ (\neg(x = u)) \Rightarrow (\exists y \ \ x = y + 1)$$

says the same thing (about the object designated by u) as the statement:

$$\forall y \ \ (\neg(y = u)) \Rightarrow (\exists z \ \ y = z + 1)$$

The fact that these statement have the same meaning is analogous with the fact that the two expressions have the same meaning. Yet another case of such an equivalence of notation is the fact that the functions:

$$(x, y) \mapsto x^2 + y \cdot u, \quad (y, z) \mapsto y^2 + z \cdot u$$

depending on the parameter u, are the same; within the notation of λ calculus:

$$\lambda x \cdot \lambda y \cdot ((S((Px)x))((Py)u)) \quad \lambda y \cdot \lambda z \cdot ((S((Py)y))((Pz)u))$$

are two equivalent terms. In all the above examples the variables x, y (resp. y, z) are bound; the "names" (i.e. variables) x, y play some intermediate role in defining the meaning of the full formula, but the final formula has a meaning independant of the precise names that have been used.

Let us give here a formal definition of this equivalence, which is denoted by $\equiv_\alpha$.

Definition 1.2.2 *Let $\Phi, \Psi \in \mathcal{L}_1(\mathcal{S}, \mathcal{V})$. The formula Φ, Ψ are called* α-equivalent*, which is denoted by $\Phi \equiv_\alpha \Psi$, iff*
(1) $\mathrm{D}_c(\Phi) = \mathrm{D}_c(\Psi),\ \ \mathrm{D}_{vl}(\Phi) = \mathrm{D}_{vl}(\Psi),\ \ \mathrm{D}_q(\Phi) = \mathrm{D}_q(\Psi)$
(2) $\forall p \in \mathrm{D}_c(\Phi) \cup \mathrm{D}_{vl}(\Phi),\ \ \Phi(p) = \Psi(p)$
(3) $\mathcal{L}(\Phi) = \mathcal{L}(\Psi)$
(4) $\forall p \in \mathrm{D}_q(\Phi), \forall Q \in \mathcal{Q},\ \ \Phi(p) \in Q\mathcal{V} \Leftrightarrow \Psi(p) \in Q\mathcal{V}$.

Lemma 1.2.3 *Let $\Phi \in \mathcal{L}_1(\mathcal{S}, \mathcal{V})$. and V be a finite subset of $\mathcal{V}$. Then one can construct a formula $\Phi' \in \mathcal{L}_1(\mathcal{S}, \mathcal{V})$ such that*
(1) $\Phi \equiv_\alpha \Phi'$
(2) $\forall v \in V, \forall Q \in \mathcal{Q}$, *$Qv$ has no occurrence in Φ'.*

Proof:Let us consider an enumeration, without repetition, of the set $\mathcal{V} \setminus (V \cup \mathrm{FV}(\Phi))$:

$$v_0, v_1, \ldots, v_n, \ldots$$

Let Φ' be the formula defined by:

$$\mathrm{D}(\Phi') := \mathrm{D}(\Phi)$$

$$\forall p \in \mathrm{D}_c(\Phi) \cup \mathrm{D}_{vl}(\Phi),\ \ \Phi'(p) := \Phi(p),$$

$$\forall p \in \mathrm{D}_q(\Phi),\ \text{if } \Phi(p) \in Q\mathcal{V},\ \text{then } \Phi'(p) := Qv_{I(p)},$$

where $I(p) := \mathrm{Card}\{q \in \mathrm{D}_q(\Phi) \mid q <_{\mathrm{lex}} p \wedge \Phi(q) \in \mathcal{Q}\mathcal{V}\}$

$$\forall p \in \mathrm{D}_q(\Phi),\ \text{if } \Phi(p) \in \mathcal{V},\ \text{then } \Phi'(p) := v_{I(p')},$$

where $(p, p') \in \mathcal{L}(\Phi)$.
One can check that $\Phi \equiv_\alpha \Phi'$ $\square$

1.3 Substitutions

In the ordinary mathematical (informal) discourse, we often use the following procedure: we establish thet a statement Φ is true for some *general* object v (general means that we did not make any assumption about v). Then, we replace v by the description of some *particular* object t and we infer, from the truth of statement Φ that the statement obtained by *substitution* of t to v in Φ, is, a fortiori, true.
Moving now to the formalized mathematical discourse, we would like to define a syntactical notion of "substituting t to v in Φ" that behaves so. Let us look at some formalized example.

Example 1.3.1

$$\Phi := \exists y \;\; I(x, y)$$

where we can think of I as denoting the $<$ relation over natural integers. Let

$$t_1 := \mathrm{Succ}(x), \;\; t_2 := \mathrm{Succ}(y)$$

where we can think of Succ *as denoting the successor mapping over natural integers. If we replace the free occurrence of y by t_1 (resp. t_2) we obtain the new formula:*

$$\Phi[y \leftarrow t_1] = \exists y \;\; I(\mathrm{Succ}(x), y), \;\; \Phi[y \leftarrow t_2] = \exists y \;\; I(\mathrm{Succ}(y), y).$$

We are not surprised to see that there exists some integer y which is strictly larger than $x + 1$ (whatever this x is); but we shall not believe that there exists some integer y which is strictly larger than $y + 1$!

The phenomenon observed in the tranformation $\Phi \mapsto \Phi[y \leftarrow t_2]$ is called a "capture of the variable y": it consists in substituting a term t, where a variable v occurs, at a position p of Φ, in such a way that the occurrence of y created by the substitution is *bound* by some position of Φ. We define below the notion of substitution in such a way that this phenomenon cannot occur.

Definition 1.3.2 *Let $\Phi \in \mathcal{L}_1(\mathcal{S}, \mathcal{V})$, $t \in \mathcal{T}(\mathcal{S}, \mathcal{V})$ and $v \in \mathcal{V}$. The formula $\Phi[v \leftarrow t]$ is the formula obtained by replacing every free occurrence of letter v by the word t .*

Definition 1.3.3 *Let $\Phi \in \mathcal{L}_1(\mathcal{S},\mathcal{V})$, $t \in \mathcal{T}(\mathcal{S},\mathcal{V})$ and $v \in \mathcal{V}$. The formula $\Phi[v := t]$ is defined (up to α equivalence) as*

$$\Phi'[v \leftarrow t]$$

where Φ' is any formula such that $\Phi \equiv_\alpha \Phi'$ and Φ' has no occurrence of a quantification of any variable occurring in t.

Let us remark that Lemma 1.2.3, applied to the set V of all variables of t, ensures that such a formula Φ' exists; it should be clear also that, the α-equivalence class of the result $\Phi'[v \leftarrow t]$ depends on the α-equivalence class of Φ but not on the chosen representative Φ' (provided it fulfills the freeness assumption concerning all the variables occurring in t).

Example 1.3.4 *Let $\Phi := \exists y \;\; I(x,y)$ and $t := \mathrm{Succ}(y)$. The formula $\Phi' := \exists z \;\; I(x,z)$ is α-equivalent to Φ and has no occurrence of $\forall y$ or $\exists y$. Hence $\Phi[x := t] = \Phi'[x \leftarrow t] = \exists z \;\; I(\mathrm{Succ}(y), z)$.*

1.4 The system NK

The symbol NK denotes the formal system called *Natural Deduction* which was devised by Gentzen in 1935 (**??**). Letter N indicates that this sytem is conceived as formalizing the "natural" way of proving theorems in ordinary mathematical texts; letter K is the first letter of the german adjective "klassich" (Gentzen's article is written in german) , since the system formalizes the so-called *classical* logic, as opposed to *intuitionistic* logics.
It consists of a set of *judgments* and a set of *inference rules* .

Judgments A judgment of NK is a couple (Γ, A) where Γ is a finite subset of $\mathcal{L}_1(\mathcal{S},\mathcal{V})$ and A is an element of $\mathcal{L}_1(\mathcal{S},\mathcal{V})$. Such a couple is denoted by

$$\Gamma \vdash A$$

We call these judgments NK-*sequents*. Γ is the *set of antecedents* (or set of hypotheses) of the sequent while A is its *subsequent* (or its conclusion).

Inference rules A *rule* of the system is a couple of the form

$$\frac{S_1, \ldots, S_n}{S}$$

where $S_1, \ldots, S_n$ are NK-sequents. Such a rule will be used in *derivations* (or proofs) to infer (or deduce) from the sequents $S_1, \ldots, S_n$ the new sequent S. We call *upper-part* (resp. *lower-part*) of the rule the sequence $S_1, \ldots, S_n$ (resp. the sequent S). In fact we shall give a finite number of *rule schemes*. The full set of rules will be the set of all *instances* of these schemes. What we call an instance of the rule is a couple $\frac{S'_1,\ldots,S'_n}{S'}$ which is the image by replacing, in the rule, every occurrence of a greek letter by a finite multiset of formulas (up to α-conversion) and every occurrence of a latin letter, by a formula (up to α-conversion); of course, a given letter must be replaced by the same multiset (or formula) for all of its occurrences.

1-Axioms

$$\frac{}{\Gamma, A \vdash A}\,\mathtt{ax}$$

2-Structural rules

$$\frac{\Gamma \vdash A}{\Gamma,\ B \vdash A}\,\mathtt{wkn}$$

3-Connector rules

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\wedge^{\ell}_{\mathtt{elim}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\wedge^{r}_{\mathtt{elim}} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\wedge_{\mathtt{intro}}$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\vee_{\mathtt{elim}} \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\vee^{\ell}_{\mathtt{intro}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\vee^{r}_{\mathtt{intro}}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash A \to B}{\Gamma \vdash B}\to_{\mathtt{elim}} \qquad \frac{\Gamma,\ A \vdash B}{\Gamma \vdash A \to B}\to_{\mathtt{intro}}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\neg_{\mathtt{elim}} \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\neg_{\mathtt{intro}}$$

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\bot_{\mathtt{classic}}$$

4-Quantifier rules

$$\frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A[x{:=}t]}\forall_{\mathtt{elim}} \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\forall_{\mathtt{intro}}(\text{ if } x \notin \mathrm{FV}(\Gamma))$$

$$\frac{\Gamma \vdash \exists x A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\exists_{\mathtt{elim}}(\text{ if } x \notin \mathrm{FV}(\Gamma, B)) \qquad \frac{\Gamma \vdash A[x{:=}t]}{\Gamma \vdash \exists x A}\exists_{\mathtt{intro}}$$

Let us give some examples of rules (i.e. instances of the rule-schemes).

Example 1.4.1 `to be filled up`

Proofs

Definition 1.4.2 *A* derivation *(or* proof*) with the system* NK *is a finite sequence* $S_0, S_1, \ldots, S_n$ *of sequents* $S_i = \Gamma_i \vdash A_i$ *fulfilling: for every* $i \in [0, n]$
- either S_i *is an axiom*
- or there exists $j < i$ *such that* $\frac{S_j}{S_i}$ *is a rule*
- or there exists $j < k < i$ *such that* $\frac{S_j, S_k}{S_i}$ *is a rule or* $\frac{S_k, S_j}{S_i}$ *is a rule.*

Example 1.4.3
Here the signature $\mathcal{S}$ *posesses two unary predicate symbols* P, Q*.*
$0 - \quad P(x), P(x) \to \bot \vdash P(x) \quad (\mathtt{Ax})$
$1 - \quad P(x), P(x) \to \bot \vdash P(x) \to \bot \quad (\mathtt{Ax})$
$2 - \quad P(x), P(x) \to \bot \vdash \bot \quad (1, 2, \to \mathtt{elim})$
$3 - \quad P(x) \vdash (P(x) \to \bot) \to \bot \quad (2, \to \mathtt{intro})$
$4 - \quad \vdash P(x) \to ((P(x) \to \bot) \to \bot) \quad (3, \to \mathtt{intro})$
$5 - \quad \vdash \forall x \;\; P(x) \to ((P(x) \to \bot) \to \bot) \quad (4, \forall \mathtt{intro})$

Example 1.4.4
Here the signature $\mathcal{S}$ *posesses two propositional symbols* P, Q *i.e. predicate symbols of arity* 0*.*
$0 - \quad P \wedge Q, P \to (Q \to R) \vdash P \wedge Q \quad (\mathtt{Ax})$
$1 - \quad P \wedge Q, P \to (Q \to R) \vdash Q \quad (0, \wedge \mathtt{elim})$
$2 - \quad P \wedge Q, P \to (Q \to R) \vdash P \quad (1, \wedge \mathtt{elim})$
$3 - \quad P \wedge Q, P \to (Q \to R) \vdash P \to (Q \to R) \quad (\mathtt{Ax})$
$4 - \quad P \wedge Q, P \to (Q \to R) \vdash (Q \to R) \quad (2, 3, \to \mathtt{elim})$
$5 - \quad P \wedge Q, P \to (Q \to R) \vdash R \quad (1, 4, \to \mathtt{elim})$
$6 - \quad P \to (Q \to R) \vdash (P \wedge Q) \to R \quad (5, \to \mathtt{intro})$
$7 - \quad \vdash (P \to (Q \to R)) \to ((P \wedge Q) \to R) \quad (6, \to \mathtt{elim})$

One can notice that the relations between upper-part and lower-part of each application of rule induce a partial ordering of the sequents which can be visualized as a planar tree. The proofs of examples 1.4.3,1.4.4, for example, are depicted on figure 1.4. A real mathematical text is (physically) a linear sequence of assertions, thus accurately modelized by definition 1.4.2. Nevertheless, for reasoning about derivations, it is useful to take into account the tree-structure exhibited above. This is why we shall rather present the proofs as follows (we take examples 1.4.3-1.4.4 again):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(x), P(x)\to\bot \vdash P(x);}\,\mathtt{ax} \quad \dfrac{}{P(x), P(x)\to\bot \vdash P(x)\to\bot}\,\mathtt{ax}}{}\,{\to_{\mathtt{elim}}}}{P(x), P(x)\to\bot \vdash \bot}\,{\to_{\mathtt{intro}}}}{P(x), P(x)\to\bot \vdash P(x);}\,{\to_{\mathtt{intro}}}}{P(x), P(x)\to\bot \vdash P(x)\to\bot}\,{\to_{\mathtt{intro}}}}{\vdash \forall x\ \ P(x)\to((P(x)\to\bot)\to\bot)}\,{\forall_{\mathtt{intro}}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P\wedge Q, P\to(Q\to R)\vdash P\wedge Q;}\,\mathtt{ax}}{P\wedge Q, P\to(Q\to R)\vdash Q}\,{\wedge^{d}_{\mathtt{elim}}} \quad \dfrac{\dfrac{}{P\wedge Q, P\to(Q\to R)\vdash P\wedge Q;}\,\mathtt{ax}}{P\wedge Q, P\to(Q\to R)\vdash P}\,{\wedge^{g}_{\mathtt{elim}}}}{P\wedge Q, P\to(Q\to R)\vdash (Q\to R)}\,{\to_{\mathtt{elim}}} \quad \dfrac{}{P\wedge Q, P\to(Q\to R)\vdash P\to(Q\to R)}\,\mathtt{ax}}{P\wedge Q, P\to(Q\to R)\vdash R}\,{\to_{\mathtt{elim}}}}{P\to(Q\to R)\vdash (P\wedge Q)\to R}\,{\to_{\mathtt{intro}}}}{\vdash (P\to(Q\to R))\to((P\wedge Q)\to R)}\,{\to_{\mathtt{intro}}}$$

1.5 The system NJ

The symbol NJ denotes the formal system called *Intuitionistic Natural Deduction*. Its set of judgments is still the same as NK but its set of rules is slightly different:
- it does not posess the rule $\bot_{\mathtt{classic}}$
- instead, it posesses the weaker rule:

$$\dfrac{\Gamma \vdash\!\!\!\!-\ \bot}{\Gamma \vdash\!\!\!\!- A}\,\bot_{\mathtt{elim}}$$

that is sometimes called "intuitionistic absurd". The fact that NJ is *weaker* than NK is shown by the following derivation in NK:

$$\dfrac{\dfrac{\Gamma\vdash\bot}{\Gamma, \neg A\vdash\bot}\,\mathtt{wkn}}{\Gamma\vdash A}\,\bot_{\mathtt{classic}}$$

The fact that it is *strictly* weaker will be shown later on. Typical examples of judgments which are derivable in NK but are not derivable in NJ are:

$$\vdash A \vee \neg A$$

(the so-called "excluded third" principle)

$$\neg\neg A \vdash A$$

(the so-called "double negation " rule)

$$\neg\forall x\ P(x) \vdash \exists x\ \neg P(x)$$

(a duality principle for quantifiers).
The non-existence of intuitionnistic proofs for these judgments can be shown, either by syntactic methods (these will be developed in chapter 3) or semantical methods (these will be developed in chapter 4).

`what is NJ interesting for ?`

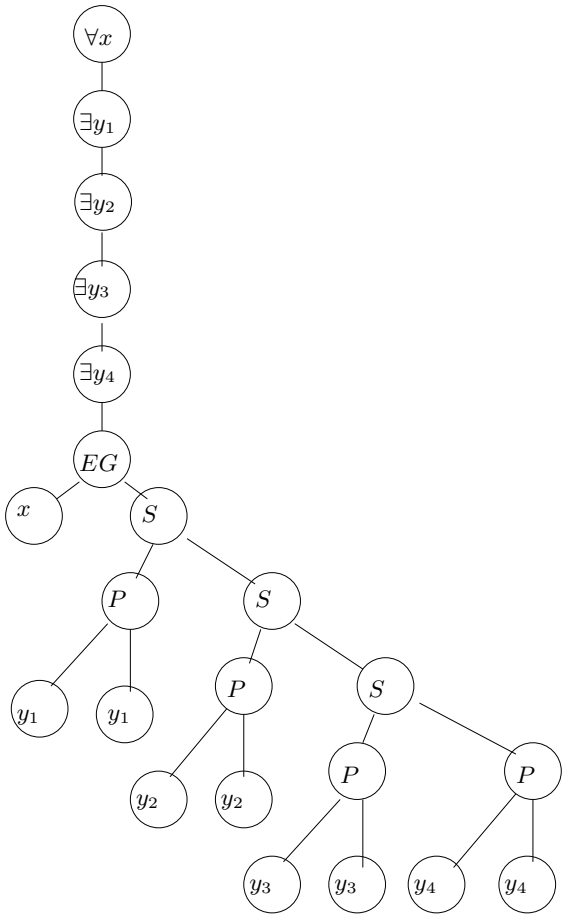

Figure 1.1: The planar tree $P(\Phi)$.

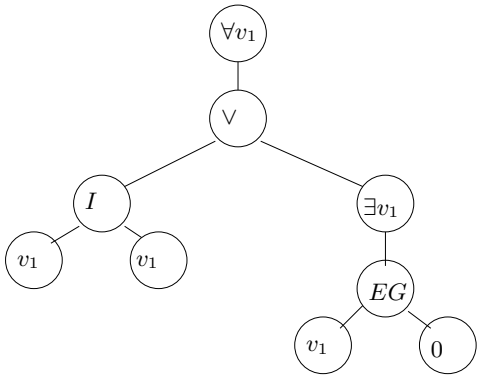

Figure 1.2: The planar tree $P(\Phi_1)$.

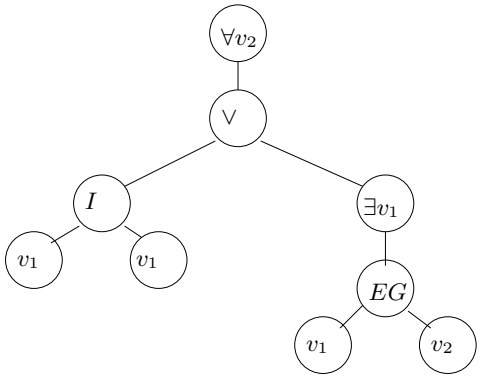

Figure 1.3: The planar tree $P(\Phi_2)$.

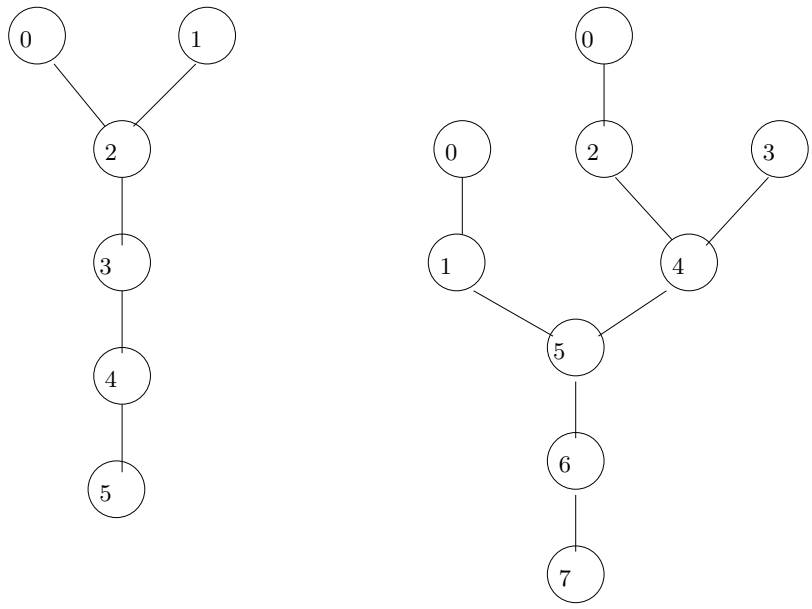

Figure 1.4: The planar trees for examples 1.4.3,1.4.4

Chapter 2

Sequent calculus

We describe in this chapter another formal system, called *sequent calculus* and denoted by LK. It was devised by Gentzen ([Gen35a]) in order to prove some properties of the system NK. We prove here the equivalence between both systems (as did Gentzen in [Gen35b]).

We postpone to chapter 3 the detailed study of the proofs in systems LJ, LK as well as their consequences

2.1 The system LK

Judgments A judgment of LK is a couple (Γ, Δ) where Γ, Δ are finite multisets of elements of $\mathcal{L}_1(\mathcal{S}, \mathcal{V})/\equiv_\alpha$; such a couple is denoted by

$$\Gamma \vdash \Delta$$

We recall a multiset m of elements of a set Ω is a (total) map:

$$m : \Omega \to \mathbb{N}.$$

The set $\mathcal{P}(\Omega)$ can be identified with those multisets m such that for every $\omega \in \Omega, m(\omega) \in \{0, 1\}$. The addition of multisets is defined by:

$$\forall \omega \in \Omega, \quad (m + m')(\omega) := m(\omega) + m'(\omega).$$

Less formally: a sequent is a word of the form

$$B_1, \ldots, B_m \vdash A_1, \ldots, A_n$$

where A_i, B_j are formula that must be taken "up to α-equivalence" and the precise ordering of the B_j's (resp. the A_i's) is irrelevant; moreover, it is possible that some formulas with different indices, are equal (or α-equivalent). We shall see later that the formal system does even have some rules (the *structural* rules) which may just modify the numbers of copies of a given formula. Intuitively, such a sequent has the same meaning as the formula $(B_1 \wedge \ldots \wedge B_m) \to (A_1 \vee \ldots \vee A_n)$. When $m = 0$ this means $A_1 \vee \ldots \vee A_n$ and when $n = 0$ it means $(B_1 \wedge \ldots \wedge B_m) \to \bot$. We call these judgments LK-*sequents*. Γ is the *set of antecedents* (or set of hypotheses) of the sequent while Δ is the *set of subsequents* (or its set of conclusions).

Inference rules A *rule* of the system is a couple of the form

$$\frac{S_1, \ldots, S_n}{S}$$

where $S_1, \ldots, S_n$ are LK-sequents. Such a rule will be used in *derivations* (or proofs) to infer (or deduce) from the sequents $S_1, \ldots, S_n$ the new sequent S. We call *upper-part* (resp. *lower-part*) of the rule the set $S_1, \ldots, S_n, S$ (resp. the sequent S). In fact we shall give a finite number of *rule schemes*. The full set of rules will be the set of all *instances* of these schemes.

1-Axioms

$$\frac{}{\bot \vdash}\bot_\ell \qquad \frac{}{A \vdash A}\mathtt{ax}$$

2-Structural rules

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\mathtt{wkn}_\ell \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\mathtt{wkn}_r$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\mathtt{contr}_\ell \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\mathtt{contr}_r$$

3-Connective rules

$$\frac{\Gamma,A,B \vdash \Delta}{\Gamma,A\wedge B \vdash \Delta}\wedge_\ell \qquad \frac{\Gamma \vdash A,\Delta \quad \Gamma \vdash B,\Delta}{\Gamma \vdash A\wedge B,\Delta}\wedge_r$$

$$\frac{\Gamma,A \vdash \Delta \quad \Gamma,B \vdash \Delta}{\Gamma,A\vee B \vdash \Delta}\vee_\ell \qquad \frac{\Gamma \vdash A,B,\Delta}{\Gamma \vdash A\vee B,\Delta}\vee_r$$

$$\frac{\Gamma \vdash A,\Delta \quad \Gamma,B \vdash \Delta}{\Gamma,A\to B \vdash \Delta}\to_\ell \qquad \frac{\Gamma,\ A \vdash B,\Delta}{\Gamma \vdash A\to B,\Delta}\to_r$$

$$\frac{\Gamma \vdash A,\Delta}{\Gamma,\neg A \vdash \Delta}\neg_\ell \qquad \frac{\Gamma,A \vdash \Delta}{\Gamma \vdash \neg A,\Delta}\neg_r$$

4-Quantifier rules

$$\frac{\Gamma,A[x{:=}t] \vdash \Delta}{\Gamma,\forall x\ \ A \vdash \Delta}\forall_\ell \qquad \frac{\Gamma \vdash A,\Delta}{\Gamma \vdash \forall x\ \ A,\Delta}\forall_r(\text{ if } x \notin \mathrm{FV}(\Gamma,\Delta))$$

$$\frac{\Gamma,A \vdash \Delta}{\Gamma,\exists x\ \ A \vdash \Delta}\exists_\ell(\text{ if } x \notin \mathrm{FV}(\Gamma,\Delta)) \qquad \frac{\Gamma \vdash A[x{:=}t],\Delta}{\Gamma \vdash \exists x\ \ A,\Delta}\exists_r$$

5-Cut rule

$$\frac{\Gamma \vdash \Delta,A \quad A,\Gamma' \vdash \Delta'}{\Gamma,\Gamma' \vdash \Delta,\Delta'}\mathtt{cut}$$

2.2 The system LJ

Of course, as the name suggests, LJ is thought of, as being the intuitionistic counterpart of LK. It is thus, as expected, a *restriction* of system LK. Nevertheless, the restriction is not obtained, as for NJ, just by replacing one rule by another weaker rule: the set of judgments of LJ is a strict subset of the set of judgments of LK, while the rules are essentially the restriction of the rules of LK to the upper-(and lower) sequences of judgments which are still authorised.

Judgments A judgment of LJ is a couple (Γ,Δ) where Γ,Δ are finite multisets of elements of $\mathcal{L}_1(\mathcal{S},\mathcal{V})/\equiv_\alpha$ and Δ has at most one element (i.e.

either it is empty or it consists of a single formula (like in judgments of NK, NJ). Less formally: a sequent is a word of the form

$$B_1, \ldots, B_m \vdash A$$

where B_j and A are formula that must be taken "up to α-equivalence" and the ordering of formulas B_i is irrelevant; it is possible that some formulas with different indices, are equal (or α-equivalent); it is also possible that the sequent has the form

$$B_1, \ldots, B_m \vdash$$

in which case it would mean the same as the sequent $B_1, \ldots, B_m \vdash \bot$. We call these judgments *intuitionistic sequents*.

Inference rules The *rules* of the system have the form

$$\frac{S_1, \ldots, S_n}{S}$$

where $S_1, \ldots, S_n$ are intuitionistic sequents. We give below a finite number of *rule schemes* from which one can deduce, by adequate instantiation, the full set of rules.

1-Axioms

$$\frac{}{\bot \vdash}\bot_g \qquad \frac{}{A \vdash A}\mathtt{ax}$$

2-Structural rules

$$\frac{\Gamma \vdash [C]}{\Gamma, A \vdash [C]}\mathtt{wkn}_g \qquad \frac{\Gamma \vdash}{\Gamma \vdash A}\mathtt{wkn}_d$$

$$\frac{\Gamma, A, A \vdash [C]}{\Gamma, A \vdash [C]}\mathtt{contr}_g$$

3-Connective rules

$$\frac{\Gamma,A,B \vdash [C]}{\Gamma,A\wedge B \vdash [C]}\wedge_\ell \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A\wedge B}\wedge_r$$

$$\frac{\Gamma,A \vdash [C] \quad \Gamma,B \vdash [C]}{\Gamma,A\vee B \vdash [C]}\vee_\ell \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A\vee B}\vee_r^1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A\vee B}\vee_r^2$$

$$\frac{\Gamma \vdash A, \quad \Gamma,B \vdash [C]}{\Gamma,A\to B \vdash [C]}\to_\ell \qquad \frac{\Gamma,\ A \vdash B}{\Gamma \vdash A\to B}\to_r$$

$$\frac{\Gamma \vdash A}{\Gamma,\neg A \vdash}\neg_\ell \qquad \frac{\Gamma,A \vdash}{\Gamma \vdash \neg A}\neg_r$$

4-Quantifier rules

$$\frac{\Gamma,A[x{:=}t] \vdash [C]}{\Gamma,\forall x\ \ A \vdash [C]}\forall_\ell \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ \ A}\forall_r(\text{ if } x \notin \mathrm{FV}(\Gamma))$$

$$\frac{\Gamma,A \vdash [C]}{\Gamma,\exists x\ \ A \vdash [C]}\exists_\ell(\text{ if } x \notin \mathrm{FV}(\Gamma,[C])) \qquad \frac{\Gamma \vdash A[x{:=}t]}{\Gamma \vdash \exists x\ \ A}\exists_r$$

5-Cut rule

$$\frac{\Gamma \vdash A \quad A,\Gamma' \vdash [C]}{\Gamma,\Gamma' \vdash [C]}\mathtt{cut}$$

2.3 Equivalence with NK, NJ

We show in this section that, essentially, the system LK (resp. LJ) proves the same formulas as the system NK (resp. NJ): for every formula φ, the sequent $\vdash \varphi$ is derivable in LK (resp. LJ) iff it is derivable in NK (resp. NJ).

However, since the four systems have different sets of judgments (in $L*$ the formulas have multiplicites while in $N*$ they have not, in LJ the right-parts of the sequents can be empty while in NJ they cannot), some translations are necessary to formulate a general equivalence which will be amenable to a proof by recurrence over the size of derivations.

Theorem 2.3.1 *Let Γ be some set of formulas and A a formula. If $\Gamma \vdash A$ is derivable in* NK*, then $\Gamma \vdash A$ is derivable in* LK*,*

(The second occurrence of $\Gamma \vdash A$ in the above statement is, in fact, the pair of multisets $(\Gamma, \{A\})$ obtained by seeing sets as particular multisets where every multiplicity belongs to $\{0, 1\}$.)

Let us call *derived rule* of a formal system FS, with upper-part $S_1, \ldots, S_n$ and lower-part S, a derivation of the system FS where the leaves are labelled by the S_i (or are axioms) and the root is labelled by S. The notation

$$\dfrac{S_1, \ldots, S_n}{\dfrac{}{S}\,FS}$$

means that tere exists a derived rule in the system SF with upper-part $S_1, \ldots, S_n$ and lower-part S.
Proof: It suffices to prove that, for every scheme of rule $\frac{S_1,\ldots,S_n}{S}$ of NK, $\frac{S_1,\ldots,S_n}{\frac{}{S}\,\mathrm{LK}}$. In some exceptional cases, we only prove that every instance of the rule has a corresponding derived rule. We say that the initial scheme of rule (resp. rule) $\frac{S_1,\ldots,S_n}{S}$ of NK can be *simulated* within the system LK.

Rules $\mathtt{ax}, \mathtt{wkn}, \wedge_{\mathtt{intro}}, \rightarrow_{\mathtt{intro}}$:
These rules are (respectively) simulated by the rules (or sequences of rules) $(\mathtt{ax} \cdot \mathtt{wkn}_\ell^*)$, $\mathtt{wkn}_\ell$, $\wedge_r$, $\rightarrow_r$.

Rules $\forall_{\mathtt{intro}}, \exists_{\mathtt{intro}}$:
These rules are (respectively) simulated by the rules $\forall_r, \exists_r$.

Rule $\vee^{\ell}_{\mathtt{intro}}$:
Derived rule:

$$\dfrac{\dfrac{\Gamma \vdash A}{\Gamma \vdash A, B}\,\mathtt{wkn}_r}{\Gamma \vdash A \vee B}\,\vee_r$$

Rule $\vee^{r}_{\mathtt{intro}}$:There is an analogous derived rule in NK.

Rule $\neg_{\mathtt{intro}}$:
Derived rule:

$$\dfrac{\dfrac{\Gamma, A \vdash \bot \quad \dfrac{}{\bot \vdash}\,\bot_l}{\Gamma, A \vdash}\,\mathtt{cut}}{\Gamma \vdash \neg A}\,\neg_r$$

Rule $\wedge^{\ell}_{\texttt{elim}}$:
Derived rule:

$$\dfrac{\Gamma \vdash A \wedge B \qquad \dfrac{\dfrac{\dfrac{}{A \vdash A}\,\texttt{ax}}{A, B \vdash A}\,\texttt{wkn}_l}{A \wedge B \vdash A}\,\wedge_l}{\Gamma \vdash A}\,\texttt{cut}$$

Rule $\wedge^{r}_{\texttt{elim}}$:analogous derived rule in NK.

Rule $\vee_{\texttt{elim}}$:
Derived rule:

$$\dfrac{\dfrac{\Gamma \vdash A \vee B \qquad \dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\,\vee_l}{\Gamma, \Gamma \vdash C}\,\texttt{cut}}{\Gamma \vdash C}\,\texttt{contr}_l$$

Rule $\rightarrow_{\texttt{elim}}$:
Derived rule:

$$\dfrac{\dfrac{\Gamma \vdash A \to B \qquad \dfrac{\dfrac{\Gamma \vdash A}{\Gamma \vdash A, B}\,\texttt{wkn}_r \quad \dfrac{}{\Gamma, B \vdash B}\,\texttt{ax}'}{\Gamma, A \to B \vdash B}\,\to_l}{\Gamma, \Gamma \vdash B}\,\texttt{cut}}{\Gamma \vdash B}\,\texttt{contr}_l$$

Rule $\neg_{\texttt{elim}}$:
Derived rule:

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash \neg A \qquad \dfrac{\Gamma \vdash A}{\Gamma, \neg A \vdash}\,\neg_l}{\Gamma, \Gamma \vdash}\,\texttt{cut}}{\Gamma \vdash}\,\texttt{contr}_l}{\Gamma \vdash \bot}\,\texttt{wkn}_r$$

Rule $\forall_{\texttt{elim}}$:

Derived rule:

$$\dfrac{\Gamma \vdash \forall x A \qquad \dfrac{\dfrac{}{A[x := t] \vdash A[x := t]}\,\mathtt{ax}}{\forall x A \vdash A[x := t]}\,\forall_l}{\Gamma \vdash A[x := t]}\,\mathtt{cut}$$

Rule $\exists_{\mathtt{elim}}$:
Derived rule:

$$\dfrac{\Gamma \vdash \exists x A \qquad \dfrac{\Gamma, A \vdash C}{\Gamma, \exists x A \vdash C}\,\exists_l}{\dfrac{\Gamma, \Gamma \vdash C}{\Gamma \vdash C}\,\mathtt{contr}_l}\,\mathtt{cut}$$

Rule $\bot_{\mathtt{classic}}$:
Derived rule:

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathtt{ax}}{\vdash \neg A, A}\,\neg_r \qquad \dfrac{\Gamma, \neg A \vdash \bot \qquad \dfrac{}{\bot \vdash}\,\bot_l}{\Gamma, \neg A \vdash}\,\mathtt{cut}}{\Gamma \vdash A}\,\mathtt{cut}$$

□

Theorem 2.3.2 *Let* Γ *be a set of formulas and* A *a formula. If* $\Gamma \vdash\!\!\!- A$ *is derivable in* NJ*, then* $\Gamma \vdash\!\!\!- A$ *is derivable in* LJ*.*

Proof: We follow the same proof strategy as for the previous theorem: we list all the rule-schemes of NJ and exhibit a simulation of it within LJ.

Rules $\mathtt{ax}, \mathtt{wkn}, \wedge_{\mathtt{intro}}, \rightarrow_{\mathtt{intro}} \forall_{\mathtt{intro}}, \exists_{\mathtt{intro}}$:
Same arguments as in the case of LK.

Rule $\vee^{\ell}_{\mathtt{intro}}$:
Derived rule:

$$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,\vee^1_r$$

Rule $\vee^r_{\mathtt{intro}}$:
Derived rule:

$$\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\vee^2_r$$

Rules $\neg_{\mathtt{intro}}, \wedge^{\ell}_{\mathtt{elim}}, \wedge^{r}_{\mathtt{elim}}, \vee_{\mathtt{elim}}$:
Same arguments as in the case of LK.

Rule $\rightarrow_{\mathtt{elim}}$:
Derived rule:

$$\dfrac{\Gamma \vdash A \to B \qquad \dfrac{\Gamma \vdash A \quad \dfrac{}{\Gamma, B \vdash B}\,\mathtt{ax}'}{\Gamma, A \to B \vdash B}\,{\to}_l}{\dfrac{\Gamma, \Gamma \vdash B}{\Gamma \vdash B}\,\mathtt{contr}_l}\,\mathtt{cut}$$

Rules $\neg_{\mathtt{elim}}, \forall_{\mathtt{elim}}, \exists_{\mathtt{elim}}$:
Same arguments as in the case of LK.

Rule $\perp_{\mathtt{i}}$:
Derived rule:

$$\dfrac{\dfrac{\Gamma \vdash \bot \qquad \dfrac{}{\bot \vdash}\,\bot_l}{\Gamma \vdash}\,\mathtt{cut}}{\Gamma \vdash A}\,\mathtt{wkn}_r$$

□
Let us now show that, conversely, "every formula derivable in LJ is derivable in NJ". In order to formulate properly this statement (though the judgments of LJ, NJ are different) we introduce a notation:
for every multiset M over a set Ω, we denote by $\mathcal{E}(M) \subseteq \Omega$ the set which is the support of M

$$\mathcal{E}(M) := \{\omega \in \Omega \mid M(e) \neq 0\}.$$

We define a map δ that translates every judgment of LJ into a judgment of NJ by:if Γ is a multiset of formulas and A a formula

$$\delta(\Gamma \vdash A) := \mathcal{E}(\Gamma) \vdash A;\ \ \delta(\Gamma \vdash) := \mathcal{E}(\Gamma) \vdash \bot.$$

Theorem 2.3.3 *Let* Γ *be a multiset of formulas and* A *a formula. If* $\Gamma \vdash A$ *(resp.* $\Gamma \vdash$ *) is derivable in* LJ *then* $\mathcal{E}(\Gamma) \vdash A$ *(resp.* $\mathcal{E}(\Gamma) \vdash \bot$*) is derivable in* NJ*.*

Proof: We show that, if $\frac{S_1,\ldots,S_n}{S}$ is a rule of LJ, then

$$\frac{\delta(S_1), \ldots, \delta(S_n)}{\delta(S)}\ \mathsf{NJ}$$

i.e. that its translation into judgments of NJ can be simulated by a finite derivation within NJ.

Rules $\mathtt{ax}, \mathtt{wkn}_l, \vee^1_r, \vee^2_r, \wedge_r, \to_r, \neg_r$:
these (schemes of) rules are also (schemes of) rules of NJ.

Rule `cut`:
Derived rule:

$$\dfrac{\dfrac{\mathcal{E}(\Gamma) \vdash A}{\mathcal{E}(\Gamma, \Gamma') \vdash A}\,\mathtt{wkn} \quad \dfrac{\dfrac{\Gamma', A \vdash C}{\Gamma' \vdash A \to C}\,{\to_{\mathtt{intro}}}}{\mathcal{E}(\Gamma, \Gamma') \vdash A \to C}\,\mathtt{wkn}}{\mathcal{E}(\Gamma, \Gamma') \vdash C}\,{\to_{\mathtt{elim}}}$$

Rule $\mathtt{contr}_l$:
Since $\mathcal{E}(\Gamma, A, A) = \mathcal{E}(\Gamma, A)$, the image by the translation δ of this scheme of rule is a trivial derived rule consisting of just one judgment (which is both its upper-part and its lower-part).

Rule $\mathtt{wkn}_l$:
this scheme of rule is also a scheme of rule of NJ.

Rule $\mathtt{wkn}_r$:
the map δ sends this scheme on the scheme of rule $\bot_{\mathtt{elim}}$ of NJ.

Rule $\to_\ell$:
Derived rule:

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash A}{\Gamma, A \to B \vdash A}\,\mathtt{wkn} \quad \dfrac{}{\Gamma, A \to B \vdash A \to B}\,\mathtt{ax}}{\Gamma, A \to B \vdash B}\,{\to_{\mathtt{elim}}} \quad \dfrac{\dfrac{\Gamma, B \vdash C}{\Gamma \vdash B \to C}\,{\to_{\mathtt{intro}}}}{\Gamma, A \to B \vdash B \to C}\,\mathtt{wkn}}{\Gamma, A \to B \vdash C}\,{\to_{\mathtt{elim}}}$$

Rule $\neg_\ell$:
Derived rule:

$$\dfrac{\dfrac{}{\Gamma, \neg A \vdash \neg A}\,\mathtt{ax}' \quad \dfrac{\Gamma \vdash A}{\Gamma, \neg A \vdash A}\,\mathtt{wkn}}{\Gamma, \neg A \vdash \bot}\,{\neg_{\mathtt{elim}}}$$

Rule $\wedge_\ell$:
Derived rule:

$$\dfrac{\dfrac{\dfrac{}{\Gamma, A \wedge B \vdash A \wedge B}\,\mathtt{ax}}{\Gamma, A \wedge B \vdash B}\,{\wedge^r_{\mathtt{elim}}} \quad \dfrac{\dfrac{}{\Gamma, A \wedge B \vdash A \wedge B}\,\mathtt{ax}}{\Gamma, A \wedge B \vdash A}\,{\wedge^\ell_{\mathtt{elim}}} \quad \dfrac{\dfrac{\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \vdash B \to C}\,{\to_{\mathtt{intro}}}}{\Gamma \vdash A \to (B \to C)}\,{\to_{\mathtt{intro}}}}{\Gamma, A \wedge B \vdash A \to (B \to C)}\,\mathtt{wkn}}{\Gamma, A \wedge B \vdash B \to C}\,{\to_{\mathtt{elim}}}}{\Gamma, A \wedge B \vdash C}\,{\to_{\mathtt{elim}}}$$

Rule $\vee_\ell$:
Derived rule:

$$\dfrac{\dfrac{}{\Gamma, A \vee B \vdash A \vee B}\,\mathtt{ax} \quad \dfrac{\Gamma, A \vdash C}{\Gamma, A \vee B, A \vdash C}\,\mathtt{wkn} \quad \dfrac{\Gamma, B \vdash C}{\Gamma, A \vee B, B \vdash C}\,\mathtt{wkn}}{\Gamma, A \vee B \vdash C}\,{\vee_{\mathtt{elim}}}$$

Rule $\forall_\ell$:
Derived rule:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, A[x := t] \vdash C}{\Gamma \vdash A[x := t] \to C}\,{\to_{\mathtt{intro}}}}{\Gamma, \forall x A \vdash A[x := t] \to C}\,\mathtt{wkn} \quad \dfrac{\dfrac{}{\Gamma, \forall x A \vdash \forall x A}\,\mathtt{ax}}{\Gamma, \forall x A \vdash A[x := t]}\,{\forall_{\mathtt{elim}}}}{\Gamma, \forall x A \vdash C}\,{\to_{\mathtt{elim}}}$$

Rule $\exists_\ell$:
Derived rule:

$$\dfrac{\dfrac{\dfrac{}{\exists x A \vdash \exists x A}\,axm}{\Gamma, \exists x A \vdash \exists x A}\,\mathtt{wkn} \qquad \Gamma, A \vdash C}{\Gamma, \exists x A \vdash C}\,\exists_{\mathtt{elim}}$$

□

We aim now at proving the converse of Theorem 2.3.1. We shall obtain this result by going through an *auxiliary* logical system, that we call LA . We first prove that LK can be simulated by LA and, later on, that LA can be simulated by NK.

Let us define LA as the system where the judgments are exactly the judgments of LJ and the rules are the rules of LJ augmented by the rule $\bot_{\mathtt{classic}}$. We summarize this definition by writing

$$\mathsf{LA} := \mathrm{LJ} + \bot_{\mathtt{classic}}.$$

For every multiset of formulas $\Delta = A_1, \ldots, A_n$ we define the notation $\neg\Delta$ by $\neg\Delta := \neg A_1, \ldots, \neg A_n$.

Lemma 2.3.4 *Let Γ, Δ be some multi-sets of formulas. If $\Gamma \vdash\!\!\!- \Delta$ is derivable in* LK *then $\Gamma, \neg\Delta \vdash\!\!\!- \bot$ is derivable in* LA.

Proof: We define a translation τ from the set of judgments of LK into the set of judgments of LA by:

$$\tau(\Gamma \vdash\!\!\!- \Delta) := \Gamma, \neg\Delta \vdash\!\!\!- \bot$$

For every scheme of rule of LK, $\frac{S_1,\ldots,S_n}{S}$, we prove that

$$\dfrac{\tau(S_1), \ldots, \tau(S_n)}{\tau(S)}\,\mathsf{LA}.$$

Left introduction rules:
One can check that $\tau(\wedge_\ell), \tau(\vee_\ell), \tau(\to_\ell), \tau(\forall_\ell), \tau(\exists_\ell)$ are instances of the corresponding rules of LJ.

Rules $\wedge_r, \to_r, \neg_r, \forall_r, \exists_r$:
For every of these rules we can exhibit a derivation in LA of its image by τ, by using the following principle:
- every rule acts on at most one formula on the right-hand side of each sequent
- using $\bot_{\texttt{classic}}$ we can transform the image by τ of a sequent into a sequent where the active formula has moved from left to right
- we can then apply the rule of LJ on these tranformed sequents
- using $\neg_\ell$ we can move back the new formula (with the new connector) to the left-hand side of the sequent
- finally, by a weakening rule, we can add the $\bot$ symbol on the right.
Let us demonstrate this method on the case of rule $\wedge_r$:
the initial rule is

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}$$

its image by τ is

$$\frac{\Gamma, \neg\Delta, \neg A \vdash \bot \quad \Gamma, \neg\Delta, \neg B \vdash \bot}{\Gamma, \neg\Delta, \neg(A \wedge B) \vdash \bot}$$

which is simulated by:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, \neg\Delta, \neg A \vdash \bot}{\Gamma, \neg\Delta \vdash A}\bot_{\texttt{classic}} \quad \dfrac{\Gamma, \neg\Delta, \neg B \vdash \bot}{\Gamma, \neg\Delta \vdash B}\bot_{\texttt{classic}}}{\Gamma, \neg\Delta \vdash A \wedge B}\wedge_r}{\Gamma, \neg\Delta, \neg(A \wedge B) \vdash}\neg_l}{\Gamma, \neg\Delta, \neg(A \wedge B) \vdash \bot}\texttt{wkn}_r$$

The other left introduction rules can be treated analogously.

Rules $\texttt{wkn}_r, \texttt{contr}_r$:
these rules are simulated (on the images by τ) respectively by rules $\texttt{wkn}_\ell$ and $\texttt{contr}_\ell$.

Rule `cut`:
The image by τ of the cut rule is simulated by

$$\dfrac{\dfrac{\dfrac{\Gamma, \neg\Delta, \neg A \vdash \bot}{\Gamma, \neg\Delta \vdash A}\,\bot_{\mathtt{classic}} \quad \dfrac{\Gamma', \neg\Delta', A \vdash \bot}{\Gamma, \Gamma', \neg\Delta, \neg\Delta', A \vdash \bot}\,\mathtt{wkn}_l}{\Gamma, \Gamma', \neg\Delta, \neg\Delta' \vdash A}\,\mathtt{wkn}_l}{\dfrac{2\Gamma, 2\Gamma', 2\neg\Delta, 2\neg\Delta' \vdash \bot}{\Gamma, \Gamma', \neg\Delta, \neg\Delta' \vdash \bot}\,\mathtt{contr}_l^*}\,\mathtt{cut}$$

Rule $\vee_r$:
The image by τ of $\vee_r$ is

$$\dfrac{\Gamma, \neg\Delta, \neg A, \neg B \vdash\!\!\!\vdash \bot}{\Gamma, \neg\Delta, \neg(A \vee B) \vdash\!\!\!\vdash \bot}$$

Let us construct a simulation for this rule. We denote $\Gamma, \neg\Delta$ by U in this simulation.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{U, \neg A, \neg B \vdash \bot}{U, \neg A \vdash B}\,\bot_{\mathtt{classic}}}{U, \neg A \vdash A \vee B}\,\vee_r^2}{U, \neg A, \neg(A \vee B) \vdash}\,\neg_l}{U, \neg A, \neg(A \vee B) \vdash \bot}\,\mathtt{wkn}_r}{U, \neg(A \vee B) \vdash A}\,\bot_{\mathtt{classic}}}{U, \neg(A \vee B) \vdash A \vee B}\,\vee_r^1}{U, 2\neg(A \vee B) \vdash}\,\neg_l}{U, \neg(A \vee B) \vdash}\,\mathtt{contr}_l}{U, \neg(A \vee B) \vdash \bot}\,\mathtt{wkn}_r$$

□
We are ready for the converse of Theorem 2.3.1.

Theorem 2.3.5 *Let Γ, Δ be multisets of formulas. If $\Gamma \vdash\!\!\!\vdash \Delta$ is derivable in* LK*, then $\mathcal{E}(\Gamma, \neg\Delta) \vdash\!\!\!\vdash \bot$ is derivable in* NK*.*

Proof: Suppose that $\Gamma \vdash\!\!\!\vdash \Delta$ is derivable in LK. By Lemma 2.3.4,

$$\Gamma, \neg\Delta \vdash\!\!\!\vdash \bot \text{ is derivable in } \mathsf{LA} = \mathrm{LJ} + \bot_{\mathtt{classic}}. \tag{2.1}$$

Let us use the translation map δ defined in the proof of Theorem 2.3.3. The proof of Theorem 2.3.3 consisted in proving that every rule of LJ has an

image by δ which is derivable in NJ. Moreover, the image by δ of the rule $\bot_{\texttt{classic}}$ is the same rule, which is a rule of NK. Hence, every rule of LA has an image by δ which is simulated in the system NK. We can thus deduce from (2.1) that

$$\delta(\Gamma, \neg\Delta \vdash \bot) \text{ is derivable in NK}$$

i.e. that

$$\mathcal{E}(\Gamma, \neg\Delta) \vdash \bot$$

is derivable in NK. □

Chapter 3

Normalizing proofs

We have remarked that the system LK (or LJ) consists of structural rules, introduction rules and a a special rule called *cut* rule. This rule is rather natural since it can be considered as a generalization of the transitivity of implication. Moreover, it was an essential ingredient for simulating the rules of NK within LK.

Neverheless, from the point of view of uniformity of the full system, it is the only rule that *eliminates* some part of the upper-sequents. This results in a greater complexity of the problem of searching a proof for a given sequent.

We show here that, in fact, this rule can be safely *eliminated* from the list of rules, without changing the set of derivable sequents. In section 3.3 we exploit this restricted form of derivations for proving several interesting properties of LK, LJ, in particular some connections with computability.

3.1 Cut elimination

Definition 3.1.1 *A derivation (in* LK *or* LJ*) is called* normal *if it does not use the cut rule.*

Theorem 3.1.2 *Let Γ, Δ be multi-sets of formulas. If the sequent $\Gamma \vdash \Delta$ is derivable in* LK *(resp.* LJ*), then it admits some* normal *derivation in* LK *(resp.* LJ*).*

We prove this statement by induction over the set of proofs, endowed with a suitable ordering. It turns out that this induction is easier to handle with a more powerful rule than the cut rule, which we introduce now.

Definition 3.1.3 *We call mix-rule the following scheme:*

$$\frac{\Gamma \vdash \Delta \quad \Gamma' \vdash \Delta'}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}$$

where A is a formula, $\Gamma' = \Gamma'_A + nA$ (for some $n \in \mathbb{N}$), and $\Delta = \Delta_A + mA$ (for some $m \in \mathbb{N}$).

We denote by LKM the formal system obtained from LK by removing the cut rule and adding the mix-rule. Let us show that LK and LKM are equivalent (i.e. derive the same sequents).

Lemma 3.1.4 *Every cut is also a mix.*

This is straightforward: a cut is a mix where the integers n, m of definition 3.1.3 are taken to be equal to 1.

Lemma 3.1.5 *Every mix can be simulated by a finite number of structural rules and at most one cut.*

Proof: Let us consider a rule

$$\frac{\Gamma \vdash \Delta \quad \Gamma' \vdash \Delta'}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}$$

where A is a formula, $\Gamma' = \Gamma'_A + nA, \Delta = \Delta_A + mA$ and $n, m \in \mathbb{N}$.
Case 1:$n = 0$ i.e. $\Gamma'_A = \Gamma'$

$$\dfrac{\dfrac{\Gamma' \vdash \Delta'}{\Gamma, \Gamma'_A \vdash \Delta'}\,\mathtt{wkn}^*_l}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\,\mathtt{wkn}^*_r$$

Case 2:$m = 0$ i.e. $\Delta_A = \Delta$

$$\dfrac{\dfrac{\Gamma \vdash \Delta}{\Gamma, \Gamma'_A \vdash \Delta}\,\mathtt{wkn}^*_l}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\,\mathtt{wkn}^*_r$$

Case 3:$n \geq 1$ and $m \geq 1$.

$$\dfrac{\dfrac{\Gamma \vdash \Delta_A + mA}{\Gamma \vdash \Delta_A, A}\,\mathtt{contr}^*_r \quad \dfrac{nA + \Gamma'_A \vdash \Delta'}{A, \Gamma'_A \vdash \Delta'}\,\mathtt{contr}^*_l}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\,cut$$

□

It is thus clear that the systems LK and LKM are equivalent. We are left now with proving that every derivation in LKM can be transformed into a normal derivation. Let us state the key-lemma of this section.

Lemma 3.1.6 *Let π be a derivation in* LKM *whihs uses exactly one mix rule and such that this mix is its last step. Then, there exists some normal derivation π' with the same conclusion as π.*

We postpone the proof of lemma 3.1.6 and show immediately why it is sufficient for proving Theorem 3.1.2.

Proof of Theorem 3.1.2:

We proceed by induction over the number of mixes (i.e. applications of the mix rule) of derivation π.

Base: π has no mix.

Then π is normal.

Induction step: π has $n + 1$ mixes.

Let us choose some node where the mix rule is applied and such that the two subderivations π_1, π_2 that are "above" this mix are normal. The derivation

π has the following form:

$$\dfrac{\dfrac{\pi_1 \quad \pi_2}{\vdots \ \Gamma \vdash \Delta \ \vdots}\,\mathtt{mix}}{\pi_3}\,\mathtt{R}$$

(where, possibly, the rule R and the subderivation π_3 do not exist). By Lemma 3.1.6 the subderivation ending in $\Gamma \vdash \Delta$ can be transformed into a normal derivation π_4 with the same last sequent. Making this replacement in the derivation π, we obtain the following derivation $\hat{\pi}$, which has only n mixes:

$$\dfrac{\vdots \ \pi_4 \ \vdots}{\pi_3}\,\mathtt{R}$$

By induction hypothesis, the derivation $\hat{\pi}$ is equivalent with some normal derivation π'.

End of the proof of Theorem 3.1.2. We now have to prove Lemma 3.1.6. We shall do this by induction over a notion of *rank* of a mix rule, that we define below.

Definition 3.1.7 *Let us consider a mix:*

$$\dfrac{\dfrac{\pi_1}{\vdots}\,\mathtt{R1} \qquad \dfrac{\pi_2}{\vdots}\,\mathtt{R2}}{\Gamma \vdash \Delta \qquad \Gamma' \vdash \Delta'}\,\mathtt{mix}$$
$$\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'$$

(on this figure π_1 (resp. π_2) designates a tuple of proofs that have, as last sequents, the upper-sequents of the mix.
- A is the formula of the mix.
- the active *occurrences of A are those which are cancelled by the mix in the multisets Δ and Γ'.*
- the degree *d of the mix is the size of A (i.e. its number of connectors and quantifiers)*
- the height *h of the mix is the sum $|\pi_1| + |\pi_2|$ where $|\pi|$ designates the number of nodes of the derivation π.*
- the rank *r of the mix is the couple of integers (d, h).*

The principal formula of a rule introducing a symbol Q (a connector or a quantifier) is the formula which contains the new occurrence of Q. A mix is called *strict* if both integers n, m in Definition 3.1.3 are non-null. Since our proof of Lemma 3.1.5 has shown that a non-strict mix can be simulated by a derivation without cut, we only have to treat strict mixes.
We consider all the possible values of (R1,R2) to gether with the fact that the principal formula of rule R1 (resp. R2) is active in the mix (or not). In principle we should thus examine $18^2 \times 4 = 1296$ cases. Fortunately, these cases can be grouped into only a reasonable number of "types of cases". We shall enumerate and treat such types of cases.
CASE 1: R1 or R2 is an axiom.
Subcase 1.1: R1 is $\bot_l$.
Then $m = 0$ i.e. the mix is not strict.
Subcase 1.2: R2 is $\bot_l$ and $\bot$ is inactive.
Then $n = 0$ i.e. the mix is not strict.
Subcase 1.3: R2 is $\bot_l$ and $\bot$ is active.

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta\end{array}}{}\,\mathtt{R1} \qquad \dfrac{}{\bot \vdash}\,\bot_l}{\Gamma \vdash \Delta_\bot}\,\mathtt{mix}$$

One can prove, by induction over the length of derivations that:
for every multisets of formulas Γ, Δ and integer $m \geq 0$, if there exists some normal derivation for $\Gamma \vdash \Delta + m\bot$, then there exists some normal derivation for $\Gamma \vdash \Delta$. (This is a tedious but routine proof that we ... leave to the reader).
Subcase 1.4: R1 is ax and the introduced formula (on the right) is inactive.
Hence $m = 0$ and the mix is not strict.
Subcase 1.5: R1 is ax and the introduced formula (on the right) is active.

$$\dfrac{\dfrac{}{A \vdash A}\,\mathtt{ax} \qquad \dfrac{}{\Gamma' \vdash \Delta'}\,\mathtt{R2}}{A, \Gamma'_A \vdash \Delta'}\,\mathtt{mix}$$

We recall that $\Gamma' = \Gamma' + nA$. Since the formula A of ax is active, $n \geq 1$. If $n = 1$, π_2 followed by R2, is a normal derivation of $A, \Gamma'_A \vdash \Delta'$. If $n \geq 2$, the derivation π_2, followed by R2 and then $(n-1)$ left-contractions, is a normal

derivation of $A, \Gamma'_A \vdash \Delta'$.
Subcase 1.6: R2 is ax.
This subcase is symmetric with subcases 1.4, 1.5 treated above (left-contractions must be replaced by right-contractions in the subcase where the formula, introduced on the left, is active).
CASE 2: R1 or R2 is a structural rule.
Subcase 2.1: R1 is a left-weakening.

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta\end{array}}{\Gamma, B \vdash \Delta}\,\mathtt{wkn}_l \qquad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash \Delta'\end{array}}{}\,\mathtt{R2}}{\Gamma, B, \Gamma'_A \vdash \Delta_A, \Delta'}\,\mathtt{mix}$$

We can derive the same final sequent by the following derivation:

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta\end{array} \qquad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash \Delta'\end{array}}{}\,\mathtt{R2}}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\,\mathtt{mix}}{\Gamma, B, \Gamma'_A \vdash \Delta_A, \Delta'}\,\mathtt{wkn}_l$$

The unique mix of this derivation has rank $(|B|, |\pi_1| + |\pi_2|)$ while the initial mix has a rank equal to $(|B|, |\pi_1|+1+|\pi_2|)$. Hence, by induction hypothesis, this mix can be eliminated.
Subcase 2.2: R1 is a right-weakening and the introduced formula (on the right) is inactive.
The mix can be removed as we did in Subcase 2.1.
Subcase 2.3: R1 is a right-weakening and the introduced formula (on the right) is active.

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta\end{array}}{\Gamma \vdash \Delta, A}\,\mathtt{wkn}_r \qquad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash \Delta'\end{array}}{\text{---}}\,\mathtt{R2}}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\,\mathtt{mix}$$

We can derive the same final sequent by the following derivation:

$$\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta\end{array} \qquad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash \Delta'\end{array}}{\text{---}}\,\mathtt{R2}}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\,\mathtt{mix}$$

This derivation has only one mix, which is the last rule, and it has rank $(|A|, |\pi_1| + |\pi_2| + 1)$ while the initial mix has a rank equal to $(|A|, |\pi_1| + 1 + |\pi_2| + 1)$. Hence, by induction hypothesis, this mix can be eliminated.

Subcase 2.4: R2 is a right-weakening.
Analogous with Subcase 2.1.

Subcase 2.5: R2 is a left-weakening.
Analogous with Subcases 2.2,2.3.

Subcase 2.6: R1 is a left-contraction.
Analogous with Subcase 2.1: we can commute the mix rule and the left-contraction.

Subcase 2.7: R1 is a right-contraction.
The mix can be reduced to a mix with smaller rank by the same kind of transformation as in Subcase 2.3.

Subcase 2.8: R2 is a contraction.
Analogous with Subcases 2.6, 2.7.

CASE 3: R1 and R2 are introduction rules. One of the principal formulas is inactive.
The common idea that allows to treat all the instances of this case is that it is possible to commute the rule which introduces an inactive formula with the mix rule: this is not surprising since these two rules do not "act" on any common formula.
We distinguish subcases according to the rule which introduces an inactive formula.

Subcase 3.1: R1 is $\wedge_\ell$.
Of course its principal formula is inactive (it is not on the side of the mix).

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma, B, C \vdash \Delta\end{array}}{\Gamma, B \wedge C \vdash \Delta}\wedge_l \quad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash \Delta'\end{array}}{}\texttt{R2}}{\Gamma, \Gamma'_A, B \wedge C \vdash \Delta_A, \Delta'}\texttt{mix}$$

We can derive the same final sequent by the following derivation:

$$\dfrac{\dfrac{\begin{array}{cc}\pi_1 & \pi_2\\ \vdots & \vdots\\ \Gamma, B, C \vdash \Delta & \Gamma' \vdash \Delta'\end{array}}{\Gamma, \Gamma'_A, B, C \vdash \Delta_A, \Delta'}\texttt{mix}}{\Gamma, \Gamma'_A, B \wedge C \vdash \Delta_A, \Delta'}\wedge_l \quad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash \Delta'\end{array}}{}\texttt{R2}$$

This derivation has only one mix, which has rank $(|A|, |\pi_1| + |\pi_2| + 1)$ while the initial mix has a rank equal to $(|A|, |\pi_1| + 1 + |\pi_2| + 1)$. Hence, by induction hypothesis, this mix can be eliminated.
Subcase 3.2: R2 is $\wedge_r$.
Of course its principal formula is inactive (it is not on the side of the mix). The same kind of transformation as for Subcase 3.1 can be preformed i.e. we can commute the mix and the $\wedge_r$ rule. Here also the rank of the new mix is strictly smaller, hence the conclusion.
Subcase 3.3: R1 is $\wedge_r$, its principal formula is inactive.

$$\dfrac{\dfrac{\begin{array}{cc}\pi_{1,1} & \pi_{1,2}\\ \vdots & \vdots\\ \Gamma \vdash B, \Delta & \Gamma \vdash C, \Delta\end{array}}{\Gamma \vdash B \wedge C, \Delta}\wedge_r \quad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash \Delta'\end{array}}{}\texttt{R2}}{\Gamma, \Gamma'_A \vdash B \wedge C, \Delta_A, \Delta'}\texttt{mix}$$

The derivation can be transformed into

$$\dfrac{\dfrac{\dfrac{\pi_{1,1}}{\vdots}\quad\dfrac{\dfrac{\pi_2}{\vdots}}{\Gamma' \vdash \Delta'}\mathtt{R2}}{\Gamma \vdash B, \Delta \quad \Gamma' \vdash \Delta'}\mathtt{mix} \quad \dfrac{\dfrac{\pi_{1,2}}{\vdots}\quad\dfrac{\dfrac{\pi_2}{\vdots}}{\Gamma' \vdash \Delta'}\mathtt{R2}}{\Gamma \vdash C, \Delta \quad \Gamma' \vdash \Delta'}\mathtt{mix}}{\Gamma, \Gamma'_A \vdash B, \Delta_A, \Delta' \qquad \Gamma, \Gamma'_A \vdash C, \Delta_A, \Delta'}\wedge_r$$
$$\Gamma, \Gamma'_A \vdash B \wedge C, \Delta_A, \Delta'$$

This new derivation has two incomparable mix rules (i.e. one is not an ancestor of the other). Their ranks are $(|A|, |\pi_{1,1}| + |\pi_2|)$ (for the leftmost one) and $(|A|, |\pi_{1,2}| + |\pi_2|)$ (for the rightmost one). Since the ranks are strictly smaller than $(|A|, |\pi_{1,1}| + |\pi_{1,2}| + |\pi_2| + 1)$, by induction hypothesis, these two mixes can be removed (independently one from each other). We thus obtain a normal proof.

Subcase 3.4: R2 is $\wedge_\ell$.

Similar to Subcase 3.3.

Subcase 3.5: R1 is $\vee_r$ or $\vee_\ell$, its principal formula is inactive.

Dual to the Subcases 3.4, 3.2

Subcase 3.6: R2 is $\vee_r$ or $\vee_\ell$, its principal formula is inactive.

Dual to the Subcases 3.1, 3.3

Subcase 3.7: R1 is $\to_\ell$.

The principal formula of $\to_\ell$ is inactive (it is not on the side of the mix). Since rule $\to_\ell$ is very similar to rule $\wedge_r$, we can use a transformation very similar to the one used in Subcase 3.3.

$$\dfrac{\dfrac{\dfrac{\pi_{1,1}}{\vdots}\quad\dfrac{\pi_{1,2}}{\vdots}}{\Gamma \vdash B, \Delta \quad \Gamma, C \vdash \Delta}\to_l \quad \dfrac{\dfrac{\pi_2}{\vdots}}{\Gamma' \vdash \Delta'}\mathtt{R2}}{\Gamma, B \to C \vdash \Delta \qquad \Gamma' \vdash \Delta'}\mathtt{mix}$$
$$\Gamma, \Gamma'_A, B \to C \vdash \Delta_A, \Delta'$$

We can derive the same final sequent by the following derivation:

$$\dfrac{\dfrac{\dfrac{\pi_{1,1}}{\vdots}\quad\dfrac{\dfrac{\pi_2}{\vdots}}{\Gamma' \vdash \Delta'}\,\texttt{R2}}{\Gamma \vdash B, \Delta}\,\texttt{mix}\qquad\dfrac{\dfrac{\dfrac{\pi_{1,2}}{\vdots}\quad\dfrac{\dfrac{\pi_2}{\vdots}}{\Gamma' \vdash \Delta'}\,\texttt{R2}}{\Gamma, C \vdash \Delta'}\,\texttt{mix}}{\Gamma, \Gamma'_A, C \vdash \Delta_A, \Delta'}}{\Gamma, \Gamma'_A, B \to C \vdash \Delta_A, \Delta'}\,{\to_l}$$

We end this subcase by the arguments already used in Subcase 3.3.
Subcase 3.8: R1 is $\to_r$.
Close to Subcase where R1 is $\vee_r$, see above.
Subcase 3.9: R2 is $\to_r$.
Close to Subcase where R2 is $\vee_r$, see above.
Subcase 3.10: R1 is $\neg_\ell$ or R1 is $\neg_r$ or R2 is $\neg_\ell$ or R2 is $\neg_r$.
Solved by the same kind of commutation.
Subcase 3.11: R1 is $\forall_\ell$ or R1 is $\exists_r$ or R2 is $\forall_\ell$ or R2 is $\exists_r$.
Solved by the same kind of commutation.
Subcase 3.12: R1 is $\exists_\ell$.

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdots}}{\Gamma, B \vdash \Delta}\,{\exists_l}\qquad\dfrac{\dfrac{\pi_2}{\vdots}}{\Gamma' \vdash \Delta'}\,\texttt{R2}}{\Gamma, \exists x\ B \vdash \Delta'\qquad \Gamma' \vdash \Delta'}\,\texttt{mix}}{\Gamma, \Gamma'_A, \exists x\ B \vdash \Delta_A, \Delta'}$$

We assume that $x \notin \mathrm{FV}(\Gamma, \Delta)$, since this condition is part of the hypothesis that the above tree of formulas is a derivation in LK. Let us choose a variable $y \notin \mathrm{FV}(\Gamma + \Delta + \Gamma' + \Delta')$. For every proof π in LK, and every couple of variables (v, v') we denote by $\pi[v := v']$ the tree of fomulas obtained by applying to every formula (which is a label of this tree) the operation $[v := v']$ (c.f. Definition 1.3.3). We claim that this tree is also a proof in

LK. We can derive the same final sequent by the following derivation:

$$\dfrac{\dfrac{\dfrac{\pi_1[x := y] \qquad \pi_2}{\Gamma, B[x := y] \vdash \Delta \quad \Gamma' \vdash \Delta'}\,\mathtt{mix}}{\Gamma, \Gamma'_A, B[x := y] \vdash \Delta_A, \Delta'}\,\exists_l}{\Gamma, \Gamma'_A, \exists y\, B[x := y] \vdash \Delta_A, \Delta'}$$

Note that the last application of rule, which is assumed to use rule $\exists_l$, does meet the restriction that $y \notin \mathrm{FV}(\Gamma + \Delta + \Gamma' + \Delta')$ (by choice of y) and that, since

$$\exists y\, B[x := y] \equiv_\alpha \exists x\, B$$

the conclusion of this derivation (remember it is a multiset of α-equivalence classes) is equal to

$$\Gamma, \Gamma'_A, \exists x\, B \vdash \Delta_A, \Delta'.$$

Subcase 3.13: R2 is $\exists_\ell$ or R1 is $\forall_r$ or R2 is $\forall_r$.
These subcases raises the same kind of difficulty as Subcase 3.12 (i.e. validity of the rules $\exists_\ell, \forall_r$ require that some variable does not appear in the context) and is solved by the same kind of trick (applying a substitution to a subproof).

CASE 4: R1 and R2 are introduction rules. Both principal formulas are active.
We distingusih one subcase for each connector or quantifier. R1 introduces the connector (resp. quantifier) on the right while R2 introduces the connector (resp. quantifier) on the left.
Subcase 4.1: R1 is $\vee_r$ and R2 is $\vee_\ell$.
The active formula is $A = B \vee C$. A derivation π of this type has the

following form:

$$\dfrac{\dfrac{\begin{array}{ccc}\pi_1 & \pi_2 & \pi_3\\ \vdots & \vdots & \vdots\\ \Gamma \vdash \Delta, B, C & B, \Gamma' \vdash \Delta' & C, \Gamma' \vdash \Delta'\end{array}}{\Gamma \vdash \Delta, B \vee C \quad B \vee C, \Gamma' \vdash \Delta'}\vee_r \quad \vee_l}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\texttt{mix}$$

This derivation can be transformed into

$$\dfrac{\dfrac{\dfrac{\begin{array}{cc}\pi_1 & \dfrac{\begin{array}{cc}\pi_2 & \pi_3\\ \vdots & \vdots\end{array}}{\Gamma', B \vee C \vdash \Delta'}\vee_l\\ \vdots & \\ \Gamma \vdash \Delta, B, C & \end{array}}{\Gamma, \Gamma'_A \vdash B, C, \Delta_A, \Delta'}\texttt{mix1} \quad \dfrac{\begin{array}{cc}\pi_1 & \pi_2\\ \vdots & \vdots\\ \Gamma \vdash \Delta, B \vee C & B, \Gamma' \vdash \Delta'\end{array}}{\Gamma, \Gamma'_A, B \vdash \Delta_A, \Delta'}\vee_r\texttt{mix2}}{2\Gamma, 2\Gamma'_A \vdash C, 2\Delta_A, 2\Delta'}\texttt{mix} \quad \dfrac{\begin{array}{cc}\pi_1 & \pi_3\\ \vdots & \vdots\\ \Gamma \vdash \Delta, B \vee C & C, \Gamma' \vdash \Delta'\end{array}}{\Gamma, \Gamma'_A, C \vdash \Delta_A, \Delta'}\vee_r\texttt{mix}}{3\Gamma, 3\Gamma'_A \vdash 3\Delta_A, 3\Delta'}\texttt{ctr}^*$$
$$\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'$$

This new derivation contains five mixes. The mixes numbered 1,2,3 are (respectively) the last rule of a sub-derivation using exactly one mix. Moreover these mixes have a rank which is strictly less than the rank of the original mix (the degree remains the same but the height is strictly smaller). By induction hypothesis, the sub-derivation ending with the rule mix$i$ can be replaced by a normal derivation $\hat{\pi}_i$. We thus get a derivation π' equivalent with π:

$$\dfrac{\dfrac{\dfrac{\begin{array}{ccc}\hat{\pi}_1 & \hat{\pi}_2 & \\ \vdots & \vdots & \hat{\pi}_3\\ \Gamma, \Gamma'_A \vdash B, C, \Delta_A, \Delta' & \Gamma, \Gamma'_A, B \vdash \Delta_A, \Delta' & \vdots\end{array}}{2\Gamma, 2\Gamma'_A \vdash C, 2\Delta_A, 2\Delta'}\texttt{mix} \quad \Gamma, \Gamma'_A, C \vdash \Delta_A, \Delta'}{3\Gamma, 3\Gamma'_A \vdash 3\Delta_A, 3\Delta'}\texttt{mix}}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\texttt{ctr}^*$$

The two mixes occurring in derivation π' have a degree ($|B|$ or $|C|$) which is strictly smaller than $|A|$, hence, using twice the induction hypothesis, these

two mixes can be removed.
Subcase 4.2: R1 is $\wedge_r$ and R2 is $\wedge_\ell$.
This subcase reduces, by duality, to Subcase 4.1.
Subcase 4.3: R1 is $\to_r$ and R2 is $\to_\ell$.
This subcase is similar to Subcase 4.1.
Subcase 4.4: R1 is $\neg_r$ and R2 is $\neg_\ell$.
The active formula is $A = \neg B$. A derivation π of this type has the follwoing form:

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma, B \vdash \Delta\end{array}}{\Gamma \vdash \Delta, \neg B}\neg_r \quad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash B, \Delta'\end{array}}{\neg B, \Gamma' \vdash \Delta'}\neg_l}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\texttt{mix}$$

This derivation can be transformed into

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta, \neg B\end{array}}{}\neg_r \quad \begin{array}{c}\pi_2\\ \vdots\\ \Gamma' \vdash B, \Delta'\end{array}}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta', B}\texttt{mix1} \quad \dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma, B \vdash \Delta\end{array} \quad \begin{array}{c}\pi_2\\ \vdots\\ \neg B, \Gamma' \vdash \Delta'\end{array}}{B, \Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\neg_l\texttt{mix2}}{2\Gamma, 2\Gamma'_A \vdash 2\Delta_A, 2\Delta'}\texttt{mix3}}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\texttt{ctr}^*$$

where mix1,mix2 have same degree but strictly smaller height than the original mix. By induction hypothesis these two mixes can be eliminated. We are then left with a derivation with one mix (inherited from mix3), which has degree $|B| < |A|$. Hence, by induction hypothesis, this last mix can also be eliminated.
Subcase 4.5: R1 is $\forall_r$ and R2 is $\forall_\ell$.
The active formula is $A = \neg B$. A derivation π of this type has the following

form:

$$\dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta, B\end{array}}{\Gamma \vdash \Delta, \forall x\ B}\forall_r \quad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ B[x := t], \Gamma' \vdash \Delta'\end{array}}{\forall x\ B, \Gamma' \vdash \Delta'}\forall_l}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\texttt{mix}$$

This derivation can be transformed into

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\pi_1[x := t]\\ \vdots\\ \Gamma \vdash \Delta, B[x := t]\end{array} \quad \dfrac{\begin{array}{c}\pi_2\\ \vdots\\ \forall x\ B, \Gamma' \vdash \Delta'\end{array}}{\forall x\ B, \Gamma' \vdash \Delta'}\forall_l}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta', B[x := t]}\texttt{mix2} \quad \dfrac{\dfrac{\begin{array}{c}\pi_1\\ \vdots\\ \Gamma \vdash \Delta, \forall x\ B\end{array}}{\forall x\ B}\forall_r \quad \begin{array}{c}\pi_2\\ \vdots\\ B[x := t], \Gamma' \vdash \Delta'\end{array}}{B[x := t], \Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\texttt{mix1}}{2\Gamma, 2\Gamma'_A \vdash 2\Delta_A, 2\Delta'}\texttt{mix3}}{\Gamma, \Gamma'_A \vdash \Delta_A, \Delta'}\texttt{ctr}^*$$

where $\pi_1[x := t]$ is the derivation obtained by preserving the tree-structure and the rules of π_1 and applying the substitution $[x := t]$ to every formula. We can finally eliminate mix1,mix2 by the arguments used in Subcase 4.4. We are then left with a derivation with one mix (inherited from mix3), which has degree $|B[x := t]|$. Since the size of a formula is its number of connectives and quantifiers, $|B[x := t]| < |A|$, and we can conclude using the induction hypothesis.

Subcase 4.6: R1 is $\exists_r$ and R2 is $\exists_\ell$.

Dual to Subcase 4.5

3.2 LK is consistent

We develop now the consequences of the cut elimination theorem. A first bunch of consequences is that some sequents cannot be derived in LK or in LJ. In particular we shall see that $\vdash$ or $\vdash \bot$ are not derivable, a result that is also called the "consistency of LK". This kind of result was a major concern of mathematical logics at the beginning of the 20th century.

A second bunch of consequences (developed in next section) will consist in seeing that "LJ is constructive" i.e. that when a statement of the form $\exists y \Phi(x, y)$ is derivable in LJ then a witness t such that $\Phi(x, t)$ is derivable can always be deduced form the given LJ-derivation.

Theorem 3.2.1 *The sequent* $\vdash$ *is neither derivable in* LK *nor in* LJ.

Proof: Let us assume that $\vdash$ is derivable in LK. Then there would exist a normal derivation of $\vdash$. But there is no rule in LK$\setminus\{\texttt{cut}\}$ that can have this sequent as lower part. The same arguments apply on LJ. □

Theorem 3.2.2 *Let A be some atomic formula.*
1- $\vdash A$ *is not derivable in* LK
2- If $A \neq \bot$, *neither* $A \vdash$ *nor* $\vdash \neg A$ *are derivable in* LK.

Proof: 1- The formula A has no occurrence of connector or quantifier. Thus every multiset of the form $\vdash nA$ can be the lower part of a rule $R \neq \texttt{cut}$ only if R is a structural rule and the upper part is itself of the same form. Hence none of these sequents is an axiom. Consequently there is no normal proof of a sequent of the form $\vdash nA$.
2- Suppose that $A \neq \bot$. Thus every multiset of the form $nA \vdash m\neg A$ can be the lower part of a rule $R \neq \texttt{cut}$ only if R is a structural rule or the rule $\neg_r$ and the upper part is itself of the same form. Since $A \neq \bot$, none of these multisets is an axiom. Consequently there is no normal proof of a sequent of the form $nA \vdash m\neg A$.
□

3.3 LJ is constructive

For sake of brevity, for every formal system F, we denote by $\Gamma \vdash_F \Delta$ the fact that $\Gamma \vdash \Delta$ is derivable in F.

Theorem 3.3.1 *Let A, B be formulas.*
1- If $\vdash_{\mathrm{LJ}} A \vee B$ then $\vdash_{\mathrm{LJ}} A$ or $\vdash_{\mathrm{LJ}} B$.
2- If $\vdash_{\mathrm{LJ}} \exists x\ A$ then, there exists some term t such that $\vdash_{\mathrm{LJ}} A[x := t]$.

Proof: 1- Suppose that $\vdash A \vee B$ is derivable in LJ. By the cut elimination theorem, it also has a normal derivation. The last rule of this derivation must be a $\vee_r^1$ or $\vee_r^2$ or a right-weakening. Since $\vdash$ is not derivable the last rule can only be a $\vee_r^1$ or $\vee_r^2$ and the upper-part of this rule is either $\vdash A$ or $\vdash B$.
2- A similar argument applies here, based on the $\exists_r$ rule. □
The above property of LJ can be named "constructivity" of LJ in the sense that, every time one derives merely the existence of some object x , it is possible, by elimination of the cuts in the derivation, to *construct* a witness t of this existence assertion.

Theorem 3.3.2 *Let A be an atomic formula, $A \neq \bot$.*
The sequent $A \vee \neg A$ is not derivable in LJ.

Proof: Suppose $A \neq \bot$ and $\vdash_{\mathrm{LJ}} A \vee \neg A$. By Theorem 3.3.1 either $\vdash_{\mathrm{LJ}} A$ or $\vdash_{\mathrm{LJ}} \neg A$. But Theorem 3.2.2 shows this is impossible. Hence $\vdash_{\mathrm{LJ}} A \vee \neg A$ does not hold. □
Let us remark that, for every formula A, $\vdash_{\mathrm{LK}} A \vee \neg A$:

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathtt{ax}}{\vdash A, \neg A}\,\neg_r}{\vdash A \vee \neg A}\,\vee_r$$

Hence the system LJ is strictly weaker than the system LK i.e.

$$\{\Phi \in \mathcal{L}_1(\mathcal{S}, \mathcal{V}) \mid \vdash_{\mathrm{LJ}} \Phi\} \subset \{\Phi \in \mathcal{L}_1(\mathcal{S}, \mathcal{V}) \mid \vdash_{\mathrm{LK}} \Phi\}.$$

We would like to extend the constructivity statement for LJ (Theorem 3.3.1) to axiomatic theories i.e. to sequents of the form

$$\mathrm{AX} \vdash \exists x\ \ A$$

where AX is some set of formulas (meaningful examples will be sets of axioms like the equality axioms, the monoid axioms, the group axioms, etc ...)

It is clear that if some axiom is of the form $\exists x\ \Phi(x)$ this property will fail. Therefore we define a notion of "Harrop formula" which captures the intuitive idea that it does not assert the existence of some object (neither a disjunction of assertions).

Definition 3.3.3 *Let $*$ be a new symbol of arity* 0.
1- The set of contexts *over the signature $\mathcal{S}$ and the set of variables $\mathcal{V}$ is the subset of formulas over the signature $\mathcal{S} \cup \{*\}$ that contain exactly one occurrence of the symbol $*$.*
2- Given a context C and a formula $A \in \mathcal{L}_1(\mathcal{S}, \mathcal{V})$ we denote by $C\langle\Phi\rangle$ the word obtained by replacing the unique occurrence of the symbol $*$ in C by the word Φ.

Note that the above defined $C\langle\Phi\rangle$ is identical with the $C[* \leftarrow \Phi]$ introduced by Definition 1.3.2 if we consider $*$ as a variable; (but the symbol $*$ cannot be quantified neither in C nor in Φ; this is why we prefer to consider $*$ as a constant and use a new notation).

Definition 3.3.4 *A formula B is called a* subformula *of formula A iff there exists a context C such that $A = C\langle B\rangle$.*

Definition 3.3.5 *1- We define inductively the set of* strictly positive contexts *(abreviated as* spc*) by:*
- the symbol $*$ is a spc
- if C is a spc *and A is a formula, then*

$$A \wedge C, C \wedge A, A \vee C, C \vee A, A \rightarrow C, \forall x\ C$$

are spc*.*
2- A subformula B of the formula A is called strictly positive sub-formula *(abreviated as* sps*) iff there exists some* spc *C such that*

$$A = C\langle B\rangle.$$

Example 3.3.6 *Let*

$$P := ((A \rightarrow \forall x\ B) \vee \exists x\ (C \rightarrow D)) \wedge ((E \vee F) \rightarrow (\exists x\ \ G \wedge H)).$$

B, D, G, H are sps *of P while A, C, E, F are not* sps *of P.*

Theorem 3.3.7 *Let* Γ *be a multiset of formulas where* $\vee$ *is not the principal operator of any* sps. *Let* E, F *be two formulas. The sequent* $\Gamma \vdash E \vee F$ *is derivable in* LJ *iff* $\Gamma \vdash_{\mathrm{LJ}} E$ *or* $\Gamma \vdash_{\mathrm{LJ}} F$.

Proof: We proceed by induction over the size of a normal proof in LJ of $\Gamma \vdash E \vee F$. Let us distinguish several cases according to the last rule of this derivation.
Case 1: axiom.
This case is impossible since $\vee$ is not the principal operator of any formula of Γ.
Case 2: $\bot_\ell$.
Impossible: the rhs of the sequent do not match.
Let us list the right-rules:
since the principal operator of the rhs is $\vee$, only two rules are possible: right-weakening and $\vee_r$.
Case 3: $\mathtt{wkn}_r$.
In this case the upper-part of the rule is $\Gamma \vdash$. It follows that $\Gamma \vdash_{\mathrm{LJ}} E$ and $\Gamma \vdash_{\mathrm{LJ}} F$.
Case 4: $\vee_r$.
Hence the upper-part of the rule is $\Gamma \vdash E$ or $\Gamma \vdash F$, which shows that one of them is derivable in LJ.
Let us list the left-rules:
Case 5: $\vee_\ell$.
Impossible since it would imnply that some formula of Γ has a principal operator equal to $\vee$.
Case 6: $\neg_\ell$.
Impossible: the rhs of the sequents do not match: the one of the lower-part of the rule is empty while the one of the sequent consists of one formula.
Case 7: $\mathtt{wkn}_\ell$.
The proof has the form

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma' \vdash E \vee F\end{array}}{\Gamma', A \vdash E \vee F}\,\mathtt{wkn}_l$$

By induction hypothesis $\Gamma' \vdash_{\mathrm{LJ}} E$ or $\Gamma' \vdash_{\mathrm{LJ}} F$. Hence, by adding the same formula A on the left (thanks to the left-weakening rule) $\Gamma \vdash_{\mathrm{LJ}} E$ or $\Gamma \vdash_{\mathrm{LJ}} F$.

Case 8: $\texttt{contr}_\ell$.
Similar reasoning as in Case 7.
Case 9: $\wedge_\ell$.

$$\frac{\begin{array}{c}\vdots\\ \Gamma', A, B \vdash E \vee F\end{array}}{\Gamma', A \wedge B \vdash E \vee F}\wedge_l$$

By induction hypothesis $\Gamma', A, B \vdash_{\mathrm{LJ}} E$ or $\Gamma', A, B \vdash_{\mathrm{LJ}} F$. Hence, by applying the rule $\wedge_\ell$ we obtain that: $\Gamma \vdash_{\mathrm{LJ}} E$ or $\Gamma \vdash_{\mathrm{LJ}} F$.
Case 10: $\forall_\ell$.

$$\frac{\begin{array}{c}\vdots\\ \Gamma', A[x := t] \vdash E \vee F\end{array}}{\Gamma', \forall x\ A \vdash E \vee F}\forall_l$$

Let H be some sps of $A[x := t]$. Then it has the form $K[x := t]$ for some sps K of $A[x := t]$. The formula K is also a sps of $\forall x\ A$, hence of Γ. By assumption the principal operator of K is nor $\vee$. Hence the principal operator of H is nor $\vee$. The multiset $\Gamma' + A[x := t]$ fulfills the hypothesis of the theorem and its proof is strictly smaller. By induction hypothesis $\Gamma', A[x := t] \vdash_{\mathrm{LJ}} E$ or $\Gamma', A[x := t] \vdash_{\mathrm{LJ}} F$. Hence, by applying the rule $\forall_\ell$ we obtain that: $\Gamma \vdash_{\mathrm{LJ}} E$ or $\Gamma \vdash_{\mathrm{LJ}} F$.
Case 11: $\exists_\ell$.
Similar reasoning as in Case 10 (without the substitution $[x := t]$).
Case 12: $\rightarrow_\ell$.

$$\frac{\begin{array}{cc}\vdots & \vdots\\ \Gamma' \vdash A & \Gamma', B \vdash E \vee F\end{array}}{\Gamma', A \rightarrow B \vdash E \vee F}\rightarrow_l$$

By induction hypothesis $\Gamma', B \vdash_{\mathrm{LJ}} E$ or $\Gamma', B \vdash_{\mathrm{LJ}} F$. Composing this derivation with the derivation of $\Gamma' \vdash A$, by using rule $\rightarrow_\ell$, we obtain a derivation in LJ of $\Gamma', A \rightarrow B \vdash_{\mathrm{LJ}} E$ or $\Gamma', A \rightarrow B \vdash_{\mathrm{LJ}} F$.

(Note we treated 12 cases while there are 17 rules in LJ$\setminus\{\texttt{cut}\}$; this is due to the fact that the five rules $\wedge_r, \rightarrow_r, \neg_r, \forall_r, \exists_r$ cannot have a lower-part equal to $\Gamma \vdash E \vee F$). $\square$

Theorem 3.3.8 *Let Γ be a multiset of formulas where $\exists$ is not the principal operator of any* sps. *Let E be some formula. The sequent $\Gamma \vdash \exists x\ E$ is derivable in* LJ *iff, there exist a finite sequence of terms $t_1, \ldots, t_n$ such that*

$$\Gamma \vdash E[x := t_1] \vee \ldots \vee E[x := t_n]$$

Proof: We proceed by induction over the size of a normal proof in LJ of $\Gamma \vdash \exists x\ E$. As for proving Theorem 3.3.7, we distinguish several cases according to the last rule of this derivation.
Case 1 (axiom), **Case 2**($\bot_\ell$), **Case 3**($\texttt{wkn}_r$) are treated as in the previous proof.
Case 4: The rule $\vee_r$ is impossible here. Let us consider the rule $\exists_r$ instead. The upper-part of this rule has the form $\Gamma \vdash E[x := t]$ for some term t. Hence $\Gamma \vdash_{\mathrm{LJ}} E[x := t]$.
Case 5: $\vee_\ell$.

$$\frac{\begin{array}{cc}\vdots & \vdots \\ \Gamma', A \vdash \exists x\ E & \Gamma', B \vdash \exists x\ E\end{array}}{\Gamma', A \vee B \vdash \exists x\ E}\vee_l$$

By induction hypothesis, there exist $p, q \in \mathbb{N}$ and terms t_i for $1 \leq i \leq p+q$ such that

$$\Gamma', A \vdash_{\mathrm{LJ}} E[x := t_1] \vee \ldots \vee E[x := t_p] \text{ and } \Gamma', B \vdash_{\mathrm{LJ}} E[x := t_{p+1}] \vee \ldots \vee E[x := t_{p+q}].$$

Using $p+q$ times rule $\vee_r$ we obtain

$$\Gamma', A \vdash_{\mathrm{LJ}} \bigvee_{i=1}^{p+q} E[x := t_i] \text{ and } \Gamma', B \vdash_{\mathrm{LJ}} \bigvee_{i=1}^{p+q} E[x := t_i].$$

Using now rule $\vee_\ell$, we obtain from the two above sequents

$$\Gamma', A \vee B \vdash_{\mathrm{LJ}} \bigvee_{i=1}^{p+q} E[x := t_i].$$

Case 6 ($\neg_\ell$), **Case 7** ($\mathtt{wkn}_\ell$), **Case 8** ($\mathtt{contr}_\ell$), **Case 9**($\wedge_\ell$), **Case 10**($\forall_\ell$), **Case 11**($\exists_\ell$), **Case 12**($\rightarrow_\ell$) can be treated in the same way as for Theorem 3.3.7. □

Definition 3.3.9 *A formula Φ is called a Harrop formula iff, no* sps *of Φ has $\vee$ or $\exists$ as principal operator (i.e. root symbol).*

Example 3.3.10 *let us consider the formulas*

$$\Phi := [\exists x\ P(x)] \wedge [\forall y\ (Q(Y) \rightarrow P(S(y)))],\quad \Psi := \neg\Phi.$$

Let $C := [*] \wedge [\forall y\ (Q(Y) \rightarrow P(S(y)))]$ and $B := \exists x\ P(x)$. one can check that:
$\Phi = C\langle B\rangle$ and C is a strictly positive context and B has an $\exists$ as principal operator. Hence Φ is not a Harrop formula.
The formula Ψ has only one spc C *such that $\Psi = C\langle\Psi'\rangle$ for some Ψ': $C := *$. But the subformula occuring in this context is $\neg\Phi$ the principal operator of which is $\neg$. Hence Ψ is a Harrop formula. (See figure 3.1).*

Theorem 3.3.11 *Let Γ be a multiset of Harrop formulas. For every formulas A, B and variable x*
1- if $\Gamma \vdash_{\mathrm{LJ}} A \vee B$ then $\Gamma \vdash_{\mathrm{LJ}} A$ or $\Gamma \vdash_{\mathrm{LJ}} B$.
2- if $\Gamma \vdash_{\mathrm{LJ}} \exists x\ A$ then, there exists some term t, such that $\Gamma \vdash_{\mathrm{LJ}} A[x := t]$.

Proof: Direct consequence of Theorem 3.3.7 and Theorem 3.3.8. □

Theorem 3.3.12 *Let Γ, Δ be multisets of formulas. If $\Gamma \vdash_{\mathrm{LK}} \Delta$ (resp. $\Gamma \vdash_{\mathrm{LJ}} \Delta$), then there exists some derivation of this sequent in* LK *(resp.* LJ*) which uses only formulas of the form $A[x_1 := t_1, \ldots, x_n := t_n]$ where A is a sub-formula of Γ, Δ and the t_i's are terms.*

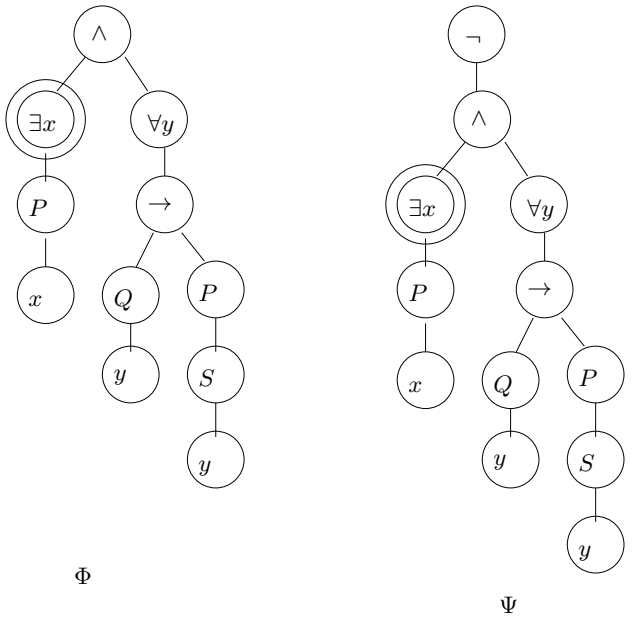

Figure 3.1: The formulas Φ, Ψ.

This is a straightforward consequence of the fact that all the rules of LK $\setminus$ {cut} (resp. LJ $\setminus$ {cut}) have upper-parts which consist of instances of subformulas of their lower-part. Hence every normal derivation (either in LK or in LJ) has the announced property and by Theorem 3.1.2 such a normal derivation exists.

Let us denote by LKP (resp. LJP) the classical sequent calculus (resp. the intuitionnistic sequent calculus) restricted to a signature where all the predicate symbols have arity 0. They are called the classical *propositional* sequent calculus (resp. the intuitionnistic *propositional* sequent calculus).

Corollary 3.3.13 *1- A propositional sequent* $\Gamma \vdash \Delta$ *is derivable in* LK *iff it is derivable in* LKP.
2- A propositional sequent $\Gamma \vdash \Delta$ *is derivable in* LJ *iff it is derivable in* LJP.
3- The derivability in LKP *(resp.* LJP*) is decidable.*

Proof: Points 1,2 follow immediatly from the subformula property stated in Theorem 3.3.12.
Let $\Gamma \vdash \Delta$ be some propositional sequent where all the multiplicities are equal to 1. We know that, if $\Gamma \vdash_{\mathrm{LK}} \Delta$, then there is a derivation of this sequent which is normal. We also have noticed that all the formulas in the sequents of this proof must be subformulas of Γ, Δ (no instanciation is possible here since the formulas do not contain terms). Moreover, one can transform the derivation in such a way that, in every rhs (resp. lhs) of sequent, the multiplicity of a formula is 1 or 2 and there is no repetition of sequent along any branch. The set of such derivations, with only formulas which are subformulas of $\Gamma \vdash \Delta$, with multiplicities ≤ 2 and without repetition on the branches is finite and one can exhaustively enumerate its elements. One can thus test whether one of them terminates in $\Gamma \vdash \Delta$. The same argument applies to LJ. $\Box$

Chapter 4

Semantics

We explicit here what is the *meaning* of a formal statement i.e a formula or a sequent. Of course we assume that the reader has already an intuitive understanding of the connectives and the quantifiers i.e. our ambition is not to teach him the language of mathematics. Our real ambition is to modelize the activity of proving mathematical theorems and to use this modelization for getting some information about what can be expected (and not expected) from mathematical reasoning. For reaching this general aim, we also want to use mathematics as a major modelization tool. Therefore:
1- our theory will be of a mathematical nature: we shall use, namely, set theory.
2- the phenomena that we are modelizing are mathematical proofs and also, "mathematical truth".
This kind of theory is named *metamathematics*: this means it studies mathematics from the outside. Moreover it turns out that our oustside point of view is, itself, mathematical.

This explains why we assume that we (and the reader) are understanding classic basic set theory. We already used it for defining and studying formulas (which are words), sequents, proofs (which are trees labelled by sequents) in Chapters 1-2-3. We keep using it for defining the meaning of formulas (which is a map from formulas into the set $\{true, false\}$, etc ...) Once these definitions are clearly established, we can consider, within set theory, questions about formal systems, for example the crucial question of "what is the

relationship between provability and truth".

4.1 Classical structures

Given a signature

$$\mathcal{S} := \langle R_1, R_2, \ldots, R_n; f_1, f_2, \ldots, f_m \rangle$$

with the arities

$$\langle r_1, r_2, \ldots, r_n; a_1, a_2, \ldots, a_m \rangle$$

a *structure* over $\mathcal{S}$ is a t-uple

$$\mathcal{A} := \langle A; R_1^{\mathcal{A}}, R_2^{\mathcal{A}}, \ldots, R_n^{\mathcal{A}}; f_1^{\mathcal{A}}, f_2^{\mathcal{A}}, \ldots, f_m^{\mathcal{A}} \rangle$$

where A is a non-empty set, for every $i \in [1, n]$, $R_i^{\mathcal{A}}$ is a map from A^{r_i} into the set of booleans $\{0, 1\}$ and, for every $j \in [1, m]$, $f_j^{\mathcal{A}}$ is a map from A^{a_j} into A. We define a new (infinite) signature

$$\mathcal{S}_{\mathcal{A}} := \langle R_1, R_2, \ldots, R_n; f_1, f_2, \ldots, f_m, (\bar{a})_{a \in A} \rangle$$

i.e. $\mathcal{S}_{\mathcal{A}}$ is the signature obtained from $\mathcal{S}$ by adding all symbols $\bar{a}$ for all the elements a of A. Every new function symbol $\bar{a}$ has arity 0, i.e. is a constant symbol. We denote by $\mathcal{L}_1(\mathcal{A})$ (resp. $\mathcal{T}(\mathcal{A})$) the set of formulas (resp. terms) over this new signature $\mathcal{S}_{\mathcal{A}}$.

Definition 4.1.1 *We call* valuation *over the structure $\mathcal{A}$ every (total) map*

$$\nu : \mathcal{T}(\mathcal{A}) \cup \mathcal{L}_1(\mathcal{A}) \to A \cup \{0, 1\}$$

fulfilling all the following clauses:
0- if $t \in \mathcal{T}(\mathcal{A})$ then $\nu(t) \in A$
if $\varphi \in \mathcal{L}_1(\mathcal{A})$ then $\nu(t) \in \{0, 1\}$
1- if $a \in A$, $\nu(\bar{a}) = a$
2- if $t_1, \ldots, t_{a_j} \in \mathcal{T}(\mathcal{A})$ then $\nu(f_j(t_1, \ldots, t_{a_j})) = f_j^{\mathcal{A}}(\nu(t_1), \ldots, \nu(t_{a_j}))$
3- $\nu(\bot) = 0$
4- if $t_1, \ldots, t_{r_i} \in \mathcal{T}(\mathcal{A})$ then $\nu(R_i(t_1, \ldots, t_{r_i})) = R_i^{\mathcal{A}}(\nu(t_1), \ldots, \nu(t_{r_i}))$
5- if $\varphi, \psi \in \mathcal{L}_1(\mathcal{A})$ then $\nu(\varphi \wedge \psi) = \min\{\nu(\varphi), \nu(\psi)\}$
6- $\nu(\varphi \vee \psi) = \max\{\nu(\varphi), \nu(\psi)\}$

7- $\nu(\varphi \to \psi) = \overline{\nu(\varphi)} + \nu(\psi)\}$
8- $\nu(\neg\varphi) = \overline{\nu(\varphi)}$
9- $\nu(\forall v\varphi) = \min\{\nu(\varphi[v \leftarrow \bar{a}]), a \in A\}$
$\nu(\exists v\varphi) = \max\{\nu(\varphi[v \leftarrow \bar{a}]), a \in A\}$

A formula φ is said *closed* if $\mathrm{FV}(\varphi) = \emptyset$ i.e. it has no free variable. One can check, by structural induction, that the value of $\nu(\varphi)$ depends on the values of $\nu(v)$ for $v \in \mathrm{FV}(\varphi)$ only. Hence the boolean value $\nu(\varphi)$ of a closed formula φ is independant of the specific valuation ν. We then write

$$\mathcal{A} \models \varphi$$

to express the fact that $\nu(\varphi) = 1$. This can be rephrased as "φ is true in the structure $\mathcal{A}$". In order to extend this notion of "truth"to arbitray formulas, we define the *universal closure* of a formula φ as follows:
Let $\{z_1, z_2, \ldots, z_k\}$ be the set $\mathrm{FV}(\varphi)$. Then

$$\mathrm{Cl}(\varphi) := \forall z_1 \ \forall z_2 \ \ldots \forall z_k \varphi.$$

(In fact a total ordering over the set $\mathcal{V}$ is required for making this notion well-defined; note, however, that all the formulas obtained by varying the ordering of the first k quantifiers, have the same value for every valuation ν).

Definition 4.1.2 *Given a structure $\mathcal{A}$, a formula $\varphi \in \mathcal{L}_1(\mathcal{S})$ and subset $\Gamma, \Delta \subseteq \mathcal{L}_1(\mathcal{S})$ we define:*
1- $\mathcal{A} \models \varphi$ iff $\mathcal{A} \models \mathrm{Cl}(\varphi)$
2- $\models \varphi$ iff , for every structure $\mathcal{A}$ over the signature $\mathcal{S}$, $\mathcal{A} \models \varphi$
3- $\Gamma \models \varphi$ iff , for every structure $\mathcal{A}$ over the signature $\mathcal{S}$, if , [for every $\psi \in \Gamma$, $\mathcal{A} \models \psi$] then [$\mathcal{A} \models \varphi$]).
4- $\Gamma \models \Delta$ iff ,for every structure $\mathcal{A}$ over the signature $\mathcal{S}$, if , [for every $\psi \in \Gamma$, $\mathcal{A} \models \psi$] then, [there exists some formula $\varphi \in \Delta$ such that $\mathcal{A} \models \varphi$]).

Example 4.1.3 `Develop the example of the 4-squares theorem in various structures.`

Notation: given a subset $\Gamma \subseteq \mathcal{L}_1(\mathcal{S})$ and a formula $\varphi \in \mathcal{L}_1(\mathcal{S})$, the notation

$$\Gamma \vdash_{\mathsf{NK}} \varphi$$

means that there exists a finite subset $\Gamma_0 \subseteq \Gamma$ such that the judgment $\Gamma \vdash \varphi$ is provable within the system NK (and likewise for the notation $\Gamma \vdash_{\mathrm{LK}} \varphi$).

Theorem 4.1.4 (accuracy) *Let* $\Gamma \subseteq \mathcal{L}_1(\mathcal{S}), \varphi \in \mathcal{L}_1(\mathcal{S})$. *Then*

$$\Gamma \vdash_{\mathsf{NK}} \varphi \;\Leftrightarrow\; \Gamma \models \varphi.$$

This theorem is known as the *accuracy* theorem for NK. We know from chapter 2 that the same statement about LK is equivalent.

The fact that

$$\Gamma \vdash_{\mathsf{NK}} \varphi \;\Rightarrow\; \Gamma \models \varphi,$$

is called the *soundness theorem*; it asserts that everything derivable is also true. This is not surprising and also not difficult to establish by inspecting every rule of NK (or LK) and checking that it preserves truth.
The fact that

$$\Gamma \vdash_{\mathsf{NK}} \varphi \;\Leftarrow\; \Gamma \models \varphi,$$

is called the *completeness theorem*;it asserts that a statement which is true in every structure, must have a derivation in NK (or LK). This is much more interesting and indeed not easy to prove! This theorem was first proved by K. Gödel in [Göd30] (for a different, but equivalent, formal system; the equivalence is proved in [Gen35b, 417-431]).

A possible way to prove it consists in establishing first that, if a set Γ is (syntactically) coherent i.e. that there is no proof of $\bot$ from the set of hypotheses Γ, then there exists a structure $\mathcal{A}$ such that $\mathcal{A} \models \Gamma$. The proof of this metatheorem is based on Zorn lemma (or, equivalently, the axiom of choice). In a second step, if we assume $\Gamma \models \varphi$ and that $\Gamma \cup \{\neg\varphi\}$ is syntactically coherent, then by the above model property, there would exist a structure $\mathcal{A}$ in which $\mathcal{A} \models \Gamma \cup \{\neg\varphi\}$, which is impossible by assumption. Hence $\Gamma \cup \{\neg\varphi\} \vdash_{\mathsf{NK}} \bot$, which leads to $\Gamma \vdash_{\mathsf{NK}} \varphi$ (by the rule $\bot_{\mathtt{classic}}$).

4.2 Kripke structures

Our aim here is to define a notion of structure and a notion of validity in such a structure, in such a way that a formula is provable in NJ (or LJ) iff it is valid. Note that, for somebody *thinking* in an intuitionistic way, it is already the case that truth is preserved by the rules of NJ but not by those of NK. But we write this course from a classical point of view: our metatheory is *classical* set theory and we would like to understand nevertheless intuitionistic reasoning, in a semantic fashion. This aim will be reached through the notion of *Kripke structure* that will play for intuitionistic proofs (i.e in NJ or LJ) the role that (classical) structures play for classical proofs (i.e in NK or LK).

Order 0 Kripke structures We treat first the restricted case of propositional logics. We call a signature propositional when it posesses no function symbol and only predicate symbols of arity 0.

Definition 4.2.1 *A propositional Kripke structure for the (propositional) signature $\mathcal{R} = \langle R_1, R_2, \ldots, R_n\rangle$ is a triple*

$$\mathcal{K} := (K, \leq, \mid\!\!\vdash_0)$$

such that, $(K, \leq)$ is a (partially) ordered set and $\mid\!\!\vdash_0 \subseteq K \times \{R_1, R_2, \ldots, R_n\}$ is a binary relation fulfilling:

$$\forall k, \ell \in K, \forall R \in \mathcal{R}, (k \leq \ell \quad \textit{and} \quad k \mid\!\!\vdash_0 R) \Rightarrow (\ell \mid\!\!\vdash_0 R).$$

The elements of K are called the nodes of the Kripke structure.

Definition 4.2.2 *The binary relation $\mid\!\!\vdash$ is the smallest binary relation which is included in $K \times \mathcal{L}_0(\mathcal{R})$, which contains $\mid\!\!\vdash_0$ and which fulfills the four clauses: for every $k \in K$*
KR1 $k \mid\!\!\vdash A \wedge B$ *iff* ($k \mid\!\!\vdash A$ *and* $k \mid\!\!\vdash B$)
KR2 $k \mid\!\!\vdash A \vee B$ *iff* ($k \mid\!\!\vdash A$ *or* $k \mid\!\!\vdash B$)
KR3 $k \mid\!\!\vdash A \to B$ *iff (for every* $k' \geq k$, *if* $k' \mid\!\!\vdash A$ *then* $k' \mid\!\!\vdash B$)
KR4 $k \mid\!\!\vdash \bot$ *is false.*

The connector $\neg$ is considered here as an abreviation:

$$\neg A := A \to \bot.$$

The expression "$k \,|\!\!\vdash R$"reads as "k forces R". The restricted relation $|\!\!\vdash_0$ is the initial forcing relation while $|\!\!\vdash$ (which is defined, inductively, above), is the forcing relation.

Remark 4.2.3

$$\begin{aligned} k \,|\!\!\vdash \neg A &\Leftrightarrow k \,|\!\!\vdash A \to \bot \\ &\Leftrightarrow \forall k' \geq k (k' \,|\!\!\vdash A \Rightarrow k' \,|\!\!\vdash \bot) \\ &\Leftrightarrow \forall k' \geq k, k' \not|\!\!\vdash A \end{aligned}$$

$$\begin{aligned} k \,|\!\!\vdash \neg\neg A &\Leftrightarrow k \,|\!\!\vdash (A \to \bot) \to \bot \\ &\Leftrightarrow \forall k' \geq k (k' \,|\!\!\vdash (A \to \bot) \Rightarrow k' \,|\!\!\vdash \bot) \\ &\Leftrightarrow \forall k' \geq k, \neg(k' \,|\!\!\vdash (A \to \bot)) \\ &\Leftrightarrow \forall k' \geq k, \neg(\forall k'' \geq k', \neg(k'' \,|\!\!\vdash A)) \\ &\Leftrightarrow \forall k' \geq k, \exists k'' \geq k', k'' \,|\!\!\vdash A. \end{aligned}$$

Note that we use, in our proofs (i.e. meta-arguments), the usual properties of negation in classical logics. This is no more contradictory than writing, in french, a grammar for the english language. This is a convenient way of defining intuitionistic semantics for readers who think in a classical way (as well would the above grammar fill the needs of a native french reader).

When $\mathrm{Card}(K) = 1$, the map $\nu : \mathcal{L}_0(\mathcal{R}) \to \{0, 1\}$ defined by

$$\nu(R) = 1 \Leftrightarrow k \,|\!\!\vdash R.$$

is a valuation (in the classical sense of Definition 4.1.1). Hence we cannot hope some new notion of semantics getting out of Kripke structures with one node. Let us give an example with three nodes.

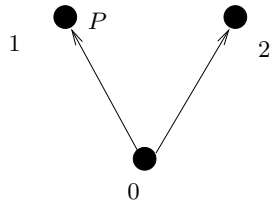

Figure 4.1: Kripke structure for example 4.2.4.

Example 4.2.4 *Let us consider a propositional signature with one propositional symbol P. We define a Kripke structure by:*

$$K := \{0, 1, 2\}, \quad 0 \leq 1, 0 \leq 2 \ ; \quad |\!\vdash_0 := \{(1, P)\}$$

Using the inductuve definition of the forcing relation we get successively:

$$1 \,|\!\vdash P, \quad 2 \,|\!\not\vdash P, \quad 2 \,|\!\vdash \neg P$$

(Note that, for a maximal node k, the formulas that are forced at k are exactly the classical consequences of the set $\{\varphi \mid k \,|\!\vdash_0 \varphi\}$).

$$0 \,|\!\not\vdash \neg\neg P, \quad 0 \,|\!\not\vdash \neg P$$

$$0 \,|\!\not\vdash \neg P \vee \neg\neg P$$

On figure 4.1 we represent the nodes by dark disks and the edges of the Hasse-diagram of the order by arrows. The names of the nodes are given below each node and the initial forcing is given by the letters on the sides of the nodes.

Example 4.2.5 *Let us consider a propositional signature with one propositional symbol P. We define a Kripke structure by:*

$$K := \{0, 1, 2, 3, 4\}$$

The ordering is the transitive closure of the set

$$\{(0, 1), (0, 4), (1, 2), (1, 3), (4, 3)\}$$

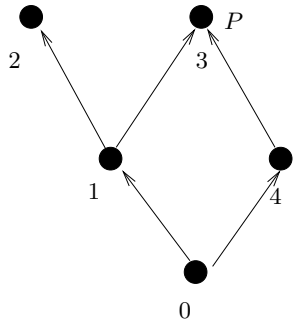

Figure 4.2: Kripke structure for example 4.2.5.

and

$$||\!\vdash_0 := \{(3, P)\}$$

(see figure 4.2). Using the inductive definition of the forcing relation we get successively:

$$3 \,||\!\vdash P \text{ hence } 0 \,||\!\not\vdash \neg P$$

$$2 \,||\!\vdash \neg P \text{ hence } 0 \,||\!\not\vdash \neg\neg P$$

$$4 \,||\!\vdash \neg\neg P \text{and } 4 \,||\!\not\vdash P, \text{ hence } 0 \,||\!\not\vdash (\neg\neg P \to P)$$

It follows that

$$0 \,||\!\not\vdash (\neg P) \vee (\neg\neg P) \vee (\neg\neg P \to P)$$

Lemma 4.2.6 *For every formula $\varphi \in \mathcal{L}_0(\mathcal{R})$ and every nodes $k, k' \in K$,*

$$(k \leq k' \text{ and } k \,||\!\vdash \varphi) \Rightarrow k' \,||\!\vdash \varphi.$$

This can be proved by structural induction.

Definition 4.2.7
1- A formula $\varphi \in \mathcal{L}_0(\mathcal{R})$ is valid *at node k, in the Kripke structure $\mathcal{K}$ iff $k \,||\!\vdash \varphi$.*

2- $\mathcal{K} \,|\!\vdash \varphi$ *means that* $\forall k \in K, k \,|\!\vdash \varphi$
Given a set $\Gamma \subseteq \mathcal{L}_0(\mathcal{R})$,
3- $\Gamma \,|\!\vdash \varphi$ *means that,* $\forall \mathcal{K}, \forall k \in K, [(\forall \psi \in \Gamma, k \,|\!\vdash \psi) \Rightarrow k \,|\!\vdash \varphi]$
4- $|\!\vdash \varphi$ *means that,* $\forall \mathcal{K}, \forall k \in K, k \,|\!\vdash \varphi$

Note that $|\!\vdash \varphi$ has the same meaning as $\emptyset \,|\!\vdash \varphi$ (as expected). One reads this expressions as "φ is Kripke-valid".

Theorem 4.2.8 (accuracy of NJ, propositional fragment) *Let* $\Gamma \subseteq \mathcal{L}_0(\mathcal{R}), \varphi \in \mathcal{L}_0(\mathcal{R})$. *Then*

$$\Gamma \vdash_{\mathsf{NJ}} \varphi \quad \Leftrightarrow \quad \Gamma \,|\!\vdash \varphi.$$

It is easy to check that every rule of NJ has the property that, if its upper sequents are Kripke-valid, then its lower sequent is also Kripke-valid. Hence it is clear that $\Gamma \vdash_{\mathsf{NJ}} \varphi \;\Rightarrow\; \Gamma \,|\!\vdash \varphi$. The converse is not easy: it is called the Kripke-completeness of NJ.

Order 1 **Kripke structures** We treat now the general case of order 1 i.e. define a notion of Kripke structure and a notion of forcing, that make sense for all first order formulas over *any* first-order signature.

Definition 4.2.9 *Let* $\mathcal{S} = \langle R_1, R_2, \ldots, R_n; f_1, \ldots, f_m \rangle$ *be a signature with arities* $\langle r_1, r_2, \ldots, r_n; a_1, a_2, \ldots, a_m \rangle$ *and* C *a set of constants (this last set* C *can be infinite, just as it is the case for classical structures). A Kripke structure over* $\mathcal{S}, C$ *is a 4-tuple*

$$\mathcal{K} := (K, \leq, \{(D(k), (f_{j,k})_{1 \leq j \leq m}, (c_k)_{c \in C}) \mid k \in K\}, \,|\!\vdash_0)$$

such that:
$(K, \leq)$ *is a (partially) ordered set*
$\forall k \in K, D(k) \neq \emptyset$
$\forall k \in K, f_{j,k} : D(k)^{a_j} \to D(k),\ c_k \in D(k)$
$\forall k, \ell \in K, k \leq \ell \Rightarrow D(k) \subseteq D(\ell)$
$\forall k, \ell \in K, k \leq \ell \Rightarrow c_k = c_\ell$

$\forall k, \ell \in K \forall j \in [1, m], k \leq \ell \Rightarrow f_{j,k} \subseteq f_{j,\ell}$
$\overline{|\!\!\vdash\!\!\!-_0} \subseteq \{(k, \varphi) \mid k \in K, \varphi$ `closed atomic formula with constants in` $C \cup \overline{D(k)}\}$
$\forall k, \ell \in K, \forall \varphi, (k \leq \ell \quad and \quad k \,|\!\!\vdash\!\!\!-_0 \varphi) \Rightarrow (\ell \,|\!\!\vdash\!\!\!-_0 R)$.

The forcing relation $|\!\!\vdash\!\!\!-_0$ is extended to non-atomic formulas by the following definition.

Definition 4.2.10 *The binary relation* $\overline{|\!\!\vdash\!\!\!-}$ *is the smallest binary relation which is included in* $\bigcup_{k \in K} \{k\} \times \mathcal{L}_1(\mathcal{S}, C \cup \overline{D(k)})$ *, which contains* $|\!\!\vdash\!\!\!-_0$ *and which fulfills the six clauses: for every* $k \in K$
KR1 $k \,|\!\!\vdash\!\!\!- A \wedge B$ *iff* $(k \,|\!\!\vdash\!\!\!- A$ *and* $k \,|\!\!\vdash\!\!\!- B)$
KR2 $k \,|\!\!\vdash\!\!\!- A \vee B$ *iff* $(k \,|\!\!\vdash\!\!\!- A$ *or* $k \,|\!\!\vdash\!\!\!- B)$
KR3 $k \,|\!\!\vdash\!\!\!- A \to B$ *iff (for every* $k' \geq k$*, if* $k' \,|\!\!\vdash\!\!\!- A$ *then* $k' \,|\!\!\vdash\!\!\!- B)$
KR4 $k \,|\!\!\vdash\!\!\!- \bot$ *is false*
KR5 $k \,|\!\!\vdash\!\!\!- \forall v$ *A iff (for every* $k' \geq k$*, for every* $d \in D(k'), k' \,|\!\!\vdash\!\!\!- A[v := \bar{d}])$
KR6 $k \,|\!\!\vdash\!\!\!- \exists v$ *A iff (there exists some* $d \in D(k), k \,|\!\!\vdash\!\!\!- A[v := \bar{d}])$

Lemma 4.2.11 *For every* $k, \ell \in K$ *and every formula* $\varphi \in \mathcal{L}_1(\mathcal{S} \cup C \cup \{\bar{d} \mid d \in D(k)\})$

$$(k \leq k' \text{ and } k \,|\!\!\vdash\!\!\!- \varphi) \Rightarrow k' \,|\!\!\vdash\!\!\!- \varphi.$$

This can be proved by structural induction.

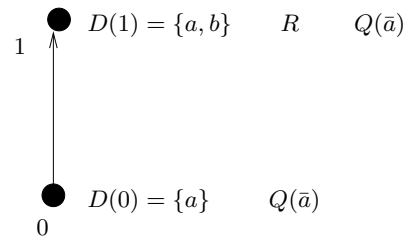

Figure 4.3: Kripke structure for example 4.2.12.

Example 4.2.12 *Let us consider a signature with one propositional symbol R and a one-place predicate symbol Q (and no function symbol nor constant symbol). We define a Kripke structure by:*

$$K := \{0,1\},\ \ 0 \leq 1\ \ ; D(0) := \{a\}, D(1) := \{a,b\}\ \ \ |\!\!\vdash_0 := \{(0, Q(\bar{a})), (1,R), (1, Q(\bar{a}))\}$$

Using the inductive definition of the forcing relation we get successively:

$$0 \,|\!\!\vdash Q(\bar{a})\ \ \texttt{hence}\ 0 \,|\!\!\vdash R \vee Q(\bar{a})$$

$$1 \,|\!\!\vdash Q(\bar{a})\ \ \texttt{hence}\ 1 \,|\!\!\vdash R \vee Q(\bar{a})$$

$$1 \,|\!\!\vdash R\ \ \texttt{hence}\ 1 \,|\!\!\vdash R \vee Q(\bar{b})$$

It follows that

$$0 \,|\!\!\vdash \forall x\ \ (R \vee Q(x)) \tag{4.1}$$

$$0 |\!\!\not\vdash R,\ \ 1 |\!\!\not\vdash Q(\bar{b}),\ \ 0 |\!\!\not\vdash \forall x\ \ Q(x)$$

It follows that

$$0 |\!\!\not\vdash R \vee \forall x\ \ Q(x) \tag{4.2}$$

(meta)-assertions (4.1)(4.2) show that

$$0 |\!\!\not\vdash [\forall x\ \ (R \vee Q(x))] \rightarrow [R \vee \forall x\ \ Q(x)]$$

Example 4.2.13 *Let us consider a signature with one one-place predicate symbol R (and no function symbol nor constant symbol). We define a Kripke structure by:*

$$\begin{array}{rcl} K & := & \{k_n \mid n \in \mathbb{N}\},\ \ k_0 \leq k_1 \leq \ldots \leq k_n \leq k_{n+1} \leq \ldots, \\ & & D(k_0) := \{0\}, \ldots D(k_n) := [0,n],\ \ \ |\!\!\vdash_0 := \{(k_n, R(\bar{m})) \mid 0 \leq m \leq n-1\} \end{array}$$

Let us examine whether :

$$k_0 \,|\!\!\vdash \neg\neg\forall x(R(x) \vee \neg R(x))? \tag{4.3}$$

Using the inductive definition of the forcing relation as well as the rules of classical logics (in our meta-proof) we get:

$$\begin{array}{rcl} (4.3) & \Leftrightarrow & \forall k, k \,|\!\!\not\vdash \neg\forall x(R(x) \vee \neg R(x)) \\ & \Leftrightarrow & \forall k, \exists k' \geq k, k' \,|\!\!\vdash \forall x(R(x) \vee \neg R(x)) \\ & \Leftrightarrow & \forall k, \exists k' \geq k, \forall k'' \geq k', \forall d \in D(k''), k'' \,|\!\!\vdash \forall(R(\bar{d}) \vee \neg R(\bar{d})) \end{array} \tag{4.4}$$

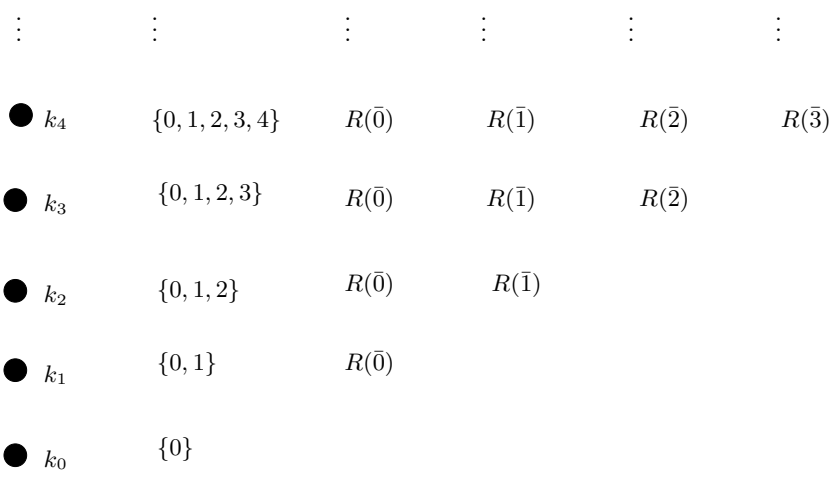

Figure 4.4: Kripke structure for example 4.2.13.

But $k_i \,|\!\not\vdash R(\overline{i+1})$ *and* $k_i \,|\!\not\vdash \neg R(\overline{i+1})$*, hence*

$$\forall k, k \,|\!\not\vdash R(\overline{i+1}) \vee \neg R(\overline{i+1})$$

which shows that property (4.4) is false. We conclude that

$$k_0 \,|\!\not\vdash \neg\neg\forall x(R(x) \vee \neg R(x)).$$

Theorem 4.2.14 (accuracy of NJ) *Let* $\Gamma \subseteq \mathcal{L}_1(\mathcal{S}), \varphi \in \mathcal{L}_1(\mathcal{S})$*. Then*

$$\Gamma \vdash_{\mathsf{NJ}} \varphi \;\Leftrightarrow\; \Gamma \,|\!\vdash \varphi.$$

Here again the implication

$$\Gamma \vdash_{\mathsf{NJ}} \varphi \;\Rightarrow\; \Gamma \,|\!\vdash \varphi.$$

just asserts that every provable statement (in an intuitionistic sense) is "true" (in the sense of Kripke interpretations). It is called the Kripke-*soundness* property of NJ. The proof consists in checking that every rule of

NJ preserves Kripke-truth.
The implication

$$\Gamma \vdash_{\mathsf{NJ}} \varphi \quad \Leftarrow \quad \Gamma \mid\!\vdash \varphi,$$

is the Kripke-*completeness* property: it asserts that a sequent which is Kripke-valid is also provable within NJ.

Chapter 5

Some decidable theories

Let us call *theory* a set of formulas (over a given signature) which is closed under logical deduction i.e. every application of a rule from LK (or NK) leads to a formula that already belongs to the theory (up to some translation when the judgments of the system are not merely formulas). Of particular interest are the following kinds of theory:
1- Axiomatic theories: i.e. given a set Γ of formulas, the set

$$\{\Phi \mid \Gamma \vdash_{\mathrm{LK}} \Phi\}$$

2- Theories of structures: i.e. given a particular structure $\mathcal{M}$ over the signature $\mathcal{S}$, the set

$$\{\Phi \mid \mathcal{M} \models \Phi\}.$$

In both cases we would like to know if there is some algorithm allowing to decide whether a formula belongs (or not) to the theory. When such an algorithm exists, we say that the theory is *decidable*.
We show here that some structures with domain the set of natural integers, have decidable first-order theory.

5.1 Integers with addition

Let us consider the structure

$$\mathcal{M} := \langle \mathbb{N}; =; + \rangle$$

i.e. the set of natural integers endowed with the equality predicate and the addition. The first-order theory of this structure is nowadays called *Presburger arithmetics* since its decidability was proved by M. Presburger in 1929. Several methods can be used to this aim.

Method 1:The original method used by Presburger consisted in producing a set of axioms Γ which is recursively enumerable and such that a formula Φ is valid in $\mathcal{M}$ if and only if $\Gamma \vdash_{\mathrm{LK}} \Phi$. In other words Presburger found a *complete r.e. axiomatisation* of the first-order theory of $\langle \mathbb{N}; =; + \rangle$. The decision procedure is the following: given a closed formula Φ, enumerate all the proofs of sequents of the form $\Gamma' \vdash A$ for finite subsets Γ' of Γ. This enumeration must either reach a sequent of the form

$$\Gamma' \vdash_{\mathrm{LK}} \Phi$$

and in this case we conclude that $\mathcal{M} \models \Phi$, or reach a sequent of the form

$$\Gamma' \vdash_{\mathrm{LK}} \neg\Phi$$

and in this case we conclude that $\mathcal{M} \not\models \Phi$.

Method 2: A second method, used for example by [Cooper, 1972], consists in finding a *quantifier elimination* procedure i.e. an algorithm which, given a formula of the form $\exists x F(x, \vec{y})$, produces a formula $G(\vec{y})$ which is semantically equivalent with $\exists x F(x, \vec{y})$ over $\mathcal{A}$ i.e.

$$\langle \mathbb{N}; =; + \rangle \models [\exists x F(x, \vec{y})] \leftrightarrow G(\vec{y})$$

Method 3: A third method, which originates in Büchi's works ([Büc60]) and was finally completely established in [Bru85], consists in reducing the statement

$$\langle \mathbb{N}; =; + \rangle \models \Phi$$

to a statement of the form

$$\mathrm{L}(\mathcal{A}) = \emptyset$$

for some finite automaton $\mathcal{A}$. The core of the algorithm is the *construction of the automaton* $\mathcal{A}$ from the formula Φ.

We detail in this chapter the method 3. In the course of the proof, we shall realize that this method indeed decides an extended structure (based on

$\mathbb{N}$, see (5.1)) and also allows a *characterisation* of the properties which are definable by some first-order formula in terms of finite automata.

Let us fix some integer $k \geq 2$ that will serve us as base for expressing integers by words. We note

$$\Sigma_k := \{0, 1, \ldots, k-1\}$$

the alphabet of digits in base k. Let

$$\nu : \Sigma_k^* \to \mathbb{N}$$

the map defined by

$$\nu(w) = \sum_{j=0}^{\ell-1} w[j] \cdot k^j$$

where $\ell = |w|$ and $w = w[\ell-1] \cdots w[0]$. More generally

$$\nu : (\Sigma_k^m)^* \to \mathbb{N}^m$$

is defined by

$$w = (w_1, \ldots, w_m) \mapsto (\nu(w_1), \ldots, \nu(w_m))$$

Example 5.1.1

$$k = 2, m = 3, w = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\nu(w) = \begin{pmatrix} \nu(0010) \\ \nu(1010) \\ \nu(0101) \end{pmatrix} = \begin{pmatrix} 2 \\ 10 \\ 5 \end{pmatrix}$$

For sake of saving space we shall rather note the vectors (whether in $(\Sigma_k^m)^*$ or in $\mathbb{N}^m$) as line-vectors. Here we can note:

$$w = (0010, 1010, 0101), \quad \nu(w) = (\nu(0010), \nu(1010), \nu(0101)) = (2, 10, 5).$$

Let us introduce an additional binary predicate V_k defined by:

$$V_k(x, y) = 1 \Leftrightarrow [y = \max\{k^e \mid k^e \text{ divides } x\} \wedge x \geq 1] \vee [y = 1 \wedge x = 0]$$

Example 5.1.2

$V_2(5,1) = 1,\ \ V_2(10,2) = 1,\ \ V_2(0,1) = 1,\ \ V_2(24,8) = 1,\ \ V_2(24,16) = 0,\ \ V_2(24,4) = 0.$

We focus now on the extended structure

$$\langle \mathbb{N}; =, V_k; + \rangle \tag{5.1}$$

Definition 5.1.3 *Let $\Phi \in \mathcal{L}_1(=, V_k, +), m \geq 0$ and $\vec{x} = (x_1, x_2, \ldots, x_m) \in \mathcal{V}^m$ such that $i < j \Rightarrow x_i \neq x_j$ (i.e. the m variables are m distinct symbols). Then*

$$M_{\Phi,\vec{x}} := \{(n_1, \ldots, n_m) \in \mathbb{N}^m \mid \langle \mathbb{N}; =, V_k; + \rangle \models \Phi(n_1, \ldots, n_m)\}$$

In words: $M_{\Phi,\vec{x}}$ is the *set of models* of the formula Φ i.e. the set of vectors of values that, when substituted to the vector of variables $\vec{x}$, make the formula true in the structure $\langle \mathbb{N}; =, V_k; + \rangle$. We used the abreviation $\Phi(n_1, \ldots, n_m)$ for $\Phi[x_1 := \bar{n_1}, \ldots, x_m := \bar{n_m}]$.
Let us remark that:
- if x_j is not a free variable of Φ, then the value of n_j has no influence on the fact that $\vec{n} \in M_{\Phi,\vec{x}}$
- some variable v might occur freely in Φ but not belong to the set $\{x_1, \ldots, x_m\}$; one can check that, in this case, the set $M_{\Phi,\vec{x}}$ is equal to $M_{\forall v\, \Phi,\vec{x}}$
- when $m = 0$, either the formula is valid and $M_{\Phi,\vec{x}} = \{\emptyset\}$ or the formula is not valid and $M_{\Phi,\vec{x}} = \emptyset$. [1].

Definition 5.1.4 *Let $M \subseteq \mathbb{N}^m$.*
1- The subset M is called k-recognizble iff $\nu^{-1}(M)$ is a recognizable subset of $(\Sigma_k^m)^*$.
2- The subset M is called k-definable iff there exists some formula $\Phi \in \mathcal{L}_1(=, V_k, +)$ such that $M = M_{\Phi,(x_1,\ldots,x_m)}$.

[1] yes, this is somewhat disturbing, but it is not a typo, just a technical detail

Theorem 5.1.5 *Let $M \subseteq \mathbb{N}^m$. If M is k-definable then M is k-recognizable.*

Proof: We remark first that every formula Φ can be transformed into an equivalent formula where the atomic subformulas have one of the two forms:

$$x_1 = x_2,$$

where x_1, x_2 are distinct variables, or

$$x_1 + x_2 = x_3$$

where x_1, x_2, x_3 are three distinct variables.
We show, by induction over the size (i.e. number of operators) of Φ, that, for every vector $\vec{x}$ of distinct variables, the set $\nu^{-1}(M_{\Phi,\vec{x}})$ is recognized by some finite automaton $\mathbb{A}_{\Phi,\vec{x}}$. The automata that we manipulate here are deterministic, complete and read from right-to-left.
Augmentation of the vector: $\vec{x} = (x_0, y_1, \ldots, y_m)$
Let $\mathbb{A}_{\Phi,\vec{y}}$ be a f.a. such that

$$\mathrm{L}(\mathbb{A}) = \nu^{-1}(M_{\Phi,\vec{y}}).$$

Let $h : (\Sigma_k^{m+1})^* \to (\Sigma_k^m)^*$ the monoid-homomorphism defined by

$$(w_0, w_1, \ldots, w_m) \mapsto (w_1, \ldots, w_m)$$

i.e. the projection onto the m last components. We claim that

$$\nu^{-1}(M_{\Phi,(x_0,\vec{y})}) = h^{-1}(\nu^{-1}(M_{\Phi,\vec{y}})).$$

It is known that the operation h^{-1} (for an homomorphism h) preserves recognizability.
Atomic formula: equality: $\Phi : x_1 = x_2$.
If one of the variables x_1, x_2 does not occur in $\vec{x}$, then $M_{\Phi,\vec{x}} = \emptyset$.
If $\vec{x} = (x_1, x_2)$, then

$$M_{\Phi,\vec{x}} = E^*,$$

where $E = \{(d_1, d_2) \in \Sigma_k^2 \mid d_1 = d_2\}$ This set is clearly rational, hence recognizable.
If $\vec{x}$ is some vector of length $m \geq 2$ of distinct variables, where x_1, x_2 both occur, then by the above case $M_{\Phi,(x_1,x_2)}$ is recognizable and by closure by augmentation of the vector, $M_{\Phi,\vec{x}}$ is recognizable too.

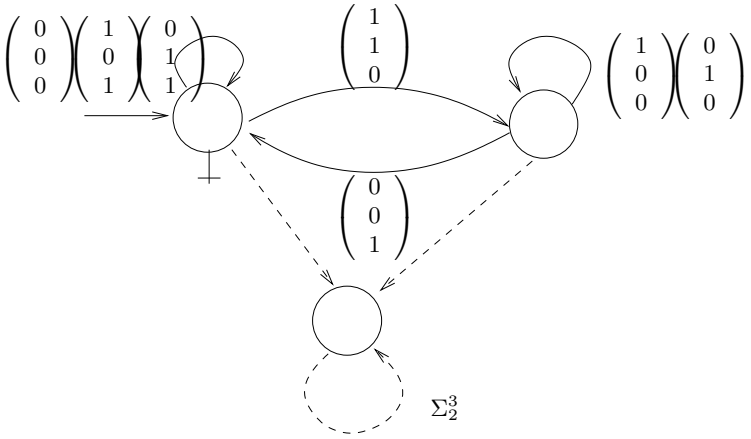

Figure 5.1: The addition automaton.

Atomic formula: addition: $\Phi : x_1 + x_2 = x_3, \vec{x} = (x_1, x_2, x_3)$
For sake of simplicity, let us show this for $k = 2$. The set $M_{\Phi,\vec{x}}$ is recognized (from right-to-left) by the f.a. of figure 5.1. The principle of this automaton is that it computes the sum, bit by bit, from right-to-left (as we nowadays learn to do at elementary school) and memorizes the carry in its state.
Atomic formula: valuation: $\Phi : V_k(x_1, x_2), \vec{x} = (x_1, x_2)$
For sake of simplicity, let us show this for $k = 2$. The set $M_{\Phi,\vec{x}}$ is recognized (from right-to-left) by the f.a. of figure 5.2.
Disjunction: $\Phi = \Psi \vee \Theta$
Let $\vec{x}$ be some vector of distinct variables. By induction hypothesis $M_{\Psi,\vec{x}}, M_{\Theta,\vec{x}}$ are both recognizable. But $M_{\Phi,\vec{x}} = M_{\Psi,\vec{x}} \cup M_{\Theta,\vec{x}}$, hence is recognizable too.
Conjunction: $\Phi = \Psi \wedge \Theta$
It is known that the set of recognizable languages is closed under intersection. Since $M_{\Phi,\vec{x}} = M_{\Psi,\vec{x}} \cap M_{\Theta,\vec{x}}$, we can conclude from the induction hypothesis that $M_{\Phi,\vec{x}}$ is recognizable.
Negation: $\Phi = \neg\Psi$
We remark that

$$M_{\neg\Psi,\vec{x}} = (\Sigma_k^m)^* \setminus M_{\Psi,\vec{x}}$$

Since recognizable sets are closed under complement, $M_{\neg\Psi,\vec{x}}$ is recognizable.
Existential quantifier: $\Phi = \exists x_0\ \Psi, \vec{x} = (x_1, \ldots, x_m)$
One can check that

$$M_{\exists x_0\ \Psi,\vec{x}} = (\mathrm{O}_m^*)^{-1} h(M_{\Psi,\vec{x}})$$

where $h : (\Sigma_k^{m+1})^* \to (\Sigma_k^m)^*$ is the projection onto the m last components,

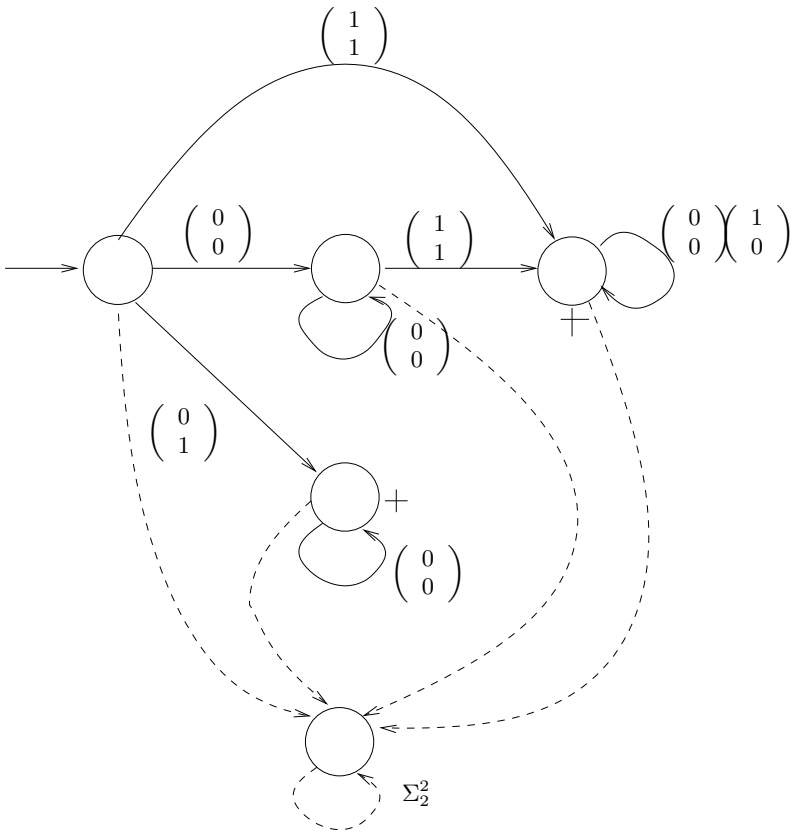

Figure 5.2: The valuation automaton.

O_m is the letter of Σ_k^m having only null components and the exponent -1 designates a left-residual. Since the set of rational subsets of a free monoid is closed under direct homomorphism and left-residuals, we deduce from the induction hypothesis that $M_{\exists x_0\ \Psi,\vec{x}}$ is rational, hence recognizable.

Universal quantifier: $\Phi = \forall x_0\ \Psi, \vec{x} = (x_1, \ldots, x_m)$

Let us remark that

$$\forall x_0\ \Psi \models\!\models \neg\exists x_0\ \neg\Psi$$

hence

$$M_{\forall x_0\ \Psi,\vec{x}} = M_{\neg\exists x_0\ \neg\Psi,\vec{x}}.$$

By induction hypothesis $M_{\Psi,\vec{x}}$ is recognizable. Applying then the arguments used for negation, for the existential quantifier, and for negation, we obtain that $M_{\forall x_0\ \Psi,\vec{x}}$ is recognizable.

□

Note that, at each step of this proof by induction, one can convert our closure arguments into *effective constructions* of some finite automaton, from the f.a. that are provided by the induction hypothesis. Thus it can be turned into an algorithm constructing the automaton $\mathbb{A}_{\Phi,\vec{x}}$ from the formula Φ and the vector $\vec{x}$.

Let us go back to our initial problem which was to find a decision procedure for the problem (slightly generalised by considering the structure (5.1)):

Instance: a first-order formula Φ over the signature $\langle =, V_k; + \rangle$
Question: is this formula valid in the structure $\langle \mathbb{N}; =, V_k; + \rangle$?

The following algorithm solves this problem:
- compute some f.a. $\mathbb{A}$ recognizing the language $M_{\Phi,\emptyset}$
- test whether $\mathrm{L}(M_{\Phi,\emptyset}) = \{\emptyset\}$?
- if yes then Φ is valid, otherwise, Φ is not valid.

We shall now delineate more precisely the links between definability and recognizability.

Theorem 5.1.6 (Büchi-Bruyère, 1985) *Let $M \subseteq \mathbb{N}^m$. The subset M is k-definable if and only if it is k-recognizable.*

We already know that every definable subset is k-recognizable. In order to prove the converse, our general strategy will consist in expressing computations of a given f.a. by formulas. To this aim we introduce new predicates and function symbols and show that they are expressible in $\mathcal{L}_1(=, V_k, +)$.
We define a predicate $P_k(*)$ by:

$$P_k(x) := \exists e \in \mathbb{N}, x = k^e.$$

We define a predicate $\in_{j,k}(*,*)$, for every $j \in [0, k-1]$ by: $\in_{j,k}(x,y) = 1$ if and only if

$$P_k(y) \text{ and } \exists b_0, \ldots, b_\ell \in [0, k-1], \exists e \in [0, \ell], x = b_\ell k^\ell + \ldots + j k^e + \ldots + b_0 k^0, \;\; y = k^e.$$

In words:$\in_{j,k}(x,y)$ means that j is a digit of the expression of x in base k and y is the "corresponding" power of k.

Example 5.1.7 *For $x = 20$, one of its expressions in base $k = 2$ is $w =$ 0010100. We can check, by reading the word w from right to left, that*

$$\in_{0,2}(20,1), \in_{0,2}(20,2), \in_{1,2}(20,4), \in_{0,2}(20,8), \in_{1,2}(20,16), \in_{0,2}(20,32), \in_{0,2}(20,64).$$

We can also see that, for every $e \geq 5$, $\in_{0,2}(20, 2^e)$ holds.

We define a predicate $\lambda_k(*)$ by:

$$\begin{array}{ll} \lambda_k(x) := & \max\{y \mid P_k(y) \text{ and } y \leq x\} \quad \text{if } x \geq 1 \\ \lambda_k(0) := & 1 \end{array}$$

$$\lambda_k(x_1, \ldots, x_m) := \max\{\lambda_k(x_1), \ldots, \lambda_k(x_m)\}$$

Example 5.1.8

$$\lambda_2(3) = 2, \lambda_2(20) = 16, \lambda_2(82) = 64, \lambda_2(20, 3, 82) = 64.$$

Lemma 5.1.9 *The predicates P_k,$\in_{j,k}$ and the function λ_k are expressible by formulas in $\mathcal{L}_1(=, V_k, +)$.*

Proof: Using the abbreviations:

$$x \leq y \ : \ \exists z \ \ x + y = z$$

$$x < y \ : \ x \leq y \wedge \neg x = y$$

$$y = \max\{x_1, \ldots, x_m\} \ : \ (\bigwedge_{j=1}^{m} x_j \leq y) \wedge (\bigvee_{j=1}^{m} y = x_j)$$

we can express the new predicates or function as follows:

$$\begin{array}{rcl} P_k(x) & : & V_k(x,x) \\ y = \lambda_k(x) & : & [x = 0 \wedge y = 1] \vee [(P_k(y) \wedge y \leq x) \wedge \forall z \ \ ((P_k(z) \wedge z \leq x) \rightarrow z \leq y)] \\ y = \lambda_k(\vec{x}) & : & y = \max(\lambda_k(x_1), \ldots, \lambda_k(x_m) \\ \in_{j,k}(x,y) & : & P_k(y) \wedge [\exists z \exists t \ \ (x = z + j \cdot y + t) \wedge (z < y) \wedge ((\forall u \ V_k(t,u) \rightarrow y < u) \vee t = 0)] \end{array}$$

□

We are now ready for a **proof of Theorem 5.1.6**.

Let $M \subseteq \mathbb{N}^m$ be some recognizable subset. Let $\mathbb{A} := \langle \Sigma_k^m, Q, q_0, Q^+, T \rangle$be a f.a. recognizing (from right-to-left) the language $\nu^{-1}(M)$. We assumer $\mathbb{A}$ is deterministic and complete. We note $Q = \{q_0, q_1, \ldots, q_p\}$. We construct a first-order formula Φ over the signature $\langle =, V_k, P_k, (\in_{j,k})_{0 \leq j \leq k-1}; +, \lambda_k \rangle$, with m free variables $x_1, x_2, \ldots, x_m$ expressing the fact that the computation of $\mathbb{A}$ over $\mu(\vec{x})$ is successful. [We designate by $\mu(\vec{x})$ the unique element of $\nu^{-1}(\vec{x})$ which begins by a letter with at least one non-null component]. Note that if $\ell = |\mu(\vec{x})|$ then $\lambda_k(\vec{x}) = 2^{\ell-1}$.

`A scheme of the computation`

The automaton enters successively the states $q(0), q(1), \ldots q(i) \ldots q(\ell)$ during its computation C over $\mu(\vec{x})$. We introduce numbers $y_0, \ldots, y_p$ such that, y_j is coding for the positions of states q_j in C:

$$y_j := \sum_{i=0}^{\ell} b_{i,j} k^j$$

where $b_{i,j} = 1 \Leftrightarrow q(i) = q_j$. The formula Φ should express the following properties:

$$\exists y_0 \ \exists y_1 \ldots \ \exists y_p$$

(these integers are coding the sequence $q(0), q(1), \ldots q(i) \ldots q(\ell)$)
such that:

`P1` : $\forall i \in [0, \ell], \exists! j \in [0, p], q(i) = q_j$

`P2` : $q(0) = q_0 \ \wedge \ q(\ell) \in Q^+$

`P3` : $\forall i \in [0, \ell - 1], \forall j \in [0, p], q(i) = q_j \rightarrow q(i+1) = T(q_j, \mu(\vec{x})[i])$

Every property Pα (for $\alpha \in [1, 3]$) is expressed by a formula Φ_α as follows:

$$\begin{aligned}
\Phi_1 \;:\; & \forall y\,[P_k(y) \wedge y \leq k \cdot \lambda_k(\vec{x})] \rightarrow \\
& [\bigvee_{j=0}^{p} \in_{1,k}(y_j, y) \wedge \bigwedge_{0 \leq j < j' \leq p} \in_{0,k}(y_j, y) \vee \in_{0,k}(y_{j'}, y)] \\
\Phi_2 \;:\; & \in_{1,k}(y_0, 2^0) \wedge \bigvee_{q_j \in Q^+} \in_{1,k}(y_j, k \cdot \lambda_k(\vec{x})) \\
\Phi_3 \;:\; & \forall y \bigwedge_{\substack{a \in \Sigma_k^m \\ 0 \leq j \leq p}} [P_k(y) \wedge y \leq \lambda_k(\vec{x}) \wedge \in_{1,k}(y_j, y) \wedge \in_{a,k}(\vec{x}, y)] \\
& \rightarrow [\in_{1,k}(y_{T(q_j,a)}, k \cdot y)]
\end{aligned}$$

where $\in_{(b_1,b_2,\ldots,b_m),k}((x_1, x_2, \ldots, x_m), y)$ means $\bigwedge_{1 \leq c \leq m} \in_{b_c,k}(x_c, y)$. Finally we define the formula Φ by:

$$\Phi := \exists y_0 \exists y_1 \ldots \exists y_p \;\; \Phi_1(\vec{x}, \vec{y}) \;\wedge\; \Phi_2(\vec{x}, \vec{y}) \;\wedge\; \Phi_3(\vec{x}, \vec{y}).$$

End of the proof of Theorem 5.1.6.

5.2 Integers with product

Bibliography

[AG93] A. Arnold and I. Guessarian. *Mathématiques pour l'informatique*. Masson, 1993.

[BHMV94] V. Bruyère, Hansel, Michaux, and Villemaire. Logic and p-recognizable sets of integers. *Bull. Belg. Math. Soc. 1*, pages 191–238, 1994.

[Bru85] V. Bruyère. Entiers et automates finis. *Mémoire de fin d'études, Université de Mons*, pages 191–238, 1985.

[Büc60] R. Büchi. Weak second-order arithmetic and finite automata. *Z. Math. Logik Grundlag. Math. 6*, pages 66–92, 1960.

[CL93] Cori and Lascar. *Logique Mathématique, tomes 1,2, cours et exercices*. Dunod, 1993.

[Dal80] Van Dalen. *Logic and structures*. Springer, 1980.

[DNR03] David, Nour, and Raffalli. *Introduction à la logique*. Dunod, 2003.

[Dow07] G. Dowek. *Les métamorphoses du calcul:une étonnante histoire de mathématiques*. Le Pommier, 2007.

[Gen35a] G. Gentzen. Untersuchungen über das logische Schliessen I. *Mathematische Zeitschrift-39*, pages 176–210, 1935. available from `http://www.digizeitschriften.de/dms/toc/?PPN=PPN266833020_0039`.

[Gen35b] G. Gentzen. Untersuchungen über das logische Schliessen II. *Mathematische Zeitschrift-39*, pages 405–431, 1935.

available from http://www.digizeitschriften.de/dms/toc/?PPN=PPN266833020_0039.

[Göd30] K. Gödel. Die vollständigkeit der axiome des logischen funktionenkalküls. *Monatshefte für Mathematik und Physik 37*, pages 349–360, 1930.

[GTW02] Grädel, Thomas, and Wilke. *Automata Logics and Infinite Games*. LNCS 2500, Springer, 2002.

[Gui78] M. Guillaume. Axiomatique et logique. In *Abrégé d'histoire des Mathématiques, chap. 11*, pages 417–483. Hermann, 1978.

[Hue86] G. Huet. *Inititation à la Logique Mathématique*. Notes de Cours du DEA d'Informatique, université Paris 9, 1986.

[Lal90] R. Lalement. *Logique, réduction, résolution*. Masson, 1990.

[Opp78] Oppen. A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic. *JCSS 16*, pages 323–332, 1978.

[Sén10] G. Sénizergues. Informatique théorique 2, 2010. Notes de cours de théorie des langages formels;http://dept-info.labri.u-bordeaux.fr/~ges/ENSEIGNEMENT/INFOT2/polycop_tdl.pdf.

[Tho97] W. Thomas. Languages, automata and logic. In *Handbook of language theory, Vol. 3, chap.7*, pages 389–455. Springer Verlag, 1997.