Introduction to Proof Theory

Abhishek De
&
Iris van der Giessen

Lecture notes for Midlands Graduate School 2024
Leicester, UK

School of Computer Science
University of Birmingham

Abstract

Proof theory is one of the major branches of logic that studies proofs as bona fide mathematical objects. It was born out of Hilbert's program for the foundations of mathematics but after a century of research has seen applications in mathematics (*proof mining, proof assistants*), computer science (*verification, programming language theory*), and linguistics (*formal natural language semantics*). The course is designed to give a taste of the intuitions and techniques bespoke to proof theory emphasising the structural side. The student will become familiar with the history of structural proof theory, sequent calculi, cut-elimination, and its application. The course is intended to be introductory, and no prior knowledge of the topic is expected.

If you find an inaccuracy of any kind, write to us at {a.de@bham.ac.uk, i.vandergiessen@bham.ac.uk}.

Acknowledgements

We are grateful to the organisers of MGS 2024 for giving us the opportunity to offer this course. We are indebted to Anupam Das and Sonia Marin for their constant support and encouragement. We thank Anupam Das and Raheleh Jalali for their helpful comments on the first draft of these notes.

We thank Tom de Jong for the template. The portrait of David Hilbert on the title page is by Matthew Leadbeater.

Contents

Abstract i

Acknowledgements ii

Contents iii

1 Introduction 1
- 1.1 History 1
- 1.2 Roadmap 3

2 The sequent calculus 4
- 2.1 Propositional logic 4
- 2.2 First-order logic 8

3 Properties of sequent calculus 14
- 3.1 Derivability 14
- 3.2 Admissibility 16

4 Applications of cut-elimination 20
- 4.1 Consistency and subformula property 20
- 4.2 Herbrand's theorem 21
- 4.3 Interpolation 24

5 Cut elimination 28
- 5.1 The need for a syntactic proof 28
- 5.2 Cut elimination as a rewriting system 29
- 5.3 The problem with structural rules 31
- 5.4 Putting everything together 33

A Additional background 38
- A.1 Capture-avoiding substitution 38
- A.2 First-order theories 39
- A.3 Rewriting theory 40

Bibliography 41

CHAPTER 1

Introduction

1.1 History

Proof theory has had a long history in philosophy and subsequently developed into a relatively new branch on the peripheries of mainstream mathematics.

Prehistory

In all ancient philosophical traditions such as the Greek, the Hindu, and the Buddhist, a major preoccupation was *epistemology* or the nature of gaining knowledge. Various methods of gaining knowledge are debated such as perception, guess, analogy, and *inference*. Aristotle is often credited with making the prototypical correct inference by concluding "All Greeks are mortal" from the premises "All men are mortal" and "All Greeks are men." Consequently, the notion of a *proof* as a series of inferences was formulated.

The Greek philosophers soon realised that allowing arbitrary principles or arbitrary steps in a proof trivialises the proof and the idea of *axiomatic systems* with carefully chosen basic principles and permissible steps was borne. The first axiomatic system, *Euclid's postulates* for geometry, satisfied this desideratum.

During the Islamic golden age, philosophers like Ibn Sina defined the quantification of predicates and developed a proto-temporal logic with modifiers such as "at all times", "at most times", and "at some time". However, proof theory did not take off on the mathematical side, since a proof was seen as a vehicle of thought, not an object of formal investigation.

The birth of modern proof theory

Proof theory *really* started in 1879, when Gottlob Frege introduced the first mathematical notation for proofs, which he called *Begrifftschrift* in German. Frege compared this ideography to a microscope which translates vernacular proofs exchanged between mathematicians into formal proofs which may be studied like any other mathematical object. Despite his extraordinary insight and formal creativity, Frege remained largely unnoticed by the mathematical community of his time.

Since Isaac Newton and Gottfried Leibniz invented calculus, the notion of an *infinitesimal* had been under attack for not being rigorous enough. About 200 years later, Frege's contemporaries like Augustin-Louis Cauchy, Karl Weierstrass, Georg Cantor, Richard Dedekind, and others finally formalised calculus rigorously with the (ε, δ) definition of limits and *set theory*. However, set theory opened a whole new can of worms. The entire foundation of mathematics was shaken by antinomies such as the *Burali-Forti paradox* (1897) and *Russell's paradox* (1901)! In this context of the foundational crisis, David Hilbert, Bertrand Russell and Alfred Whitehead sparked renewed interest in Frege's work.

In 1899, Hilbert provided a modern foundation of Euclidean geometry in his book *Grundlagen der Geometrie* by postulating twenty axioms that he proved to be consistent (*i.e.* without contradiction) and complete. Encouraged by this success, he planned to take on number theory next. Indeed, at the 1900 International Congress of Mathematics, Hilbert raised the purely proof-theoretic problem in his famous communication of twenty-three open problems: to show by purely finite combinatorial arguments that number theory is consistent.

Parallelly, the foundational crisis triggered another movement. In 1918, in his book *Das Kontinuum*, Hermann Weyl criticised set theory and analysis as "a house built on sand" and developed a system in which large portions of analysis can be carried out. This foundational position is called *predicativity*. In 1921, Weyl discovered the new foundational proposal that L.E.J Brouwer had meanwhile championed: *intuitionism*. This radical proposal urged the abandonment of the principle of the excluded middle for infinite totalities and of non-constructive mathematics, and thus most of infinitary mathematics. The costs to be paid were high: the intuitionistic reconstruction of mathematics had to sacrifice a great deal of classical mathematics. Hilbert rejected this revisionist approach to mathematics and his program was supposed to establish the foundations of mathematics in a way that even intuitionists would accept it.

However, Kurt Gödel established in 1931, with his incompleteness theorem that Hilbert's program was a hopeless dream: consistency of arithmetic cannot be established by purely arithmetical arguments.

Hilbert's dream was fruitful nonetheless: Gerhard Gentzen, a student of Hermann Weyl, established the consistency of arithmetic in 1936, by a purely combinatorial argument on the structure of proofs. This result seems to contradict Gödel's incompleteness theorem; however, Gentzen used in his argument a transfinite induction up to Cantor's ordinal ε_0 – and this part of the reasoning lies outside arithmetic.

Meanwhile, intuitionism acquired a more tangible form after Arendt Heyting's proposal for intuitionistic logic in 1930 and Andrei Kolmogorov's development of an axiomatic system that championed the idea that proofs are *effectively constructed*.

The foundational crisis is not as grave as it used to be in the early 20th century.

However, Gentzen's work on consistency and the idea of effective construction of proofs laid out by intuitionism led to the foundation of proof theory as a subject.

Recent trends

In modern proof theory, what matters today is not the consistency result in itself, but rather the method invented by Gentzen to establish this result. It is based on a formal innovation, the sequent calculus, and a fundamental discovery, the cut-elimination theorem. About a century of active research since Gentzen has seen proof theory mature into various directions:

- The study of various proof syntaxes such as sequent calculus, deep inference, combinatorial proofs, proof-nets, etc. is called *structural proof theory*. The goal is to obtain structural invariants to facilitate automated deduction, model checking, the study of complexity classes, and the identity of proofs.
- Gentzen's method of proving consistency gave a bound on the amount of transfinite induction used to prove consistency of arithmetic. The study of such bounds for various other theories is called *ordinal analysis*.
- One can carefully analyse the size of proofs. In particular, the study of lower bounds on the size of any proof of a theorem leads to interesting connections with complexity theory in the area of *proof complexity*.
- The idea of effectively constructing proofs (BHK interpretation) has been formalised into the *Curry-Howard isomorphism* and has led several advancements in *programming language theory*.
- Various other proof interpretations have been devised; for example, the Dialectica interpretation reduces classical theories to intuitionistic ones. This has found application in *proof mining* where seemingly non-constructive proofs are *mined* to obtain explicit bounds, ranges or rates of convergence.
- Finally, techniques from proof theory have been applied to determine exactly which axioms are required to prove everyday theorems of mathematics in a field called *reverse mathematics*.

1.2 Roadmap

These notes are supposed to serve as an introduction to structural proof theory. We will base it on Gentzen's sequent calculus and prove his cut elimination theorem. We have decided to treat classical logic for two reasons:

1. the semantics of classical logic based on truth values is easy to understand;
2. the structural concerns are the same for classical and intuitionistic logic.

The notes are organised as follows. The sequent calculus systems for classical propositional and first-order logic are introduced in Chapter 2. We discuss various properties of the sequent calculus such as derivability and admissibility in Chapter 3. One of the major results of proof theory is cut elimination. We first see some applications of the theorem in Chapter 4 and finally prove it Chapter 5. For the sake of readability, some finickity details are relegated to the appendix.

Chapter 2

The sequent calculus

2.1 Propositional logic

Fix a countable set of atomic propositions $\mathcal{A} = \{a, b, \dots\}$.

Definition 2.1. Propositional formulas (denoted $\varphi, \psi, \dots$) are given by the following grammar.

$$\varphi, \psi \quad ::= \quad \top \quad | \quad \bot \quad | \quad a \in \mathcal{A} \quad | \quad \neg\varphi \quad | \quad \varphi \vee \psi \quad | \quad \varphi \wedge \psi$$

The set of all formulas is denoted by Form.

Note that this is essentially an inductive definition of the set of formulas. We can unfold it to make it more explicit: Form is the smallest set such that

- $\top \in \mathsf{Form}$ and $\bot \in \mathsf{Form}$;
- For all $a \in \mathcal{A}$, $a \in \mathsf{Form}$;
- If $\varphi \in \mathsf{Form}$, then $\neg\varphi \in \mathsf{Form}$;
- If $\varphi \in \mathsf{Form}$ and $\psi \in \mathsf{Form}$ are formulas, then $\varphi \vee \psi \in \mathsf{Form}$ and $\varphi \wedge \psi \in \mathsf{Form}$.

Classical logic is the logic of truth values. In our notation, $\top$ denotes the truth value *true* and $\bot$ denotes the truth value *false*.

Exercise 2.2. For $i \in \{1, 2, \dots, n+1\}$ and $j \in \{1, 2, \dots, n\}$ let the atomic proposition a_{ij} denote "the ith pigeon is placed in the jth pigeonhole". Write a formula expressing the Pigeonhole Principle.

To assign meaning to formulas, we will assign truth values to atoms and define the *satisfaction relation* over assignments and formulas. This is also known as truth table semantics.

Definition 2.3. Let $\iota : \mathcal{A} \to \{\top, \bot\}$ an assignment of atomic propositions. The **satisfaction relation** $\models \subseteq 2^{\mathcal{A}} \times \mathsf{Form}$ is defined inductively as follows.

- $\iota \models \top$;
- $\iota \not\models \bot$;
- $\iota \models a$ iff $\iota(a) = \top$;
- $\iota \models \neg\varphi$ iff $\iota \not\models \varphi$;
- $\iota \models \varphi \vee \psi$ iff $\iota \models \varphi$ or $\iota \models \psi$;
- $\iota \models \varphi \wedge \psi$ iff $\iota \models \varphi$ and $\iota \models \psi$.

Definition 2.4. A formula φ is said to be **satisfiable** if there exists ι such that $\iota \models \varphi$. A formula φ is said to be **valid** if for every valuation ι, $\iota \models \varphi$. We write $\models \varphi$ to indicate that φ is valid. Valid formulas are sometimes referred to as **tautologies**.

Theorem 2.5 ([Coo71; Lev73])**.** *Checking satisfiability is NP-complete.*

Exercise 2.6. Show that φ is valid if and only if $\neg\varphi$ is unsatisfiable.

Define the *material implication* $\varphi \supset \psi := \neg\varphi \vee \psi$ denoting "if φ then ψ". The peculiarity of a material implication is the vacuous case *viz.* when $\iota \not\models \varphi$, then $\iota \models \varphi \supset \psi$. Several paradoxes arise from reasoning with material implication; consequently, other forms of conditionals have been considered in both mathematical and philosophical logic. However, material implication is at the heart of reasoning in classical logic, the subject of our study, so we will not debate its merits (or lack thereof) any further.

Define *equivalence* $\varphi \equiv \psi := (\varphi \supset \psi) \wedge (\psi \supset \varphi)$.

Exercise 2.7. φ and ψ are said to be **equisatisfiable** when φ is satisfiable iff ψ is satisfiable. Show that $\varphi \equiv \psi$ is valid iff φ and ψ are equisatisfiable.

Exercise 2.8. Show that the following are valid formulas.

(i) (Involution of negation) $\neg\neg\varphi \equiv \varphi$;

(ii) (De Morgan's law) $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$ and $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$.

A **sequent** is an expression of the form $\Gamma \Rightarrow \Delta$ where Γ and Δ are finite lists of formulas. Γ is called the **antecedent** and Δ is called its **succedent**. They are both referred to as **cedents**.

The intended meaning of a sequent $\varphi_1, \ldots, \varphi_m \Rightarrow \psi_1, \ldots, \psi_n$ is

$$\bigwedge_{i=1}^{m} \varphi_i \supset \bigvee_{j=1}^{n} \psi_j.$$

We adopt the convention that an empty conjunction (say, when $m = 0$ above) is $\top$ and an empty disjunction (say, when $n = 0$ above) is $\bot$.

We are now ready to define the propositional sequent calculus proof system PK (standing for *Propositional Kalkül*).

Definition 2.9. A PK **proof** is a rooted tree, in which the nodes are sequents, generated inductively from *inference rules* in Figure 2.1. The root of the tree is called the **endsequent** and is the sequent proved by the proof. Subtrees of a proof are called **subproofs**. We write $\vdash_{\mathsf{PK}} \Gamma \Rightarrow \Delta$ and $\vdash_{\mathsf{PK}} \varphi$ if there is an PK proof for $\Gamma \Rightarrow \Delta$ and if $\vdash_{\mathsf{PK}} \varnothing \Rightarrow \varphi$ respectively.

An inference rule is an expression of the form

$$\frac{\mathcal{S}_1 \quad \mathcal{S}_2 \quad \dots \quad \mathcal{S}_n}{\mathcal{S}}$$

where $\mathcal{S}$ and $\mathcal{S}_i$s are sequents. The upper sequents are called **premisse(s)** and the lower sequent is called the **conclusion**. The distinguished formula in the conclusion is called the **principal formula**. A rule with no premisses is called an **axiom**. The intended reading is from top to bottom *viz.* assuming the premisses, the conclusion is true.

Inference rules are building blocks of proofs. In other words, each rule should be understood as a *rule schema* that represents many *instances* of the rule. For example, the following are two instances of the $\wedge_r$ rule:

$$\wedge_r \frac{c \Rightarrow \neg a, a \quad c \Rightarrow \neg a, b}{c \Rightarrow \neg a, a \wedge b} \qquad \wedge_r \frac{\Rightarrow a \quad \Rightarrow b \vee c}{\Rightarrow a \wedge (b \vee c)}$$

Proofs vs. programs correspondence

The *proofs vs. programs correspondence* or the *Curry-Howard isomorphism* is a deep concept in logic. Roughly, it states that formulas correspond to data types and proofs of those formulas correspond to programs. For example, conjunction corresponds to product type, disjunction to sum type, and implication to function type. For more details, see [SU06].

We will now briefly discuss each type of rule:

Identity rules. These rules contain repeated occurrences of schema variables: in the initial rule, the formula φ is repeated in the conclusion, and in the cut rule, the formula φ is repeated in the premises. Checking if an application of one of these rules is correct requires comparing the identity of two occurrences of formulas. The cut rule corresponds to the composition of functions by the Curry-Howard isomorphism.

Structural Rules. Structural rules do the equivalent of resource management in programs. The exchange rule allows one to use resources in any order, contraction allows one to duplicate resources, and weakening allows one to discard resources.

Introduction rules. Using the left introduction rules, one can form a function with complex input using function(s) over simple input(s). Dually, using the right introduction rules, one can form a function with complex output using function(s) over simple output(s).

Example 2.10 (Law of excluded middle)**.**
The following is a PK proof of the law of excluded middle, an unabashed classical

Identity rules:

$$\text{init}\ \frac{}{\varphi \Rightarrow \varphi} \qquad \text{cut}\ \frac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Left structural rules:

$$\mathsf{w}_l\ \frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta} \qquad \mathsf{c}_l\ \frac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta} \qquad \mathsf{ex}_l\ \frac{\Gamma, \psi, \varphi, \Gamma' \Rightarrow \Delta}{\Gamma, \varphi, \psi, \Gamma' \Rightarrow \Delta}$$

Right structural rules:

$$\mathsf{w}_r\ \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi} \qquad \mathsf{c}_r\ \frac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi} \qquad \mathsf{ex}_r\ \frac{\Gamma \Rightarrow \Delta, \psi, \varphi, \Delta'}{\Gamma \Rightarrow \Delta, \varphi, \psi, \Delta'}$$

Left introduction rules:

$$\bot_l\ \frac{}{\bot, \Gamma \Rightarrow \Delta} \qquad \neg_l\ \frac{\Gamma \Rightarrow \Delta, \varphi}{\neg\varphi, \Gamma \Rightarrow \Delta} \qquad \vee_l\ \frac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta} \qquad \wedge_l^0\ \frac{\varphi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta} \qquad \wedge_l^1\ \frac{\psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}$$

Right introduction rules:

$$\top_r\ \frac{}{\Gamma \Rightarrow \Delta, \top} \qquad \neg_r\ \frac{\Gamma, \varphi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi} \qquad \vee_r^0\ \frac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \qquad \vee_r^1\ \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \qquad \wedge_r\ \frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}$$

Figure 2.1: Inference rules of PK

principle (i.e. it doesn't hold in some *non*-classical logics).

$$\mathsf{c}_r\ \dfrac{\vee_r^1\ \dfrac{\neg_r\ \dfrac{\vee_r^0\ \dfrac{\text{init}\ \dfrac{}{\varphi \Rightarrow \varphi}}{\varphi \Rightarrow \varphi \vee \neg\varphi}}{\Rightarrow \varphi \vee \neg\varphi, \neg\varphi}}{\Rightarrow \varphi \vee \neg\varphi, \varphi \vee \neg\varphi}}{\Rightarrow \varphi \vee \neg\varphi}$$

Exercise 2.11. (Modus ponens) Give a PK proof for the sequent $\varphi \supset \psi, \varphi \Rightarrow \psi$.

Theorem 2.12 (Soundness). *If* $\vdash_{\mathsf{PK}} \varphi$ *then* $\models \varphi$.

Theorem 2.13 (Completeness). *If* $\models \varphi$ *then* $\vdash_{\mathsf{PK}} \varphi$.

Proof-theorists are generally reluctant to justify the definition of their sequent calculus by the external notion of "truth value" of a formula since proofs for them are first-class citizens. However, the notion of "truth value" has been much emphasised by the likes of Tarski and is widespread in logic, especially in *model theory*.

The soundness and completeness result serves as a bridge between proof theory and model theory. It is, therefore, *not* a theorem of proof theory but of mathematical logic, in general. We will not prove it here and will point the interested reader to standard references [Kle52; Joh87].

Exercise 2.14. Show that for any formula φ, $\varphi \wedge \neg\varphi$ is not provable.

2.2 First-order logic

First-order logic is an extension of propositional logic and allows us to express and prove more (mathematical) statements. Within mathematical practice, key items are *properties of* and *relations between* mathematical *objects*. Think of statements like, "n is even", "8 is prime", "$f(x) = 0$", and "list $[a, b, c]$ is the reverse of list $[c, b, a]$".

The power of first-order logic is that we can prove statements that hold for *all* objects in a given domain, or that there *exists* an object such that a statement holds. This is called *quantification*. Examples are, "*for all* natural numbers n, n is even or n is odd", "there *exists* an x such that $f(x) = 0$", and "*for all* finite lists there *exists* a reverse list". With this powerful language, first-order logic provides a framework to capture mathematical structures such as groups, ordered sets, and arithmetic.

The predicate symbols are there to express properties of and relations between objects. For example we could write $E(n)$ to mean "n is even", $O(n)$ to mean "n is odd" or $R(l_1, l_2)$ to mean that "finite list l_1 is the reverse of finite list l_2. The arity of a predicate symbol and relation symbol denote the number of arguments the symbol takes. So E and O in the example have arity 1, and R has arity 2. Formally, we introduce a first-order signature as follows.

Definition 2.15. A first-order **signature** is a pair $\sigma = (\mathcal{R}, \mathcal{F})$ where:
- $\mathcal{R} = \{P, Q, R, \ldots\}$ is a countable set of **predicate symbols**;
- $\mathcal{F} = \{f, g, h, \ldots\}$ is countable set of **function symbols**.

Each function and predicate symbol has a fixed **arity** $n \in \mathbb{N}$. 0-ary predicate symbols are propositional atoms and 0-ary function symbols are called **constants**.

The signature defines the non-logical symbols of the logic. For the rest of the section, fix a signature $\sigma = (\mathcal{R}, \mathcal{F})$ such that there is a special binary predicate $= \in \mathcal{R}$ called **equality**.

The signature provides the building blocks of *terms* and *formulas* introduced below. Informally speaking, terms denote concepts as individual entities that in itself cannot be true or false. In the text above, "n", "0", and "$f(x)$" are terms. Formulas denote statements that in principal can be true or false. Examples of formulas from above in the language of first-order logic are "$f(x) = 0$", "$\forall n(E(n) \vee O(n))$", "$\exists x(f(x) = 0)$", and "$\forall l \exists k.R(k, l)$".

Definition 2.16. Let $\mathcal{V} = \{x, y, z, \ldots\}$ be a countable set of **variables**. **Terms** (denoted $t, t', \ldots$) are given by the following grammar.

$$t, t' \quad ::= \quad x \in \mathcal{V} \quad | \quad f(t_1, t_2, \ldots, t_n)$$

where f is an n-ary function symbol.

Remark 2.17. By definition, constants are terms.

Definition 2.18. If P is an n-ary predicate symbol and $t_1, \ldots, t_n$ are terms, then $P(t_1, \ldots, t_n)$ is an **atomic formula**. The set of atomic formulas is denoted by $\mathcal{A}$. **First-order formulas** (denoted $\varphi, \psi, \ldots$) are given by the following grammar.

$$\varphi, \psi \quad ::= \quad \top \mid \bot \mid a \in \mathcal{A} \mid \neg\varphi \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \exists x \varphi \mid \forall x \varphi$$

Example 2.19 (Uniqueness)**.** The following formula expresses that there is a unique x such that $\varphi(x)$ holds.

$$\exists x(\varphi(x) \wedge \forall y(\varphi(y) \supset x = y))$$

Exercise 2.20. Write a first-order formula that expresses that the binary predicate P represents a total unary function.

We will now assign truth values to first-order formulas *i.e.* define what it means for a first-order formula to be valid. We will first assign 'meaning' to the non-logical symbols. Fix a signature $\sigma = (\mathcal{R}, \mathcal{F})$.

Definition 2.21. A **first-order structure** for σ (or, a σ-**structure**) is a pair $\mathcal{M} = (D, \iota)$ where D is a non-empty set called the **domain** and ι is a function over $\mathcal{R} \cup \mathcal{F}$ called **interpretation** such that:

- For each n-ary predicate symbol P, $\iota(P) \subseteq D^n$.
  (For a 0-ary relation symbol P, $\iota(P)$ is independent of D and is either $\varnothing$ or a singleton set with a designated element (not in D), say $\{*\}$. This corresponds to assignment of truth values $\bot$ and $\top$ to propositional atoms.)
- For each n-ary function symbol f, $\iota(f) : D^n \to D$ is a function.
  (So, for constants c, $\iota(c) \in D$.)

For convenience, we often denote $\iota(P)$ and $\iota(f)$ by $P^{\mathcal{M}}$ and $f^{\mathcal{M}}$ respectively.

Let $\rho : \mathcal{V} \to D$ be an assignment of variables. Given a σ-structure $\mathcal{M}$, this assignment can be extended to arbitrary terms as follows.

$$\rho(f(t_1, \ldots, t_n) = f^{\mathcal{M}}(\rho(t_1), \ldots \rho(t_n))$$

Definition 2.22. Fix a σ-structure $\mathcal{M} = (D, \iota)$. The **satisfaction relation** $\models \subseteq D^{\mathcal{V}} \times \text{Form}$ is defined inductively as follows.

$$
\begin{array}{lll}
\mathcal{M}, \rho \models (t = t') & \text{iff} & \rho(t) = \rho(t') \\
\mathcal{M}, \rho \models P(t_1, \ldots, t_n) & \text{iff} & (\rho(t_1), \ldots, \rho(t_n)) \in P^{\mathcal{M}} \\
\mathcal{M}, \rho \not\models \bot & & \\
\mathcal{M}, \rho \models \top & & \\
\mathcal{M}, \rho \models \neg\varphi & \text{iff} & \mathcal{M}, \rho \not\models \varphi \\
\mathcal{M}, \rho \models \varphi \wedge \psi & \text{iff} & \mathcal{M}, \rho \models \varphi \text{ and } \mathcal{M}, \rho \models \psi \\
\mathcal{M}, \rho \models \varphi \vee \psi & \text{iff} & \mathcal{M}, \rho \models \varphi \text{ or } \mathcal{M}, \rho \models \psi \\
\mathcal{M}, \rho \models \forall x \varphi & \text{iff} & \mathcal{M}, \rho[x \mapsto d] \models \varphi \text{ for all } d \in D \\
\mathcal{M}, \rho \models \exists x \varphi & \text{iff} & \mathcal{M}, \rho[x \mapsto d] \models \varphi \text{ for some } d \in D
\end{array}
$$

where $\rho[x \mapsto d]$ denotes the interpretation which agrees with ρ for all variables different from x, and maps x to d.

Remark 2.23. We caution the reader to not conflate the syntactic and semantic equality in Definition 2.22.

Definition 2.24. A σ-structure $\mathcal{M}$ is a **model** for a formula φ, denoted $\mathcal{M} \models \varphi$, if for all assignments ρ, $\mathcal{M}, \rho \models \varphi$. A sentence φ is **satisfiable** if it has a model. A sentence φ is **valid**, written $\models \varphi$, if $\mathcal{M} \models \varphi$ for every structure $\mathcal{M}$.

Proposition 2.25. *A formula φ is valid if and only if $\neg\varphi$ is unsatisfiable.*

Example 2.26. Let $\varphi = \exists x \exists y \neg(x = y)$ and $\psi = \exists x \exists y (x = y)$. $\mathcal{M}$ is a model of φ whenever the domain of $\mathcal{M}$ has cardinality greater than 1. On the other hand, ψ is valid.

Theorem 2.27 ([Tra50])**.** *Satisfiability of first-order logic (with at least one binary predicate symbol) over the class of all finite models is undecidable (Σ^0_1-complete).*

Exercise 2.28. Show the following are valid.

1. (De Morgan's law) $\neg\exists x \varphi \equiv \forall x \neg\varphi$;
2. (Prenexing) $(\exists x \varphi) \circ \psi \equiv \exists x(\varphi \circ \psi)$ and $(\forall x \varphi) \circ \psi \equiv \forall x(\varphi \circ \psi)$ where $\circ = \{\wedge, \vee\}$.

Remark 2.29. There is a long philosophical debate about the inclusion (or exclusion) of empty domains. One of the tangible effects of having empty domains is that we no longer have $(\exists x \varphi) \vee \psi \equiv \exists x(\varphi \vee \psi)$.

From this exercise, one can show the following.

Theorem 2.30 (Prenex normal form)**.** *A formula is said to be in **prenex normal form** if it is of the form $Q_1 x_1 Q_2 x_2 \ldots Q_m x_m \psi$ where $Q_i \in \{\forall, \exists\}$ and ψ is quantifier-free. For every first-order formula φ, there is an equisatisfiable formula ψ such that ψ is in prenex normal form.*

To introduce the proof system for first-order logic, we first need to define some notions.

Definition 2.31. The **set of free variables** $\mathrm{FV}(t)$ of term t is inductively defined as follows.

$$\begin{aligned} \mathrm{FV}(x) &:= \{x\} \\ \mathrm{FV}(f(t_1,\ldots,t_n)) &:= \mathrm{FV}(t_1) \cup \cdots \cup \mathrm{FV}(t_n). \end{aligned}$$

The **set of free variables** $\mathrm{FV}(\varphi)$ of formula φ is inductively defined by:

$$\begin{aligned} \mathrm{FV}(P(t_1,\ldots,t_n)) &:= \mathrm{FV}(t_1) \cup \cdots \cup \mathrm{FV}(t_n) \\ \mathrm{FV}(\bot) = \mathrm{FV}(\top) &:= \varnothing \\ \mathrm{FV}(\neg\varphi) &:= \mathrm{FV}(\varphi) \\ \mathrm{FV}(\varphi \wedge \psi) = \mathrm{FV}(\varphi \vee \psi) &:= \mathrm{FV}(\varphi) \cup \mathrm{FV}(\psi) \\ \mathrm{FV}(\forall x\varphi) = \mathrm{FV}(\exists x\varphi) &:= \mathrm{FV}(\varphi) \setminus \{x\}. \end{aligned}$$

The **sets of bound variables** $\mathrm{BV}(t)$ and $\mathrm{BV}(\varphi)$ respectively of a term t and formula φ respectively are defined exactly as above except in the following cases.

$$\begin{aligned} \mathrm{BV}(x) &:= \varnothing \\ \mathrm{BV}(\forall x\varphi) = \mathrm{BV}(\exists x\varphi) &:= \mathrm{BV}(\varphi) \cup \{x\}. \end{aligned}$$

Remark 2.32. Note that constants and propositional atoms have no free or bound variables.

Definition 2.33. A formula φ is called **open** if $\mathrm{FV}(\varphi) \neq \varnothing$ and **closed** otherwise. Closed formulas are also called **sentences**. We say that a variable x is **fresh** for a formula φ if $x \notin \mathrm{FV}(\varphi)$.

Example 2.34. Suppose $0, f \in \mathcal{F}$ such that 0 is a constant and f is a unary function symbol. Then, $f(x) = 0$ is an open formula with free variable x, and $\exists x(f(x) = 0)$ is a sentence.

Remark 2.35. A variable can be both bound and free in a formula. For example, x is both free and bound in $\forall x P(x) \wedge \forall y(Q(y,x) \vee Q(x,y))$. Throughout the text, we will adopt the convention to *rename* bound variables to maintain the invariant $\mathrm{FV}(\varphi) \cap \mathrm{BV}(\varphi) = \varnothing$ for all formulas φ.

Finally, $\varphi[t/x]$ denotes φ where every occurrence of the variable x has been replaced by term t. In order to prevent that some $y \in \mathrm{FV}(t)$ may become bound by a quantifier $\forall y$ or $\exists y$ in φ, we work with *capture-avoiding substitution* as discussed in Appendix A.1.

We are now ready to extend PK, to define a sequent calculus system LK[1] (standing for *Logistischer klassischer Kalkül*) for first-order logic.

[1]LK usually refers to the sequent calculus for pure first-order logic *i.e. without* equality.

Left quantifier introduction rules:

$$\forall_l \frac{\varphi[t/x], \Gamma \Rightarrow \Delta}{\forall x\varphi, \Gamma \Rightarrow \Delta} \qquad \exists_l \frac{\varphi[y/x], \Gamma \Rightarrow \Delta}{\exists x\varphi, \Gamma \Rightarrow \Delta}\ y \text{ is fresh}$$

Right quantifier introduction rules:

$$\forall_r \frac{\Gamma \Rightarrow \Delta, \varphi[y/x]}{\Gamma \Rightarrow \Delta, \forall x\varphi}\ y \text{ is fresh} \qquad \exists_r \frac{\Gamma \Rightarrow \Delta, \varphi[t/x]}{\Gamma \Rightarrow \Delta, \exists x\varphi}$$

Equality rules:

$$=_r \frac{}{\Rightarrow t = t} \qquad =_l \frac{\Gamma[s/t] \Rightarrow \Delta[s/t]}{s = t, \Gamma \Rightarrow \Delta}$$

Figure 2.2: Quantifier rules and equality rules of LK. In $\exists_l$ and $\forall_r$, y is called an **eigenvariable** and the side condition "y is fresh" means that y is not free in any of the formulas in the conclusion of the rule. The $=_l$ rule is known as **Leibniz rule**.

Definition 2.36. The sequent calculus LK consists of the rules for PK presented in Figure 2.1 and the rules presented in Figure 2.2. All notions of **proof**, **endsequent**, **conclusion**, and **premisse** are defined analoguous to Definition 2.9. We write $\vdash_{\mathsf{LK}} \Gamma \Rightarrow \Delta$ and $\vdash_{\mathsf{LK}} \varphi$ if there is an LK proof for $\Gamma \Rightarrow \Delta$ and if $\vdash_{\mathsf{LK}} \varnothing \Rightarrow \varphi$ respectively.

Exercise 2.37 (Symmetry and transitivity of equality)**.** Give LK proofs showing that equality is symmetric and transitive.

Intuitively, the $\forall_r$ rule states that to prove $\forall x\varphi$, it is enough to show $\varphi[y/x]$ for an arbitrarily chosen y. The freshness condition on y captures the idea that y is arbitrary. For example, in the following 'proof', the eigenvariable in the step marked $*$ is not fresh and ends up establishing an absurd statement.

$$\forall_r \cfrac{\forall_r \cfrac{=_r \cfrac{}{\Rightarrow y = y}}{\Rightarrow \forall z(y = z)}\ *}{\Rightarrow \forall x \forall z(x = z)}$$

Example 2.38.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi[z/x,u/y] \Rightarrow \varphi[u/y,z/x]}\ \text{init}}{\forall y\varphi[z/x] \Rightarrow \varphi[u/y][z/x]}\ \forall_l}{\forall y\varphi[z/x] \Rightarrow \exists y\varphi[u/y]}\ \exists_r}{\forall y\varphi[z/x] \Rightarrow \forall y\exists x\varphi}\ \forall_r\ u \text{ is fresh}}{\exists x\forall y\varphi \Rightarrow \forall y\exists x\varphi}\ \exists_l\ z \text{ is fresh}$$

Consider the sequent $\forall x\exists y\varphi \Rightarrow \exists x\forall y\varphi$. At first glance, it might seem that this could be proved by the same recipe. However, that is absurd since among other things, it would mean pointwise continuity implies uniform continuity. We will later show that it is not provable.

Exercise 2.39 (Drinker's paradox)**.** The drinker's paradox states that "There is someone in the pub such that, if he is drinking, then everyone in the pub is drinking." This is expressed as $\varphi = \exists x(\mathsf{D}(x) \supset \forall y(\mathsf{D}(y)))$ in first-order logic where D is a unary predicate symbol denoting its argument is drinking. Show that $\vdash_{\mathsf{LK}} \varphi$.

Theorem 2.40 (Soundness)**.** *If* $\vdash_{\mathsf{LK}} \varphi$ *then* $\models \varphi$.

Theorem 2.41 (Gödel's Completeness)**.** *If* $\models \varphi$ *then* $\vdash_{\mathsf{LK}} \varphi$.

Gödel's completeness is a milestone result in mathematical logic, first proved by Kurt Gödel in 1929. The proof has been subsequently simplified by Leon Henkin and Gisbert Hasenjaeger. As before, we will not prove it here and will point the interested reader to standard references [Her73].

Exercise 2.42. Show that if $x, y \in \mathrm{FV}(\varphi)$, then $\nvdash_{\mathsf{LK}} \forall x\exists y\varphi \Rightarrow \exists x\forall y\varphi$.

Corollary 2.43. *The set of valid first-order formulas is recursively enumerable.*

Exercise 2.44 (Finite model property does not hold)**.** Show that there is a first-order sentence φ that is not valid but every finite first-order structure is a model of φ.

First-order logic provides a language to formalise mathematical structures such as groups, ordered sets, and arithmetic. This is done by adding extra axioms resulting in *first-order theories*. A small introduction to first-order theories is provided in the Appendix A.2.

Chapter 3

Properties of sequent calculus

In this chapter, we will closely inspect the rules of the sequent calculus. We will see if some variants can replace them and will wonder if there are any redundant rules. We will introduce *Hauptzats* or the *main result*. It is the cornerstone of proof theory and we will discuss its various applications in Chapter 4.

3.1 Derivability

A **sequent calculus** is a set of rules. Recall that a rule should be understood as a *rule schema* with many *instances* of the rule.

Definition 3.1. Let r be the following rule schema.

$$r\,\frac{\mathcal{S}_1 \quad \mathcal{S}_2 \quad \dots \quad \mathcal{S}_n}{\mathcal{S}}$$

Then, r is said to be **derivable** in a sequent calculus SC if for every instance of r,

$$r\,\frac{s_1 \quad s_2 \quad \dots \quad s_n}{s}$$

there is a proof of the sequent s from the sequents s_i using the rules from SC. (One can view this as a proof in SC where s_is might occur as leaves.)

Example 3.2. Consider the following rule (known as the multiplicative right conjunction introduction rule)

$$\wedge_r^m\,\frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma' \Rightarrow \Delta', \psi}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \varphi \wedge \psi}$$

Additive rules	**Multiplicative rules**
$\text{cut}^a \; \dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$	$\text{cut} \; \dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$
$\vee_l \; \dfrac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta}$ $\vee_r^0 \; \dfrac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \quad \vee_r^1 \; \dfrac{\Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}$	$\vee_l^m \; \dfrac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma' \Rightarrow \Delta'}{\varphi \vee \psi, \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$ $\vee_r^m \; \dfrac{\Gamma \Rightarrow \Delta, \varphi, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}$
$\wedge_l^0 \; \dfrac{\varphi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta} \quad \wedge_l^1 \; \dfrac{\psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}$ $\wedge_r \; \dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}$	$\wedge_l^m \; \dfrac{\varphi, \psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}$ $\wedge_r^m \; \dfrac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma' \Rightarrow \Delta', \psi}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \varphi \wedge \psi}$

Figure 3.1: Additive and multiplicative rules in LK

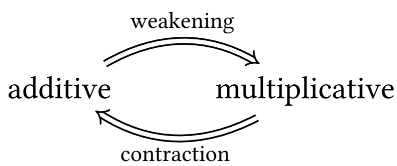
It is derivable in LK.

$$\wedge_r \; \dfrac{\text{ex}_l^*,\text{w}_l^*,\text{ex}_r^*,\text{w}_r^* \; \dfrac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \varphi} \qquad \text{w}_l^*,\text{ex}_r^*,\text{w}_r^* \; \dfrac{\Gamma' \Rightarrow \Delta', \psi}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \varphi \wedge \psi}$$

The left conjunction and disjunction rules also have multiplicative versions. On the other hand, the cut has an *additive* version (cf. Figure 3.1). The rationale behind the nomenclature 'multiplicative' and 'additive' is beyond the scope of these notes. In the sequent calculi we introduced, we presented additive conjunction and disjunction rules, and the multiplicative cut rule.

Exercise 3.3. Show that the multiplicative conjunction and disjunction rules, and the additive cut rule are derivable in LK.

In fact, the multiplicative and additive rules are interderivable. This can be succinctly schematised as follows.



Proposition 3.4. *The* cut *rule is not derivable in* LK $\setminus$ {cut}.

Proof. Let a and b be distinct atoms. From the hypotheses $a \Rightarrow b$ and $\Rightarrow a$, it is impossible to derive $\Rightarrow b$ in LK $\setminus$ {cut} since no rules can be applied to b to get a. ☐

3.2 Admissibility

Definition 3.5. Let r be the following rule schema.

$$r\,\frac{\mathcal{S}_1 \quad \mathcal{S}_2 \quad \dots \quad \mathcal{S}_n}{\mathcal{S}}$$

Then, r is said to be **admissible** in a sequent calculus SC if for every instance of r,

$$r\,\frac{s_1 \quad s_2 \quad \dots \quad s_n}{s}$$

if sequents s_i is provable in SC for all $i \leq n$, then sequent s is provable in SC.

Remark 3.6. When we add an admissible rule to a sequent calculus, we cannot prove new sequents, *i.e.* if rule r is admissible in sequent calculus SC, then sequent s is provable in SC $\cup \{r\}$ if and only if s is provable in SC.

Remark 3.7 (Admissibility vs. Eliminability). Admissibility is sometimes stated in terms of eliminability *i.e.* a rule r is admissible in a sequent calculus SC $\setminus \{r\}$ if and only if it can be eliminated in SC $\cup \{r\}$.

Remark 3.8. Every derivable rule is admissible, but not vice versa in general (for example, cut; cf. Proposition 3.4 and Theorem 3.17).

We look at some admissible rules which will be useful later.

Proposition 3.9 (Axiom expansion)**.** *The* init *rule is admissible in* LK $\setminus$ {init} $\cup$ {a-init} *where* a-init *is defined as follows and a is any atomic formula.*

$$\text{a-init}\,\frac{}{a \Rightarrow a}$$

Proof. The init rule has no premises, so its admissibility means that for every formula φ, the sequent $\varphi \Rightarrow \varphi$ is provable in LK $\setminus$ {init} $\cup$ {a-init}. The proof proceeds by induction on the structure of φ.
The base case is when φ is atomic. This is provable by the a-init rule. For the induction case, there are several subcases.

Case 1. $\varphi = \neg\psi$:

$$\neg_l \dfrac{\text{ex},\neg_r \dfrac{\dfrac{IH}{\psi \Rightarrow \psi}}{\Rightarrow \neg\psi, \psi}}{\neg\psi \Rightarrow \neg\psi}$$

Case 2. $\varphi = \psi_0 \wedge \psi_1$:

$$\wedge_r \dfrac{\wedge_l^0 \dfrac{\dfrac{IH}{\psi_0 \Rightarrow \psi_0}}{\psi_0 \wedge \psi_1 \Rightarrow \psi_0} \quad \wedge_l^1 \dfrac{\dfrac{IH}{\psi_1 \Rightarrow \psi_1}}{\psi_0 \wedge \psi_1 \Rightarrow \psi_1}}{\psi_0 \wedge \psi_1 \Rightarrow \psi_0 \wedge \psi_1}$$

Case 3. $\varphi = \psi_0 \vee \psi_1$: This is symmetric to the previous case.
Case 4. $\varphi = \exists x\psi$

$$\exists_l \dfrac{\exists_r \dfrac{\dfrac{IH}{\psi[y/x] \Rightarrow \psi[y/x]}}{\psi[y/x] \Rightarrow \exists x\psi}}{\exists x\psi \Rightarrow \exists x\psi}$$

Case 5. $\varphi = \forall x\psi$: This is symmetric to the previous case.

□

Exercise 3.10. Show that the w_r rule is admissible in $\mathsf{LK} \setminus \{\mathsf{w}_r\} \cup \{\text{a-w}\}$ where a-w is defined as follows and a is any atomic formula.

$$\text{a-w} \dfrac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, a}$$

Proposition 3.11. *The* c_r *rule is not admissible in* $\mathsf{LK} \setminus \{\mathsf{c}_r\} \cup \{\text{a-}\mathsf{c}_r\}$ *where* a-c_r *is defined as follows and a is an atomic formula.*

$$\text{a-c}_r \dfrac{\Gamma \Rightarrow \Delta, a, a}{\Gamma \Rightarrow \Delta, a}$$

Proof. Consider the law of excluded middle. We showed in Example 2.10 that it is provable in PK (and hence in LK). If there were a proof of the sequent in $\mathsf{LK} \setminus \{\mathsf{c}_r\} \cup \{\text{a-}\mathsf{c}_r\}$, there would be one in $\mathsf{LK} \setminus \{\mathsf{c}_r, \mathsf{cut}\} \cup \{\text{a-}\mathsf{c}_r\}$ by cut-admissibility stated in Theorem 3.17. The bottom-most rule on a cut-free proof can only be $\vee_r$ or w_r. We obtain that there is no cut-free proof in $\mathsf{LK} \setminus \{\mathsf{c}_r\} \cup \{\text{a-}\mathsf{c}_r\}$. □

Remark 3.12. Symmetric results hold for the left structural rules.

Definition 3.13. A rule r with n premises

$$r\,\frac{\mathcal{S}_1 \quad \mathcal{S}_2 \quad \dots \quad \mathcal{S}_n}{\mathcal{S}}$$

is said to be **invertible** if for all $i \leq n$ the rule

$$\frac{\mathcal{S}}{\mathcal{S}_i}$$

is admissible. In other words, rule r is invertible when for each instance of the rule: if the conclusion is provable then so are all the premisses.

Example 3.14 (Right conjunction rule is invertible)**.** We show that the inverse of the rule is derivable, and hence admissible in LK.

$$\mathsf{cut}\,\dfrac{\Gamma \Rightarrow \Delta, \varphi \wedge \psi \qquad \wedge_l^0\,\dfrac{\mathsf{init}\,\dfrac{}{\varphi \Rightarrow \varphi}}{\varphi \wedge \psi \Rightarrow \varphi}}{\Gamma \Rightarrow \Delta, \varphi}$$

Exercise 3.15. Show that:
(i) multiplicative right disjunction is invertible; and
(ii) multiplicative right conjunction is *not* invertible.

Implication $\supset$ is not a primitive symbol in these lecture notes, but is defined as $\varphi \supset \psi := \neg\varphi \vee \psi$. The following exercise shows that the sequent arrow $\Rightarrow$ could be viewed as an external implication.

Exercise 3.16. Prove the following fact using invertible rules:

$$\vdash_{\mathsf{LK}} \Gamma \Rightarrow \Delta, \varphi \supset \psi \text{ iff } \vdash_{\mathsf{LK}} \Gamma, \varphi \Rightarrow \Delta, \psi$$

The structural rules in LK capture resource management in programs. Other formulations of the sequent calculus relax some of these structural rules while still obtaining a calculus for classical first-order logic. We briefly discuss two directions without going into actual proofs.

Multisets and sets. A sequent $\Gamma \Rightarrow \Delta$ is defined on the basis of *lists* Γ and Δ. One can also consider *multisets* instead of lists. A multiset is a collection of objects in which elements may occur more than once, but in which the order does not matter. When using multisets, applications of the exchange rules ex_l, ex_r will be implicit. We can even further relax the structure by assuming Γ and Δ to be *sets* in which in addition the contraction rules c_l, c_r become implicit.

Admissible rules. When using multisets some of the rules in LK can be changed so that weakening and contraction become admissible, hence becoming implicit. For example, the weakening rules w_l and w_r become admissible when we replace the additive rules $\wedge_r^0, \wedge_r^1$ and $\vee_l^0, \vee_l^1$ in LK by the multiplicative rules $\wedge_r^m$ and $\vee_l^m$, respectively, and rule init by the following rule:

$$\mathsf{init}' \frac{}{\Gamma, \varphi \Rightarrow \Delta, \varphi}$$

One of the major theorems of proof theory is the admissibility of cuts *i.e.* if a sequent is provable in LK then it is provable in LK without cuts. This is known as the *Hauptsatz* by Gerard Gentzen in 1935.

Theorem 3.17 (Cut-admissibility)**.** *The* cut *rule is admissible in* LK $\setminus$ {cut}.

One might wonder what is the point of cuts if one can get rid of them. We list some main reasons.

(i) Cuts are useful from the proofs vs. programs correspondence since they represent the composition of functions.

(ii) Cuts can give up to a non-elementary reduction in the size of proofs as stated in Theorem 3.18 below.

(iii) Moreover, cut-admissibility is a highly non-trivial result and it is not a priori clear that we can eliminate cuts.

Theorem 3.18 ([Sta79; Ore82])**.** *There is a sequent* $\Gamma \Rightarrow \Delta$ *such that there is an* LK *proof of* $\Gamma \Rightarrow \Delta$ *of size* n *and all cut-free* LK *proofs of* $\Gamma \Rightarrow \Delta$ *of size at least* $\mathsf{Tower}(n)$ *where* Tower *is inductively defined as* $\mathsf{Tower}(1) = 2$ *and* $\mathsf{Tower}(n+1) = 2^{\mathsf{Tower}(n)}$.

However, cut-admissibility also has many advantages. We will discuss some of them in Chapter 4.

Chapter 4

Applications of cut-elimination

4.1 Consistency and subformula property

Theorem 4.1 (Consistency). $\nvdash_{\mathsf{LK}} \bot$

Proof. If there were a proof, there would be a cut-free proof. The only rule that can be applied is $\bot_r$, and then we have an empty sequent which is neither an axiom nor can any rule be applied. Therefore, it is not provable. □

Corollary 4.2. *For all φ, either $\nvdash_{\mathsf{LK}} \varphi$ or $\nvdash_{\mathsf{LK}} \neg\varphi$.*

Proof. Suppose $\vdash_{\mathsf{LK}} \varphi$ and $\vdash_{\mathsf{LK}} \neg\varphi$. Then, $\vdash_{\mathsf{LK}} \bot$ as follows. Contradiction!

$$\mathsf{cut}\,\dfrac{\mathsf{w}_r\,\dfrac{\begin{matrix}\vdots\\ \varnothing \Rightarrow \varphi\end{matrix}}{\varnothing \Rightarrow \bot, \varphi} \qquad \neg_l\,\dfrac{\begin{matrix}\vdots\\ \varnothing \Rightarrow \neg\varphi\end{matrix}}{\varphi \Rightarrow \varnothing}}{\varnothing \Rightarrow \bot}$$

□

Cut-free proofs are *analytic i.e.* proofs that do not go beyond their subject matter. The term was first used by Bernard Bolzano, who was unhappy with his proof of the intermediate value theorem that relied on geometric intuitions. In modern proof theory, 'concepts' are interpreted as subformulas.

Definition 4.3. Fix a signature σ. Let the set of all σ-terms be $\mathbb{T}$. Let φ be a first-order formula. The set of subformulas of φ, denoted $\mathsf{SF}(\varphi)$, is the smallest set such that:

- $\varphi \in \mathsf{SF}(\varphi)$;
- If $\neg\psi \in \mathsf{SF}(\varphi)$, then $\psi \in \varphi$;
- If $\psi_0 \circ \psi_1 \in \mathsf{SF}(\varphi)$, then $\{\psi_0, \psi_1\} \subseteq \varphi$ where $\circ \in \{\vee, \wedge\}$;
- If $Qx\psi \in \mathsf{SF}(\varphi)$, then $\psi[t/x] \in \varphi$ for all $t \in \mathbb{T}$ where $Q \in \{\exists, \forall\}$.

Theorem 4.4 (Subformula property)**.** *Let $\pi \vdash_{\mathsf{LK}} \Gamma \Rightarrow \Delta$ where π is cut-free. Then any formula occurring in π is a subformula of one of the formulas in $\Gamma \cup \Delta$.*

One immediate corollary of the subformula property is that proof-search is decidable for propositional logic.

Theorem 4.5 (Decidability)**.** *Given a propositional formula φ, it is decidable whether $\vdash_{\mathsf{PK}} \varphi$.*

Proof. The set of subformulas of a propositional formula is linear in its size. Consequently, the height of a cut-free proof (construing cedents as sets) of a sequent is linear in its size. One can check all possible 'proofs' of a certain height in finite time. □

Remark 4.6. A first-order formula may have infinitely many subformulas even over the empty signature since we assume an infinite supply of variables and $\varphi[y/x]$ and $\varphi[z/x]$ cannot be identified because they can be simultaneously used in the same sequent.

4.2 Herbrand's theorem

Herbrand's theorem is a fundamental result of mathematical logic that essentially allows a certain kind of reduction of first-order logic to propositional logic. It is thus the logical foundation for most automatic theorem provers. What follows is a simple proof of Herbrand's theorem. However, sequent calculus and cut-elimination were not known at the time of Herbrand and he had to prove his theorem in a much more complicated way. We will first prove the mid-sequent lemma and Herbrand's theorem will follow immediately.

Lemma 4.7 (Mid-sequent lemma)**.** *Let $\vdash_{\mathsf{LK}} \Gamma \Rightarrow \Delta$ where Γ, Δ only contain formulas in prenex normal form. Then there exists a cut-free proof $\Gamma \Rightarrow \Delta$ that can be factored as*

$$\begin{array}{c} \pi' \\ \Gamma' \Rightarrow \Delta' \\ \pi \, \| \\ \Gamma \Rightarrow \Delta \end{array}$$

*such that (i) π only contains instances of structural and quantifier rules; and (ii) Γ', Δ' contain only quantifier-free formulas. Here $\Gamma' \Rightarrow \Delta'$ is called the **mid-sequent**.*

Proof. By Theorem 3.17, Proposition 3.9, and Exercise 3.10, let π be a cut-free LK proof of $\Gamma \Rightarrow \Delta$ with identity and weakening only on atomic formulas. We will transform π in a proof $[\pi]$ of the requisite shape by induction on π.
The base case is when the last rule applied in π is an instance of init, $\bot_l$, $\top_r$, and $=_r$. In all these cases, $[\pi] = \pi$. For the induction case, suppose π of the form:

$$\cfrac{\overset{\pi_1}{s_1} \quad \dots \quad \overset{\pi_n}{s_n}}{\Gamma \Rightarrow \Delta}\, r$$

There are three subcases.

Case 1. r is a quantifier or a structural rule. Then, $n = 1$ and $[\pi]$ is obtained from $[\pi_1]$ by applying r.

Case 2. r is unary . Assume it is a right rule (It is symmetric for left unary rules). Let the principal formula be φ. Since Δ are in prenex normal form, φ is quantifier-free. Let $\Delta = \Sigma, \varphi$. Note that $n = 1$ and let ψ be the subformula of φ in s_1. Wlog s_1 is of the form $\Gamma \Rightarrow \Sigma, \psi$. By hypothesis, $[\pi_1]$ can be factored as

$$\begin{array}{c} \pi' \\ \Gamma' \Rightarrow \Sigma', \psi \\ \delta(\psi) \,\Vert \\ \Gamma \Rightarrow \Sigma, \psi \end{array}$$

where $\delta(\psi)$ only contains quantifier and structural rules and $\Gamma' \Rightarrow \Sigma', \psi$ is quantifier-free. Then, $[\pi]$ is:

$$\begin{array}{c} \pi' \\ \cfrac{\Gamma' \Rightarrow \Sigma', \psi}{\Gamma' \Rightarrow \Sigma', \varphi}\, r \\ \delta(\varphi) \,\Vert \\ \Gamma \Rightarrow \Sigma, \varphi \end{array}$$

Case 3. r is binary. As before assume it is a right rule and let $\Delta = \Sigma, \varphi$ where φ is the quantifier-free principal formula. Note that $n = 2$ and let ψ_1 and ψ_2 be the subformulas of φ in s_1 and s_2 respectively. Wlog s_i is of the form $\Gamma \Rightarrow \Sigma, \psi_i$. By hypothesis, $[\pi_i]$ can be factored as

$$
\begin{array}{c}
\pi_i' \\
\Gamma_i \Rightarrow \Sigma_i, \psi_i \\
\delta_i(\psi_i) \, \Big\| \\
\Gamma \Rightarrow \Sigma, \psi_i
\end{array}
$$

where $\delta_i(\psi_i)$ only contains quantifier and structural rules and $\Gamma_i \Rightarrow \Sigma_i, \psi$ is quantifier-free for $i \in \{1, 2\}$. Then, $[\pi]$ is:

$$
\dfrac{
\dfrac{\begin{array}{c}\pi_1' \\ \Gamma_1 \Rightarrow \Sigma_1, \psi_1\end{array}}{\Gamma_1, \Gamma_2 \Rightarrow \Sigma_1, \Sigma_2, \psi_1}\,\text{a-w}_l^*,\text{a-w}_r^*
\qquad
\dfrac{\begin{array}{c}\pi_2' \\ \Gamma_2 \Rightarrow \Sigma_2, \psi_2\end{array}}{\Gamma_1, \Gamma_2 \Rightarrow \Sigma_1, \Sigma_2, \psi_2}\,\text{a-w}_l^*,\text{a-w}_r^*
}{
\begin{array}{c}
\Gamma_1, \Gamma_2 \Rightarrow \Sigma_1, \Sigma_2, \varphi \\
\delta_2(\varphi) \, \Big\| \\
\Gamma_1, \Gamma \Rightarrow \Sigma_1, \Sigma, \varphi \\
\delta_1(\varphi) \, \Big\| \\
\dfrac{\Gamma, \Gamma \Rightarrow \Sigma, \Sigma, \varphi}{\Gamma \Rightarrow \Sigma, \varphi}\,\text{c}_l^*,\text{c}_r^*
\end{array}
}\, r
$$

□

Theorem 4.8 (Herbrand's theorem). *Let* $\vdash_{\text{LK}} \exists \vec{x} \varphi$ *with* φ *quantifier-free. Then, there exist sequences of terms* $\vec{t}_1, \ldots, \vec{t}_n$ *such that* $\vdash_{\text{LK}} \varphi[\vec{t}_1/\vec{x}], \ldots, \varphi[\vec{t}_n/\vec{x}]$.

Proof. By the mid-sequent theorem, there is a proof of $\Rightarrow \exists \vec{x} \varphi$ that can be factored as

$$
\begin{array}{c}
\pi' \\
\Rightarrow \Gamma \\
\pi \, \Big\| \\
\Rightarrow \exists \vec{x} \varphi
\end{array}
$$

such that π contains only quantifier and structural rules, and Γ is quantifier-free. Therefore, Γ is of the form $\varphi[\vec{t}_1/\vec{x}], \ldots, \varphi[\vec{t}_n/\vec{x}]$. □

Exercise 4.9 (Strengthening and generalising is difficult).

1. Show that Herbrand's Theorem cannot be strengthened by taking $n = 1$.
2. Let $\varphi = \forall x(R(y) \vee \neg R(x))$. Show that $\vdash_{\text{LK}} \exists y \varphi$ but for all terms $t_1, \ldots, t_n$, $\nvdash_{\text{LK}} \varphi[\vec{t}_1/\vec{x}], \ldots, \varphi[\vec{t}_n/\vec{x}]$.

Universal quantifiers can be removed by adding more symbols to the language in a process called *Herbrandisation*. This is outside the scope of the current note.

4.3 Interpolation

Craig's interpolation theorem states that for each provable implication $\varphi \supset \psi$ there is an *interpolant* θ such that $\varphi \supset \theta$, $\theta \subset \psi$, and the non-logical symbols in θ occur in φ and in ψ. The theorem represents in a way the 'end of history' as it seems to be the last significant property of first-order logic that has come to light [vBen08]. Interestingly, despite seeming like a bespoke metalogical result, interpolation has found applications in model checking and query reformulation in databases.

Definition 4.10. The **vocabulary** of a formula φ, denoted $\mathsf{Voc}(\varphi)$, is the set of non-logical symbols in φ. For a cedent Γ, $\mathsf{Voc}(\Gamma) = \bigcup_{\varphi \in \Gamma} \mathsf{Voc}(\varphi)$.

Remark 4.11. For a propositional formula φ, $\mathsf{Voc}(\varphi) \subset \mathcal{A}$, the set of atomic propositions. For a first-order formula φ, $\mathsf{Voc}(\varphi) \subseteq \mathcal{R} \cup \mathcal{F}$, where $(\mathcal{R}, \mathcal{F})$ is the signature.

Theorem 4.12 (Craig's interpolation theorem). *Suppose* $\vdash_{\mathsf{LK}} \varphi \supset \psi$*. Then, there is a formula* θ *such that:*

1. $\mathsf{Voc}(\theta) \subseteq \mathsf{Voc}(\varphi) \cap \mathsf{Voc}(\psi)$,
2. $\vdash_{\mathsf{LK}} \varphi \supset \theta$, *and*
3. $\vdash_{\mathsf{LK}} \theta \supset \psi$.

The formula θ *is called an* ***interpolant****.*

Example 4.13 (Interpolants are not necessarily unique). Let $\varphi = (a \wedge b) \vee (\neg c \wedge d)$ and $\psi = e \vee a \vee b \vee \neg c$. We have $\vdash_{\mathsf{PK}} \varphi \supset \psi$ and that $\mathsf{Voc}(\varphi) \cap \mathsf{Voc}(\psi) = \{a, b, c\}$. There are multiple interpolants *viz.* $a \vee \neg c$, $b \vee \neg c$, and $a \vee b \vee \neg c$.

Several proofs of interpolation are known in the literature. We will present a proof-theoretic technique known as *Maehara's method*. We will only prove Theorem 4.12 for the propositional case. First, we will set up some notation.

Definition 4.14. Let Γ, Γ', Δ, and Δ' be cedents and θ be a formula such that $\mathsf{Voc}(\theta) \subseteq \mathsf{Voc}(\Gamma, \Delta) \cap \mathsf{Voc}(\Gamma', \Delta')$, $\vdash_{\mathsf{PK}} \Gamma \Rightarrow \Delta, \theta$, and $\vdash_{\mathsf{PK}} \theta, \Gamma' \Rightarrow \Delta'$. We write this as $\Gamma; \Gamma' \overset{\theta}{\Rightarrow} \Delta; \Delta'$ and $\Gamma; \Gamma' \Rightarrow \Delta; \Delta'$ is called a **split sequent**.

Lemma 4.15. *Suppose* $\vdash_{\mathsf{PK}} \Gamma, \Gamma' \Rightarrow \Delta, \Delta'$*. Then, there exists* $\theta \in \mathsf{Form}$ *such that* $\Gamma; \Gamma' \overset{\theta}{\Rightarrow} \Delta; \Delta'$.

The propositional version of Theorem 4.12 follows immediately from Lemma 4.15.

Proof of Theorem 4.12. By Exercise 3.16, we have that $\vdash_{\mathsf{PK}} \varphi \Rightarrow \psi$. Plugging $\Gamma = \varphi$, $\Gamma' = \varnothing$, $\Delta = \varnothing$, and $\Delta' = \psi$ in Lemma 4.15, we have that there exists θ such that $\varphi; \varnothing \overset{\theta}{\Rightarrow} \varnothing; \psi$. Using Exercise 3.16 again, we are done. □

Remark 4.16. Note that if $\Gamma; \Gamma' \overset{\theta}{\Rightarrow} \Delta; \Delta'$, we have,

$$\text{cut}\ \frac{\Gamma \Rightarrow \Delta, \theta \qquad \theta, \Gamma' \Rightarrow \Delta}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

So, the proof of Lemma 4.15 can be seen as "reverse cut-elimination".

Proof of Lemma 4.15. Suppose $\vdash_{\mathsf{PK}} \Gamma, \Gamma' \Rightarrow \Delta, \Delta'$. By Theorem 3.17, there is a *cut-free* proof π. We will construct an interpolant θ by induction on the structure of π.

The base case is an application of the init, $\top_r$, or $\bot_l$ rule. However, since we have split sequents we have several cases, depending on which side of the *split* the formulas are. We will treat one salient case:

$$\pi = \text{init}\ \frac{}{;\varphi \Rightarrow ; \varphi}$$

We claim that $\theta = \top$. Indeed, $\mathrm{Voc}(\top) = \varnothing \subseteq \mathrm{Voc}(\varnothing) \cap \mathrm{Voc}(\varphi) = \varnothing$, $\vdash_{\mathsf{PK}} \Rightarrow \top$ and $\vdash_{\mathsf{PK}} \varphi \Rightarrow \varphi$.

For the induction step, there are several subcases based on the bottommost rule of π. Again, the cases are doubled because of the split sequents. We will treat two salient cases.

- The bottom-most rule is an instance of $\neg_l$ of the following form.

$$\pi = \neg_l\ \frac{\overset{\pi'}{\Gamma; \Gamma' \Rightarrow \varphi, \Delta; \Delta'}}{\neg\varphi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'}$$

By applying induction hypothesis on π', we have $\Gamma; \Gamma' \overset{\theta'}{\Longrightarrow} \varphi, \Delta; \Delta'$ for some θ'. We claim that $\theta = \theta'$.

$$\begin{aligned} \mathrm{Voc}(\theta) &\subseteq \mathrm{Voc}(\Gamma, \varphi, \Delta) \cap \mathrm{Voc}(\Gamma', \Delta') && \text{[By induction hypothesis]} \\ &= \mathrm{Voc}(\neg\varphi, \Gamma, \Delta) \cap \mathrm{Voc}(\Gamma', \Delta') && [\mathrm{Voc}(\varphi) = \mathrm{Voc}(\neg\varphi)] \end{aligned}$$

We have $\vdash_{\mathsf{PK}} \neg\varphi, \Gamma \Rightarrow \Delta, \theta$ as follows and $\vdash_{\mathsf{PK}} \theta, \Gamma' \Rightarrow \Delta'$ directly from induction hypothesis.

$$\neg_l\ \frac{\overset{IH}{\Gamma \Rightarrow \varphi, \Delta, \theta}}{\neg\varphi, \Gamma \Rightarrow \Delta, \theta}$$

- The bottom-most rule is an instance of $\vee_l$ of the following form.

$$\pi = \dfrac{\overset{\pi_1}{\varphi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'} \quad \overset{\pi_2}{\psi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'}}{\varphi \vee \psi, \Gamma; \Gamma' \Rightarrow \Delta; \Delta'} \vee_l$$

By applying induction hypothesis on π_1 and π_2, we have $\varphi, \Gamma; \Gamma' \overset{\theta_1}{\Longrightarrow} \Delta; \Delta'$ and $\psi, \Gamma; \Gamma' \overset{\theta_2}{\Longrightarrow} \Delta; \Delta'$ for some θ_1, θ_2. We claim that $\theta = \theta_1 \vee \theta_2$.

$$\begin{aligned}
\mathrm{Voc}(\theta) &= \mathrm{Voc}(\theta_1) \cup \mathrm{Voc}(\theta_2) && (1)\\
&\subseteq (\mathrm{Voc}(\varphi, \Gamma, \Delta) \cap \mathrm{Voc}(\Gamma', \Delta')) \cup (\mathrm{Voc}(\psi, \Gamma, \Delta) \cap \mathrm{Voc}(\Gamma', \Delta')) && (2)\\
&= (\mathrm{Voc}(\varphi, \Gamma, \Delta) \cup \mathrm{Voc}(\psi, \Gamma, \Delta)) \cap \mathrm{Voc}(\Gamma', \Delta') \\
&= \mathrm{Voc}(\varphi \vee \psi, \Gamma, \Delta) \cap \mathrm{Voc}(\Gamma', \Delta') && (3)
\end{aligned}$$

(1) and (3) hold since $\mathrm{Voc}(\varphi_1 \vee \varphi_2) = \mathrm{Voc}(\varphi_1) \cup \mathrm{Voc}(\varphi_2)$ and (2) holds by induction. We have $\vdash_{\mathsf{PK}} \varphi \vee \psi, \Gamma \Rightarrow \Delta, \theta$ and $\vdash_{\mathsf{PK}} \theta, \Gamma' \Rightarrow \Delta'$ as follows.

$$\dfrac{\dfrac{\overset{IH}{\varphi, \Gamma \Rightarrow \Delta, \theta_1}}{\varphi, \Gamma \Rightarrow \Delta, \theta} \vee_r^0 \quad \dfrac{\overset{IH}{\varphi, \Gamma \Rightarrow \Delta, \theta_2}}{\psi, \Gamma \Rightarrow \Delta, \theta} \vee_r^1}{\varphi \vee \psi, \Gamma \Rightarrow \Delta, \theta} \vee_l \qquad \dfrac{\overset{IH}{\theta_1, \Gamma' \Rightarrow \Delta'} \quad \overset{IH}{\theta_2, \Gamma' \Rightarrow \Delta'}}{\theta, \Gamma' \Rightarrow \Delta'} \vee_l$$

The interpolant for each case is summarised in Figure 4.1. The reader is encouraged to verify them. □

Remark 4.17. Cut-freeness is crucial for the proof since it is not clear how to obtain an interpolant for the conclusion of an instance of the cut from the interpolants of the premisses. Furthermore, note that our proof is constructive and it gives a *non-deterministic* algorithm to construct interpolants. However, it has been shown that it is not possible to use this algorithm to generate all possible interpolants.

Exercise 4.18. Verify Example 4.13 using the algorithm implicit in the proof of Lemma 4.15. Which interpolant do you find? Can you find another interpolant by Maehara's method?

Initial rule:

$$\text{init}\ \dfrac{}{;\varphi \xRightarrow{\top} ;\varphi} \qquad \text{init}\ \dfrac{}{\varphi; \xRightarrow{\varphi} ;\varphi} \qquad \text{init}\ \dfrac{}{;\varphi \xRightarrow{\neg\varphi} \varphi;} \qquad \text{init}\ \dfrac{}{\varphi; \xRightarrow{\bot} \varphi;}$$

Boolean rules:

$$\bot_l\ \dfrac{}{;\bot \xRightarrow{\top} ;} \qquad \bot_l\ \dfrac{}{\bot; \xRightarrow{\bot} ;} \qquad \top_r\ \dfrac{}{; \xRightarrow{\top} ;\top} \qquad \top_r\ \dfrac{}{; \xRightarrow{\bot} \top;}$$

Disjunction rules:

$$\vee_l\ \dfrac{\varphi, \Gamma; \Gamma' \xRightarrow{\theta_1} \Delta; \Delta' \quad \psi\Gamma; \Gamma' \xRightarrow{\theta_2} \Delta; \Delta'}{\varphi \vee \psi, \Gamma; \Gamma' \xRightarrow{\theta_1 \vee \theta_2} \Delta; \Delta'} \quad \vee_l\ \dfrac{\Gamma; \Gamma', \varphi \xRightarrow{\theta_1} \Delta; \Delta' \quad \Gamma, ; \Gamma', \psi \xRightarrow{\theta_2} \Delta; \Delta'}{\Gamma; \Gamma', \varphi \vee \psi \xRightarrow{\theta_1 \wedge \theta_2} \Delta; \Delta'}$$

$$\vee_r^0\ \dfrac{\Gamma, \Gamma' \xRightarrow{\theta} \varphi, \Delta; \Delta'}{\Gamma, \Gamma' \xRightarrow{\theta} \varphi \vee \psi, \Delta; \Delta'} \quad \vee_r^0\ \dfrac{\Gamma, \Gamma' \xRightarrow{\theta} \Delta; \Delta', \varphi}{\Gamma, \Gamma' \xRightarrow{\theta} \Delta; \Delta', \varphi \vee \psi} \quad \vee_r^1\ \dfrac{\Gamma, \Gamma' \xRightarrow{\theta} \psi, \Delta; \Delta'}{\Gamma, \Gamma' \xRightarrow{\theta} \varphi \vee \psi, \Delta; \Delta'} \quad \vee_r^1\ \dfrac{\Gamma, \Gamma' \xRightarrow{\theta} \Delta; \Delta', \psi}{\Gamma, \Gamma' \xRightarrow{\theta} \Delta; \Delta', \varphi \vee \psi}$$

Conjunction rules:

$$\wedge_l^0\ \dfrac{\varphi, \Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta'}{\varphi \wedge \psi, \Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta'} \quad \wedge_l^0\ \dfrac{\Gamma; \Gamma', \varphi \xRightarrow{\theta} \Delta; \Delta'}{\Gamma; \Gamma', \varphi \wedge \psi \xRightarrow{\theta} \Delta; \Delta'} \quad \wedge_l^1\ \dfrac{\psi, \Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta'}{\varphi \wedge \psi, \Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta'} \quad \wedge_l^1\ \dfrac{\Gamma; \Gamma', \psi \xRightarrow{\theta} \Delta; \Delta'}{\Gamma; \Gamma', \varphi \wedge \psi \xRightarrow{\theta} \Delta; \Delta'}$$

$$\wedge_r\ \dfrac{\Gamma; \Gamma' \xRightarrow{\theta_1} \varphi, \Delta; \Delta' \quad \Gamma; \Gamma' \xRightarrow{\theta_2} \psi, \Delta; \Delta'}{\Gamma; \Gamma' \xRightarrow{\theta_1 \vee \theta_2} \varphi \wedge \psi, \Delta; \Delta'} \quad \wedge_r\ \dfrac{\Gamma; \Gamma' \xRightarrow{\theta_1} \Delta; \Delta', \varphi \quad \Gamma; \Gamma' \xRightarrow{\theta_2} \Delta; \Delta', \psi}{\Gamma; \Gamma' \xRightarrow{\theta_1 \wedge \theta_2} \Delta; \Delta', \varphi \wedge \psi}$$

Negation rules:

$$\neg_l\ \dfrac{\Gamma; \Gamma' \xRightarrow{\theta} \varphi, \Delta; \Delta'}{\neg\varphi, \Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta'} \quad \neg_l\ \dfrac{\Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta', \varphi}{\Gamma; \Gamma', \neg\varphi \xRightarrow{\theta} \Delta; \Delta'} \quad \neg_r\ \dfrac{\varphi, \Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta'}{\Gamma; \Gamma' \xRightarrow{\theta} \neg\varphi, \Delta; \Delta'} \quad \neg_r\ \dfrac{\Gamma; \Gamma', \varphi \xRightarrow{\theta} \Delta; \Delta'}{\Gamma; \Gamma' \xRightarrow{\theta} \Delta; \Delta', \neg\varphi}$$

Figure 4.1: Construction of interpolants of split sequents in PK.

Chapter 5

Cut elimination

The proof of cut elimination is quite involved and is probably one of the trickiest termination arguments in all of graduate maths. One of the difficulties stems from the fact that the cut rule is not derivable (Proposition 3.4).

"The cut rule is not a derivable rule in the system obtained from LK by deleting the cut rule. That is, it is impossible to replace the cut rule in a uniform way by repeated applications of other rules, as each application of the cut rule will play a different role in a given proof. Therefore, we have to eliminate the cut rule depending on how it is applied." [Ono98]

5.1 The need for a syntactic proof

The completeness of first-order logic implicitly gives us cut admissibility. In particular, given $\models \Gamma \Rightarrow \Delta$, Schütte's proof [Sch77] of the theorem gives a *cut-free proof* of $\Gamma \Rightarrow \Delta$. So, given a proof π of $\Gamma \Rightarrow \Delta$ (possibly with cuts), going through soundness and completeness as black boxes, we magically obtain a cut-free proof π_0 of $\Gamma \Rightarrow \Delta$.

Can we demystify this black box that inputs π and produces π_0? Can we see this as a procedure? Given a different proof π' of the same endsequent, does it produce a different cut-free proof π_0'? Unfortunately, not! Any proof of completeness is inherently non-constructive and no information of π is retained. However, we can give more direct proofs of cut elimination that are more *procedural*. These sorts of proofs are more informative:

1. by the proofs vs programs correspondence, the cut elimination procedure on π corresponds to evaluating the program corresponding to π;
2. the size of π gives an upper bound on the size of π_0.

One can now see that if π and π' correspond to different programs or are of different sizes, then $\pi_0 \neq \pi_0'$.

Remark 5.1. For the rest of this chapter, we will construe cedents as multisets (rather than lists). A multiset is a collection of objects in which elements may occur more than once, but in which the order does not matter. So applications of rule ex will be implicit.

5.2 Cut elimination as a rewriting system

To obtain a constructive proof, we will define a *rewriting system* over proofs such that cut-free proofs will be *normal forms* and cut elimination will correspond to *weak normalisation i.e.* starting from a proof, we will give a strategy for transforming it into a cut-free proof into finitely many steps. See Appendix A.3 for background on rewriting theory.

What is the most trivial situation when we can immediately get rid of a cut?[1]

$$\text{cut}\ \dfrac{\text{init}\ \dfrac{}{\varphi \Rightarrow \varphi} \qquad \overset{\pi}{\varphi, \Gamma \Rightarrow \Delta}}{\varphi, \Gamma \Rightarrow \Delta} \qquad \rightsquigarrow_{\text{cut}} \qquad \overset{\pi}{\varphi, \Gamma \Rightarrow \Delta}$$

Obviously, not all cuts appear in this format. What can we do then? We can *simplify* cuts *i.e.* we can replace cuts on complex formulas with cuts on simpler formulas.

Definition 5.2. The **degree** $d(\varphi)$ of a formula φ is defined inductively as follows.

$$\begin{aligned} d(a) &:= 0 && \text{if } a \in \mathcal{A} \\ d(\neg\varphi) &:= d(\varphi) + 1 && \\ d(\varphi \circ \psi) &:= \max(d(\varphi), d(\psi)) + 1 && \text{for } \circ \in \{\wedge, \vee\} \\ d(\mathcal{Q}x\varphi) &:= d(\varphi) + 1 && \text{for } \mathcal{Q} \in \{\forall, \exists\} \end{aligned}$$

The degree d of an instance of the cut rule is the degree of the cut formula.

$$\text{cut}\ \dfrac{\vee_r^0\ \dfrac{\overset{\pi}{\Gamma \Rightarrow \Delta, \varphi}}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \qquad \vee_l\ \dfrac{\overset{\pi'}{\varphi, \Gamma' \Rightarrow \Delta'} \quad \overset{\pi''}{\psi, \Gamma' \Rightarrow \Delta'}}{\varphi \vee \psi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \qquad \rightsquigarrow_{\text{cut}} \qquad \text{cut}\ \dfrac{\overset{\pi}{\Gamma \Rightarrow \Delta, \varphi} \quad \overset{\pi'}{\varphi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Clearly, the cut degree decreases. Moreover, note that the subproof π'' is deleted. If the rule on the cut formula was $\vee_r^1$ instead of $\vee_r^0$, then π' would be deleted and π'' would be retained.

[1] Throughout the rest of this chapter, cut formulas and their subformulas will be distinguished in magenta and cyan.

This is an instance of a *key case* of cut elimination (where cuts get simplified). Depending on the outermost operator of the cut formula and the rule applied on it, there are several key cases.

Exercise 5.3. Suppose we have the following where the principal formula in rules $\circ_l$ and $\circ_r$ is φ.

$$\text{cut}\ \dfrac{\circ_r\,\dfrac{\cdots}{\Gamma \Rightarrow \Delta, \varphi} \qquad \circ_l\,\dfrac{\cdots}{\varphi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Write the key case for the following instances:

1. $\varphi = \neg\psi$ and $\circ = \neg$
2. $\varphi = \exists x\psi$ and $\circ = \exists$

However, it might not always be the case that the cut formulas are principal immediately. Consequently, we need some *commutation cases*. For instance, the following is a commutation of $\vee_r^0$ with cut.

$$\text{cut}\ \dfrac{\begin{matrix}\pi\\ \vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{matrix} \qquad \vee_r^0\,\dfrac{\begin{matrix}\pi'\\ \vdots\\ \varphi, \Gamma' \Rightarrow \Delta', \psi_0\end{matrix}}{\varphi, \Gamma' \Rightarrow \Delta', \psi_0 \vee \psi_1}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi_0 \vee \psi_1} \quad \rightsquigarrow_{\text{cut}} \quad \vee_r^0\,\dfrac{\text{cut}\ \dfrac{\begin{matrix}\pi\\ \vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{matrix} \qquad \begin{matrix}\pi'\\ \vdots\\ \varphi, \Gamma' \Rightarrow \Delta', \psi_0\end{matrix}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi_0}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi_0 \vee \psi_1}$$

Not all commutation cases are so benign. For example, some commutation cases increase the total number of cuts and copies subproofs:

$$\text{cut}\ \dfrac{\begin{matrix}\pi\\ \vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{matrix} \qquad \wedge_r\,\dfrac{\begin{matrix}\pi_0\\ \vdots\\ \varphi, \Gamma' \Rightarrow \Delta', \psi_0\end{matrix} \qquad \begin{matrix}\pi_1\\ \vdots\\ \varphi, \Gamma' \Rightarrow \Delta', \psi_1\end{matrix}}{\varphi, \Gamma' \Rightarrow \Delta', \psi_0 \wedge \psi_1}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi_0 \wedge \psi_1} \quad \rightsquigarrow_{\text{cut}}$$

$$\wedge_r^0\,\dfrac{\text{cut}\ \dfrac{\begin{matrix}\pi\\ \vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{matrix} \qquad \begin{matrix}\pi_0\\ \vdots\\ \varphi, \Gamma' \Rightarrow \Delta', \psi_0\end{matrix}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi_0} \qquad \text{cut}\ \dfrac{\begin{matrix}\pi\\ \vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{matrix} \qquad \begin{matrix}\pi_1\\ \vdots\\ \varphi, \Gamma' \Rightarrow \Delta', \psi_1\end{matrix}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi_1}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta', \psi_0 \wedge \psi_1}$$

Note that in both of these reductions, the cut degree remained the same. What measure decreases in commutation steps?

Definition 5.4. The **left rank** r_l (**right rank** r_r respectively) of an instance of a cut is the maximum number of consecutive sequents from the left premisse (right premisse, respectively) of the cut such that they all contain the cut formula. The **rank** r of a cut rule is $r_l + r_r$.

In commutation steps, the rank decreases.

Remark 5.5. We will only treat first-order logic without equality in this chapter. In fact, it is not clear if cut elimination can be constructively proved with the equality rules we have presented. For example, in the following proof, it is neither possible to reduce the height of this cut nor the complexity of the cut formula in the standard manner. See [Ind24] for a detailed discussion.

$$\text{cut}\ \dfrac{=_l\ \dfrac{\varnothing \Rightarrow \Delta[s/t], s = u}{s = t \Rightarrow \Delta, t = u} \qquad =_l\ \dfrac{\Gamma[t/u] \Rightarrow \Sigma[t/u]}{t = u, \Gamma \Rightarrow \Sigma}}{s = t, \Gamma \Rightarrow \Delta, \Sigma}$$

5.3 The problem with structural rules

One key case we have not accounted for till now is when a cut formula is principal in a structural rule. We have the following (quite natural) rewrite rules:

$$\text{cut}\ \dfrac{\overset{\pi}{\Gamma \Rightarrow \Delta, \varphi} \qquad \text{w}_l\ \dfrac{\overset{\pi'}{\Gamma' \Rightarrow \Delta'}}{\varphi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \rightsquigarrow_{\text{cut}} \quad \text{w}_l^*,\text{w}_r^*\ \dfrac{\overset{\pi'}{\Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

$$\text{cut}\ \dfrac{\overset{\pi}{\Gamma \Rightarrow \Delta, \varphi} \qquad \text{c}_l\ \dfrac{\overset{\pi'}{\varphi, \varphi, \Gamma' \Rightarrow \Delta'}}{\varphi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \rightsquigarrow_{\text{cut}} \quad \text{c}_l^*,\text{c}_r^*\ \dfrac{\text{cut}\ \dfrac{\overset{\pi}{\Gamma \Rightarrow \Delta, \varphi} \qquad \text{cut}\ \dfrac{\overset{\pi}{\Gamma \Rightarrow, \Delta, \varphi} \quad \overset{\pi'}{\varphi, \varphi, \Gamma' \Rightarrow \Delta'}}{\varphi, \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}}{\Gamma, \Gamma, \Gamma' \Rightarrow \Delta, \Delta, \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

However, these rules immediately pose a problem: they render the rewrite system non-confluent and non-terminating respectively. Consider the following two rewritings.

$$\text{w}_l^*,\text{w}_r^*\ \dfrac{\overset{\pi}{\Gamma \Rightarrow \Delta}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \leftsquigarrow_{\text{cut}} \quad \text{cut}\ \dfrac{\text{w}_r\ \dfrac{\overset{\pi}{\Gamma \Rightarrow \Delta}}{\Gamma \Rightarrow \Delta, \varphi} \qquad \text{w}_l\ \dfrac{\overset{\pi'}{\Gamma' \Rightarrow \Delta'}}{\varphi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \rightsquigarrow_{\text{cut}} \quad \text{w}_l^*,\text{w}_r^*\ \dfrac{\overset{\pi'}{\Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

This is known as **Lafont's counterexample** and shows that cut elimination is non-confluent and cannot be a meaningful basis for the identity of proofs since that would equate all proofs.

Exercise 5.6 (Failure of strong normalisation).
Consider the following cut elimination step.

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{a \Rightarrow a}\,\mathsf{init}}{a \Rightarrow a, \varphi, \varphi}\,\mathsf{w}_r^2}{a \Rightarrow a, \varphi}\,\mathsf{c}_r \qquad \dfrac{\dfrac{\dfrac{}{b \Rightarrow b}\,\mathsf{init}}{\varphi, \varphi, b \Rightarrow b}\,\mathsf{w}_l^2}{\varphi, b \Rightarrow b}\,\mathsf{c}_l}{a, b \Rightarrow a, b}\,\mathsf{cut}
\quad \rightsquigarrow_{\mathsf{cut}} \quad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \Rightarrow a}\,\mathsf{init}}{a \Rightarrow a, \varphi, \varphi}\,\mathsf{w}_r^2}{a \Rightarrow a, \varphi}\,\mathsf{c}_r \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{a \Rightarrow a}\,\mathsf{init}}{a \Rightarrow a, \varphi, \varphi}\,\mathsf{w}_r^2}{a \Rightarrow a, \varphi}\,\mathsf{c}_r \qquad \dfrac{\dfrac{}{b \Rightarrow b}\,\mathsf{init}}{\varphi, \varphi, b \Rightarrow b}\,\mathsf{w}_l^2}{\varphi, a, b \Rightarrow a, b}\,\mathsf{cut}}{a, a, b \Rightarrow a, a, b}\,\mathsf{cut}}{a, b \Rightarrow a, b}\,\mathsf{c}_l, \mathsf{c}_r
$$

There are several options for the next step. Show that:

1. there exists a non-terminating rewriting sequence. (Hint: show that one can always choose a cut to interact with a contraction to get larger and larger proofs).
2. there exists a terminating rewriting sequence.

There are two ways to deal with non-confluence and non-termination.

- On one hand, one can construe these to be features and not bugs. In order, to obtain weak normalisation in the presence of possible non-termination, one needs to impose *normalisation strategies* that would ensure that following the strategy from any proof, one can obtain a cut-free proof in finitely many steps. Several strategies have been explored in the literature: for example, *always reducing the top-most cut*, *always reducing the most complex cut*, and so on.
- On the other hand, one can seek to rectify these 'defects'. Gentzen introduced a generalised cut rule (called 'mix') to solve this issue.

$$
\mathsf{mix}\,\dfrac{\Gamma \Rightarrow \Delta, \overbrace{\varphi, \varphi, \ldots, \varphi}^{m\text{-times}} \qquad \overbrace{\varphi, \varphi, \ldots, \varphi}^{n\text{-times}}, \Gamma' \Rightarrow \Delta'}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \qquad (m, n \geq 0 \text{ and } \varphi \notin \Delta \cup \Gamma')
$$

  $\mathsf{LK} \setminus \{\mathsf{cut}\} \cup \{\mathsf{mix}\}$ is strongly normalising. The proof is beyond the scope of these notes.

Remark 5.7. We will use φ^m to denote m occurrences of φ.

Exercise 5.8. Show that mix is derivable in LK.

In the following section, we will show weak normalisation of LK with respect to mix. The use of mix is convenient mostly because it provides an elegant way to deal with contraction rules.

5.4 Putting everything together

We will fix a cut-reduction strategy and design a measure that will decrease with each step of reduction. In particular, we will eliminate *top-most* mix rules *i.e.* given a proof π, we will consider subproofs of π of following shape (where π_l and π_r are mix-free):

$$
\begin{prooftree}
\AxiomC{π_l}
\noLine
\UnaryInfC{$\Gamma \Rightarrow \Delta, \varphi^m$}
\AxiomC{π_r}
\noLine
\UnaryInfC{$\varphi^n, \Gamma' \Rightarrow \Delta'$}
\LeftLabel{mix}
\RightLabel{$m, n \geq 0$ and $\varphi \notin \Delta \cup \Gamma'$}
\BinaryInfC{$\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$}
\end{prooftree}
$$

Recall, in *key* reduction steps, $m = n = 1$, the cut formula is principal in both the left and right premise of the mix rules and the degree will reduce. In *commutation* reduction steps, the degree remains the same and the rank reduces.[2]

Remark 5.9. For each top-most mix rule we have $r \geq 2$, because the cut formula occurs at least once in the left premise ($r_l \geq 1$) and at least once in the right premise ($r_r \geq 1$).

Example 5.10.

$$
\begin{prooftree}
\AxiomC{}
\LeftLabel{init}
\UnaryInfC{$a \Rightarrow a$}
\LeftLabel{$\wedge_l^0$}
\UnaryInfC{$a \wedge b \Rightarrow a$}
\LeftLabel{$\vee_r^0$}
\UnaryInfC{$a \wedge b \Rightarrow \color{blue}{a \vee \neg c}$}
\AxiomC{}
\LeftLabel{init}
\UnaryInfC{$\neg c \Rightarrow \neg c$}
\LeftLabel{$\vee_r^1$}
\UnaryInfC{$\neg c \Rightarrow \color{blue}{a \vee \neg c}$}
\LeftLabel{$\wedge_l^0$}
\UnaryInfC{$\neg c \wedge d \Rightarrow \color{blue}{a \vee \neg c}$}
\LeftLabel{$\vee_l$}
\BinaryInfC{$(a \wedge b) \vee (\neg c \wedge d) \Rightarrow \color{blue}{a \vee \neg c}$}
\AxiomC{}
\LeftLabel{init}
\UnaryInfC{$a \Rightarrow a$}
\LeftLabel{$\vee_r^{0*}$}
\doubleLine
\UnaryInfC{$a \Rightarrow a \vee b \vee \neg c$}
\AxiomC{}
\LeftLabel{init}
\UnaryInfC{$\neg c \Rightarrow \neg c$}
\LeftLabel{$\vee_r^{1*}$}
\doubleLine
\UnaryInfC{$\neg c \Rightarrow a \vee b \vee \neg c$}
\LeftLabel{$\vee_l$}
\BinaryInfC{$\color{blue}{a \vee \neg c} \Rightarrow a \vee b \vee \neg c$}
\LeftLabel{mix}
\BinaryInfC{$(a \wedge b) \vee (\neg c \wedge d) \Rightarrow a \vee b \vee \neg c$}
\end{prooftree}
$$

The cut formula is $a \vee \neg c$ and so we have degree $d = 2$. For the rank we trace the cut formulas upwards as indicated in blue. We see that $r_l = 3$ and $r_r = 1$, and so we have rank $r = 4$.

Lemma 5.11 (Mix reduction lemma). *Let π be a proof of the form*

$$
\begin{prooftree}
\AxiomC{π_l}
\noLine
\UnaryInfC{$\Gamma \Rightarrow \Delta, \varphi^m$}
\AxiomC{π_r}
\noLine
\UnaryInfC{$\varphi^n, \Gamma' \Rightarrow \Delta'$}
\LeftLabel{mix}
\BinaryInfC{$\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$}
\end{prooftree}
$$

where π_0 and π_1 do not contain mix. *There is a reduction strategy that takes π to a proof π' of the same end-sequent $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ which does not contain* mix *rules.*

[2] Degree and rank is generalised straightforwardly to mix.

Proof. Let d denote the degree of the mix rule in π and let r its rank. Below we define each reduction step and we prove that each step reduces by induction on the lexicographic order of (d, r), *i.e.* either the degree reduces, or the degree stays the same and the rank reduces. We distinguish between the following situations:

1. $r = 2$. In this case we define reduction rules that reduce d. When a logical rule is applied, the reduction step will be a *key* reduction step.
2. $r > 2$. In this case we define reduction rules that keep d the same and reduce r. Here we distinguish between $r_l > 1$ or $r_r > 1$. The reduction steps will be *commutation* steps.

Case 1 ($r = 2$): This means that $n = m = 1$ and φ is principal in both premises. There are different cases depending on the last rule applied in π_l and π_r. We treat some cases:

- Suppose w_l is applied to the right premise. The reduction is as follows:

$$\mathsf{mix}\;\dfrac{\dfrac{\pi_l}{\Gamma \Rightarrow \Delta, \varphi} \qquad \mathsf{w}_l\;\dfrac{\dfrac{\pi'}{\Gamma' \Rightarrow \Delta'}}{\varphi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \rightsquigarrow_{\mathsf{cut}} \quad \mathsf{w}_l^*,\mathsf{w}_r^*\;\dfrac{\dfrac{\pi'}{\Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

  This results in a proof without mix.
- Suppose $\neg\psi$ is the cut formula principal in $\neg_r$ and $\neg_l$ in the left and right premise of the mix respectively. This results in the following *key* reduction step:

$$\mathsf{mix}\;\dfrac{\neg_r\;\dfrac{\dfrac{\pi'}{\psi, \Gamma \Rightarrow \Delta}}{\Gamma \Rightarrow \Delta, \neg\psi} \qquad \neg_l\;\dfrac{\dfrac{\pi''}{\Gamma' \Rightarrow \Delta', \psi}}{\neg\psi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \rightsquigarrow_{\mathsf{cut}} \quad \mathsf{w}_l^*,\mathsf{w}_r^*\;\dfrac{\mathsf{mix}\;\dfrac{\dfrac{\pi''}{\Gamma' \Rightarrow \Delta', \psi} \qquad \dfrac{\pi'}{\psi, \Gamma \Rightarrow \Delta}}{\Gamma^-, \Gamma' \Rightarrow \Delta, \Delta'^-}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

  where Γ^- and Δ' denote the multisets Γ and Δ respectively but without occurrences of ψ. Similarly for Δ'^-. The new mix rule has a smaller induction parameter. Indeed the cut degree is smaller than d which suffices to apply the induction hypothesis.
- Suppose $\forall x\psi$ is the cut formula and derived by $\forall_r$ and $\forall_l$. The *key* reduction is defined as follows:

$$\mathsf{mix}\;\dfrac{\forall_r\;\dfrac{\dfrac{\pi'[y]}{\Gamma \Rightarrow \Delta, \psi[y/x]}}{\Gamma \Rightarrow \Delta, \forall x\psi} \qquad \forall_l\;\dfrac{\dfrac{\pi''}{\psi[t/x], \Gamma' \Rightarrow \Delta'}}{\forall x\psi, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \rightsquigarrow_{\mathsf{cut}}$$

$$
\dfrac{\dfrac{\overset{\pi'[t]}{\Gamma \Rightarrow \Delta, \psi[t/x]} \qquad \overset{\pi''}{\psi[t/x], \Gamma' \Rightarrow \Delta'}}{\Gamma^-, \Gamma' \Rightarrow \Delta, \Delta'^-}\,\text{mix}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\,\mathsf{w}_l^*, \mathsf{w}_r^*
$$

where Γ^- and Δ'^- denote the multisets Γ and Δ respectively but without occurrences of $\psi[t/x]$. The notation $\pi'[y]$ means the proof where we indicate the fresh variable y of $\forall_r$. Since y is fresh, substituting any term s into its proof yield another valid proof $\pi'[s]$. Here we substitute t obtained from the right premise. The cut degree is smaller than d which suffices to apply the induction hypothesis.

Case 2a ($r_r > 1$): We distinguish between the cases in which cut formula φ occurs in the antecedent of the left premise or not.

If yes, we have the following reduction:

$$
\dfrac{\overset{\pi_l}{\varphi, \Gamma \Rightarrow \Delta, \varphi^m} \qquad \overset{\pi_r}{\varphi^n, \Gamma' \Rightarrow \Delta'}}{\varphi, \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\,\text{mix} \qquad \rightsquigarrow_{\text{cut}} \qquad \dfrac{\dfrac{\overset{\pi_r}{\varphi^n, \Gamma' \Rightarrow \Delta'}}{\varphi^n, \varphi, \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\,\mathsf{w}_l^*, \mathsf{w}_r^*}{\varphi, \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}\,\mathsf{c}_l^*
$$

This results in a proof without mix.

If not, we consider all possible rules applied to the right premise of mix. The principal formula might be among the cut formulas but does not need to be. We consider rules $\wedge_l$ and c_l, and leave the remaining cases to the reader.

- Suppose $\wedge_l$ is applied to the right premise with principal formula $\psi_0 \wedge \psi_1$. There are multiple cases depending on the shape of φ:
  - If $\varphi \neq \psi_0 \wedge \psi_1$, the proof looks as follows

$$
\dfrac{\overset{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \qquad \dfrac{\overset{\pi'}{\varphi^n, \Gamma', \psi_0 \Rightarrow \Delta'}}{\varphi^n, \Gamma', \psi_0 \wedge \psi_1 \Rightarrow \Delta'}\,\wedge_l^0}{\Gamma, \Gamma', \psi_0 \wedge \psi_1 \Rightarrow \Delta, \Delta'}\,\text{mix}
$$

which reduces to either of the following depending on the shape of φ:

$$
\text{If } \varphi \neq \psi_0 : \qquad \rightsquigarrow_{\text{cut}} \qquad \dfrac{\dfrac{\overset{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \qquad \overset{\pi'}{\varphi^n, \Gamma', \psi_0 \Rightarrow \Delta'}}{\Gamma, \Gamma', \psi_0 \Rightarrow \Delta, \Delta'}\,\text{mix}}{\Gamma, \Gamma', \psi_0 \wedge \psi_1 \Rightarrow \Delta, \Delta'}\,\wedge_l^0
$$

If $\varphi = \psi_0$: $\rightsquigarrow_{\text{cut}}$
$$\dfrac{\text{mix}\ \dfrac{\overset{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \quad \overset{\pi'}{\varphi^n, \Gamma', \psi_0 \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}}{\Gamma, \Gamma', \psi_0 \wedge \psi_1 \Rightarrow \Delta, \Delta'}\ \text{w}_l$$

In both cases, the created mix rule has the same degree as d, but its rank is smaller than r. This justifies the reduction steps.

- If $\varphi = \psi_0 \vee \psi_1$ the proof to be reduced looks as follows, where $\psi_0 \vee \psi_1$ does not occur in Γ':

$$\text{mix}\ \dfrac{\overset{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \quad \wedge_l^0\ \dfrac{\overset{\pi'}{\varphi^n, \Gamma', \psi_0 \Rightarrow \Delta'}}{\varphi^n, \Gamma', \psi_0 \wedge \psi_1 \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

We define the following reduction:

$$\rightsquigarrow_{\text{cut}} \quad \text{c}_l,\text{c}_r\ \dfrac{\text{mix}\ \dfrac{\overset{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \quad \wedge_l\ \dfrac{\text{mix}\ \dfrac{\overset{\pi'}{\Gamma \Rightarrow \Delta, \varphi^m} \quad \overset{\pi'}{\varphi^n, \Gamma', \psi_0 \Rightarrow \Delta'}}{\Gamma, \Gamma', \psi_0 \Rightarrow \Delta, \Delta'}}{\Gamma, \Gamma', \psi_0 \wedge \psi_1 \Rightarrow \Delta, \Delta'}}{\Gamma, \Gamma, \Gamma' \Rightarrow \Delta, \Delta, \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

To justify the reduction we have to take into account two mix rules. We first argue that the upper mix rule can be replaced by a mix-free subproof. This is the case because the degree is the same as d, but its rank is lower than r. So by induction hypothesis there exists a mix-free subproof of $\Gamma, \Gamma', \psi_0 \wedge \psi_1 \Rightarrow \Delta, \Delta'$. This allows us to examine the other mix rule. Observe that again the cut degree remains the same. The cut rank is lower, because its right rank is 1 as $\psi_0 \wedge \psi_1 \notin \Gamma$ by assumption and $\psi_0 \wedge \psi_1 \notin \Gamma'$ by definition of the upper mix rule. So the total rank is $r_l + 1$, which is smaller than $r = r_l + r_r$ since we assumed $r_r > 1$. Therefore, the induction hypothesis also applies to the lower mix rule.

- Suppose rule c_l is applied to the right premise with principal formula ψ. There are two cases:

- If $\varphi \neq \psi$ the proof and reduction look as follows:

$$\text{mix}\ \dfrac{\overset{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \quad \text{c}_l\ \dfrac{\overset{\pi'}{\varphi^n, \Gamma', \psi, \psi \Rightarrow \Delta'}}{\varphi^n, \Gamma', \psi \Rightarrow \Delta'}}{\Gamma, \Gamma', \psi \Rightarrow \Delta, \Delta'} \rightsquigarrow_{\text{cut}} \text{c}_l\ \dfrac{\text{mix}\ \dfrac{\overset{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \quad \overset{\pi'}{\varphi^n, \Gamma', \psi, \psi \Rightarrow \Delta'}}{\Gamma, \Gamma', \psi, \psi \Rightarrow \Delta, \Delta'}}{\Gamma, \Gamma', \psi \Rightarrow \Delta, \Delta'}$$

The degree of mix remains the same as d, but the rank is smaller than r.
- If $\varphi = \psi$ the proof and reduction look as follows:

$$\text{mix}\ \dfrac{\dfrac{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \qquad c_l\ \dfrac{\dfrac{\pi'}{\varphi^n, \Gamma', \psi, \psi \Rightarrow \Delta'}}{\varphi^n, \Gamma', \psi \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'} \quad \rightsquigarrow_{\text{cut}} \quad \text{mix}\ \dfrac{\dfrac{\pi_l}{\Gamma \Rightarrow \Delta, \varphi^m} \qquad \dfrac{\pi'}{\varphi^n, \Gamma', \psi, \psi \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Again, the degree remains the same, but the rank reduces.

Case 2b ($r_l > 1$): This case is symmetric to the **Case 2a**, so we will not go into further detail.

□

Theorem 5.12 (Mix elimination theorem)**.** *Every proof π can be transformed to a proof π' without* mix *rules that proves the same endsequent as π.*

Proof. Let k be the number of mix rules in π. Take a top-most mix rule in π. By Lemma 5.11 we can eliminate this mix rule resulting in a proof π' proving the same end sequent but with $k-1$ mix rules. Repeating this process k times, we obtain a proof of the same endsequent that does not contain any mix rule. □

We can analyse the blow-up in size of the proof in the mix reduction lemma, and obtain the following result. (The degree of a proof is the maximum degree of a mix in it.)

Theorem 5.13. *Given a proof of height k and degree n, one construct a cut-free proof of height less than $T(n,k)$ where $T(0,k) = k$ and $T(m+1,k) = 4^{T(m,k)}$.*

Appendix A

Additional background

A.1 Capture-avoiding substitution

A substitution $\varphi[t/x]$ denotes the operation of substituting all free occurrences of variable x with term t. However, $y \in \mathrm{FV}(t)$ may become bound by a quantifier $\forall y$ or $\exists y$ in φ. To take a concrete example, suppose $\varphi = \exists y(P(y,x) \wedge \neg P(x,x))$. Note that $\forall x \varphi$ is satisfiable. Naively substituting y for x in φ would result in $\varphi[y/x] = \exists y(P(y,y) \wedge \neg P(y,y))$ which is not satisfiable. To maintain meaningful invariants under substitutions, we define capture-avoiding substitutions.

Definition A.1. We define **capture avoiding substitution** $\varphi[t/x]$ by induction on φ. Notation $x \sim y$ denotes that x and y are syntactically the same variable.

$$
\begin{aligned}
y[t/x] &:= \begin{cases} t & \text{if } y \sim x \\ y & \text{if } y \nsim x \end{cases} \\
f(t_1,\dots,t_n)[t/x] &:= f(t_1[t/x],\dots,t_n[t/x]) \\
(t_1 = t_2)[t/x] &:= t_1[t/x] = t_2[t/x] \\
P(t_1,\dots,t_n)[t/x] &:= P(t_1[t/x],\dots,t_n[t/x]) \\
\bot[t/x] &:= \bot \text{ and } \top[t/x] := \top \\
(\neg\varphi)[t/x] &:= \neg\varphi[t/x] \\
(\varphi \circ \psi)[t/x] &:= \varphi[t/x] \circ \psi[t/x] \\
(Qy\varphi)[t/x] &:= \begin{cases} Qx\varphi & \text{if } y \sim x \\ Qy\varphi[t/x] & \text{if } y \nsim x \text{ and } y \notin \mathrm{FV}(t) \\ Qz(\varphi[z/y])[t/x] & \text{if } y \nsim x \text{ and } y \in \mathrm{FV}(t) \text{ where } z \text{ is fresh} \end{cases}
\end{aligned}
$$

where $\circ \in \{\wedge, \vee\}$, $Q \in \{\exists, \forall\}$.

Example A.2. Let $\varphi = \exists y(P(y,x) \land \neg P(x,x))$. Then, $\varphi[y/x] = \exists z(P(z,y) \land \neg P(y,y))$.

Proposition A.3. *Let $\exists x\varphi$ be a formula such that the variable y does not occur in it. Then $\vdash_{\mathsf{LK}} \exists x\varphi \equiv \exists y(\varphi[y/x])$.*

The symmetric result holds for $\forall x\varphi$.

Corollary A.4. *For any formula φ, there exists ψ such that $\mathrm{FV}(\psi) \cap \mathrm{BV}(\psi) = \varnothing$ and $\vdash_{\mathsf{LK}} \varphi \equiv \psi$.*

A.2 First-order theories

Definition A.5. Fix a signature σ. A **first-order theory** T of σ is a set of σ-sentences. A first-order structure that satisfies all sentences in T is said to be a **model** of T. If T is finite or recursively enumerable, it is said to be **effective**.

Example A.6. Let $\sigma = (\{=\}, \{\circ\})$ where $\circ$ is a binary function symbol. Let T be the set of the following sentences.

$$\forall x \forall y \exists z(\circ(x,y) = z)$$
$$\forall x \forall y \forall z(\circ(\circ(x,y),z) = \circ(x, \circ(y,z)))$$
$$\exists e \forall x(\circ(x,e) = x \land \circ(e,x) = x)$$

T represents the theory of monoids. Similarly, we have first-order theories of other algebraic structures such as groups, abelian groups, rings, and so on. Two of the most important first-order theories in logic are *Peano arithmetic* and *Zermelo-Frankel set theory*.

Definition A.7. Let T be a first-order theory and φ be a first-order sentence. We say that φ is a **syntactic consequence** of T, denoted $T \vdash \varphi$, if φ is provable in LK possibly using sentences in T as axioms. We say that φ is a **semantic consequence** of T, denoted $T \models s$, if φ holds in every model of T.

Gödel's completeness can be strengthened to any first-order theory.

Theorem A.8 (Strong completeness)**.** *If $T \models \varphi$ then $T \vdash \varphi$*

Corollary A.9 (Compactness)**.** *Let T be a theory. Then T has a model if and only if each finite set $T' \subseteq T$ has a model.*

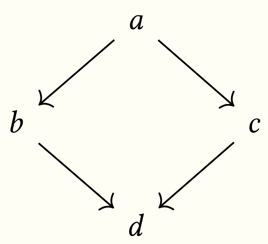
Proof. The left to right is immediate. In the other direction, we reason by contraposition. Suppose T has no model. Then, $T \models \bot$. By Theorem A.8, $T \vdash \bot$. Let T' be the set of sentences in T used in this proof. Clearly, T' is finite and $T' \vdash \bot$. By soundness, we obtain $T' \models \bot$. □

A.3 Rewriting theory

An **abstract rewrite system** $\mathcal{A}$ consists of a set of rules Φ defined on a particular set of objects A, which in most cases consists of a language of terms. The rules of the system determine how an object a can be rewritten into b (denoted $a \longrightarrow b$). Rewriting theory comes with its own set of bespoke terminology.

Definition A.10. Let $\mathcal{A} = (A, \Phi)$ be an abstract rewrite system.

1. Every element $a \in A$ is called a **normal form** of A if there is no $b \in A$ such that $a \longrightarrow b$.
2. $\mathcal{A}$ has the **diamond property** (DP) if $\longleftarrow \circ \longrightarrow \subseteq \longrightarrow \circ \longleftarrow$ *i.e.* for all $a, b, c \in A$ there exists $d \in A$ such that the following holds.



3. $\mathcal{A}$ is **confluent** (CR) if ${}^*\!\longleftarrow \circ \longrightarrow^* \subseteq \longrightarrow^* \circ {}^*\!\longleftarrow$.
4. $\mathcal{A}$ is **terminating** or **(strongly) normalising** (SN) if there is no infinite reduction sequences.
5. $\mathcal{A}$ is **(weakly) normalising** (WN) if every element in A reduces to a normal form.

See [Ter03] for more details.

Bibliography

[Coo71] Stephen A. Cook. "The complexity of theorem-proving procedures". In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing*. STOC '71. Shaker Heights, Ohio, USA: Association for Computing Machinery, 1971, pp. 151–158. ISBN: 9781450374644. DOI: 10.1145/800157.805047. URL: https://doi.org/10.1145/800157.805047 (cit. on p. 5).

[Her73] Hans Hermes. *Introduction to Mathematical Logic*. Springer Berlin Heidelberg, 1973. ISBN: 9783642871320. DOI: 10.1007/978-3-642-87132-0. URL: http://dx.doi.org/10.1007/978-3-642-87132-0 (cit. on p. 13).

[Ind24] Andrzej Indrzejczak. "The Logicality of Equality". In: *Peter Schroeder-Heister on Proof-Theoretic Semantics*. Ed. by Thomas Piecha and Kai F. Wehmeier. Cham: Springer Nature Switzerland, 2024, pp. 211–238. ISBN: 978-3-031-50981-0. DOI: 10.1007/978-3-031-50981-07. URL: https://doi.org/10.1007/978-3-031-50981-07 (cit. on p. 31).

[Joh87] Peter T Johnstone. *Notes on logic and set theory*. Cambridge University Press, 1987 (cit. on p. 8).

[Kle52] Stephen Cole Kleene. *Introduction to metamathematics*. Elsevier Science Inc., 1952 (cit. on p. 8).

[Lev73] Leonid Anatolevich Levin. "Universal sequential search problems". In: *Problemy Peredachi Informatsii* 9.3 (1973), pp. 115–116 (cit. on p. 5).

[Ono98] Hiroakira Ono. "Proof-theoretic methods in nonclassical logic–an introduction". In: *Theories of types and proofs* 2 (1998), pp. 207–254 (cit. on p. 28).

[Ore82] Vladimir P Orevkov. "Lower bounds for increasing complexity of derivations after cut elimination". In: *Journal of Soviet Mathematics* 20 (1982), pp. 2337–2350 (cit. on p. 19).

[Sch77] K Schutte. *Proof Theory*. en. Grundlehren der Mathematischen Wissenschaften. Berlin, Germany: Springer, Sept. 1977 (cit. on p. 28).

[Sta79] Richard Statman. “Lower bounds on Herbrand’s theorem”. In: *Proceedings of the American Mathematical Society* 75.1 (1979), pp. 104–107 (cit. on p. 19).

[SU06] Morten Heine Sørensen and Pawel Urzyczyn. *Lectures on the Curry-Howard Isomorphism.* Vol. 149 (Studies in Logic and the Foundations of Mathematics). Elsevier Science Inc., 2006 (cit. on p. 6).

[Ter03] Terese. *Cambridge tracts in theoretical computer science: Term rewriting systems series number 55.* en. Cambridge tracts in theoretical computer science. Cambridge, England: Cambridge University Press, Mar. 2003 (cit. on p. 40).

[Tra50] Boris A Trakhtenbrot. “Impossibility of an algorithm for the decision problem for finite classes”. In: *Doklady Akademiia Nauk SSSR.* Vol. 70. 1950, p. 569 (cit. on p. 10).

[vBen08] Johan van Benthem. “The many faces of interpolation”. In: *Synthese* 164.3 (July 2008), pp. 451–460. ISSN: 1573-0964. DOI: 10.1007/s11229-008-9351-5. URL: http://dx.doi.org/10.1007/s11229-008-9351-5 (cit. on p. 24).