DISSERTATION

Characteristic Clause Sets and Proof Transformations

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der technischen Wissenschaften unter der Leitung von

Univ.Prof. Dr.phil. Alexander Leitsch
Institut für Computersprachen
Theoretische Informatik und Logik

eingereicht an der

Technischen Universität Wien
Fakultät für Informatik

von

Dipl.-Ing. Stefan Hetzl
Matrikelnummer: 9925353
Langackergasse 11b/2/2
A-1190 Wien

Wien, am 30. April 2007 .....

Stefan Hetzl

Kurzfassung

Die Beweistheorie jener Zweig der mathematischen Logik, in dem mathematisches Schließen und mathematische Beweise untersucht werden. Sie entstand aus Hilberts Programm: der Suche nach Konsistenzbeweisen für formale Theorien. In den 1950ern begann sich der Fokus der Beweistheorie auf Anwendungen formaler Methoden auf konkrete Beweise zu verschieben.

Die Methode CERES (cut-elimination by resolution) verwendet Techniken des Automatischen Beweisens zur Automatisierung der Schnittelimination. Der beweistheoretische Kern dieser Methode ist die Extraktion einer *charakteristischen Klauselmenge* aus einem Beweis. Eine Resolutionswiderlegung dieser Klauselmenge dient als Skelett eines schnittfreien Beweises.

Die vorliegende Dissertation ist eine Untersuchung des Potentials dieser Art von Klauselmengen zur Charakterisierung des mathematischen Inhaltes und der Struktur eines formalen Beweises. Es wird eine Variante dieser Klauselmengen vorgestellt, das *Profil*, welches die folgenden Vorteile gegenüber der originalen charakteristischen Klauselmenge bietet:

Es erzeugt niemals längere Beweise, sondern ist besser in der Behandlung von Redundanzen, was eine nicht-elementare Beschleunigung ermöglicht. Außerdem hat es die angenehme theoretische Eigenschaft invariant unter Regelpermutationen zu sein. Daraus folgt sofort, dass zwei Beweise mit dem gleichen Beweisnetz auch das gleiche Profil haben.

In dieser Arbeit wird eine große Klasse von Beweistransformationen definiert, die das Profil nicht verändern. Als Basis dieses Resultats wird zuvor eine detaillierte Analyse des Verhaltens des Profils unter der Schnittelimination durchgeführt, die zu einem sehr natürlichen Resultat führt.

Es wird gezeigt werden, dass das Profil in einer sehr engen Beziehung zu Herbrand-Disjunktionen steht: Das Profil besteht aus zwei Teilen die genau zu redundanzfreien Varianten der beiden partiellen Herbrand-Disjunktionen eines Beweises mit Schnitten korrespondieren.

In einer Fallstudie werden zwei unterschiedliche Beweise eines mathematisches Theorems mit Hilfe von charakteristischen Klauselmengen analysiert, um das Anwendungspotential zu illustrieren.

DOCTORAL THESIS

Characteristic Clause Sets and Proof Transformations

carried out at the

Institute of Computer Languages
Theory and Logic Group
of the Vienna University of Technology

under the supervision of

Univ.Prof. Dr.phil. Alexander Leitsch

by

Dipl.-Ing. Stefan Hetzl
Langackergasse 11b/2/2
A-1190 Wien

Abstract

Proof Theory is the branch of mathematical logic that investigates mathematical reasoning and mathematical proofs. This area emanated from Hilbert's Program calling for consistency proofs of formal theories. In the 1950s the focus of proof theory began shifting towards applications of formal methods to concrete proofs in order to obtain new mathematical results.

The method CERES (cut-elimination by resolution) uses techniques from automated theorem proving for the automation of cut-elimination. The main proof-theoretical tool of this method is the extraction of a *characteristic clause set* from a proof, a resolution refutation of which serves as the skeleton of a cut-free proof.

This thesis is an investigation of the potential of these kind of clause sets for characterizing the mathematical content and structure of a formal proof. We first define a variant of these clause sets, the *profile* that has several advantages w.r.t. the original characteristic clause sets:

It is computationally superior in the sense that it will never generate longer proofs with CERES, but is better in detecting certain redundancies thus allowing even a non-elementary speed-up. Furthermore, it has the nice theoretical property of being invariant under rule permutations which shows that two proofs having the same proof net will also have the same profile.

We will isolate a large class of proof transformations and show that they leave the profile invariant. As a basis for this result we will give a detailed analysis of the behavior of the profile under cut-elimination whose result will be particularly natural.

We will show that the profile is intimately related to Herbrand-disjunctions. It turns out that the profile has two dual parts corresponding to pruned versions of the two partial Herbrand-disjunctions that can be extracted from a proof with cuts: One being the instances of the end-sequent and one the instances of the cut-formulas.

Finally we will perform a case study where two different proofs of a simple mathematical theorem are analyzed by characteristic clause sets in order to demonstrate its potential for applications.

Acknowledgments

First and foremost I want to thank my advisor, Alexander Leitsch. He is an excellent teacher who led me step-by-step to an ever deepening understanding of logic and proof theory. At the same time he gave me a large amount of freedom making it possible for me to explore things on my own and thus to become increasingly competent when working alone. I also owe a lot to him concerning my general understanding of science. It is only through him that I learned disciplined scientific thinking. I am also grateful for the immense amount of time he spent in discussions with me and with proof-reading my work.

I also want to thank the whole Theory and Logic Group in Vienna for providing a stimulating atmosphere for scientific work: I am enjoying the various seminars and discussions very much. I have learned a great deal from discussions of all kinds of different topics with Chris Fermüller and I gained a lot of understanding of proof theory from interesting discussions with Matthias Baaz.

This thesis also benefitted a lot from my work in the CERES project group with A. Leitsch and my colleagues Clemens Richter and Hendrik Spohr. Implementing many of the methods of this thesis led me to a deeper understanding of the details which in turn improved the mathematical analysis.

I am grateful to Alessandra Carbone for many valuable comments and suggestions concerning my work and particularly for agreeing to take the burden of being a reviewer and examiner of this thesis.

I would also like to thank the group Preuves, Programmes et Systèmes of the Université Paris 7, and in particular Michel Parigot, for the hospitality during my stay in Paris in the second term of the year 2005/2006.

Contents

Chapter 1

Introduction

The history of logic starts with Aristotle's fundamental insight that there are propositions that are true not by virtue of their *meaning* but by virtue of their *form*. His syllogisms are a systematic collection of the abstract forms of valid deductive arguments, independent of their concrete meaning. For example, each proposition of the form "All A are B. All B are C. Therefore all A are C" is true whatever the meaning of A, B and C is. Aristotle's work remained dominant in logic until the 19th century.

In the early 1920s, the influential mathematician David Hilbert proposed the research program of providing a formalization of mathematics in an axiomatic form. The purpose of this axiomatization was the justification of mathematical reasoning, and in particular to show its consistency by restricted means: The consistency proof itself should be carried out by finitary methods which are themselves not doubtable.

In his landmark work [27], Kurt Gödel proved the incompleteness theorems: In every axiomatic theory containing a certain amount of number theory there exist true propositions whose truth cannot be shown within the theory. And furthermore, the consistency of the theory is an example of such a proposition. This result not only invalidated a certain specific formalization of mathematical reasoning but shows that – in principle – there can not exists a single axiomatic theory containing all mathematics, as in particular for the consistency proof of the theory, it must be transcended.

In [24] Gerhard Gentzen gave a proof of the consistency of Peano Arithmetic that is divided into two parts: A finitary part consisting of a proof transformation and an assumption whose truth cannot be shown in Peano Arithmetic but which entails the termination of the transformation. Most of the basic methods of the finitary part has already been developed in [23] for pure first-order logic: The sequent calculus for the formalization of proofs and the proof transformation of cut-elimination.

Cut-elimination brings a sequent calculus proof into a form where each formula occurring in the proof is a sub-formula of the theorem shown. Mathematically, this means that the concepts and structures present in a theorem are sufficient for proving it, for example number-theoretic statements can be proved by purely number-theoretic means and while the employment of e.g. analytic methods is useful in practice it is – in principle – not necessary. Moreover, the cut-elimination theorem is not a mere existence proof but a constructive method – it does not only show that an elementary proof exists but it gives a method for actually *constructing* such an elementary proof from any proof.

In the 1950s the work of Georg Kreisel (see e.g. [35, 36, 37]) marks a shift of emphasis in the research in consistency proofs: Instead of seeking a general justification of an axiomatic system one can *apply* the methods used for the consistency proof to concrete mathematical proofs formalized in the system. There exist several examples of such applications: Girard's demonstration (in [26]) that from the proof of Fürstenberg and Weiss of van der Waerden's theorem by cut-elimination the original combinatorial argument of van der Waerden can be obtained. Another example is Luckhardt analysis [39] of Roth's theorem about approximations of irrational numbers. The work of U. Kohlenbach (see e.g. [34]) is an application of proof interpretations, in particular of Gödel's functional interpretation, to the analysis of proofs. Most of these analyses are carried out by hand and require not only knowledge of the logical methods involved but also in-depth knowledge of the mathematical field under analysis.

With the increasing power of computers, the body of completely formalized mathematics that is available in electronic form has greatly increased. Several projects have been founded that provide an environment for computer-aided formalization of proofs ("proof assistants") with the aim of formalizing serious mathematical proofs, for example Mizar[1], Isabelle[2] or Coq[3]. These systems are successful: It is practically possible to formalize also large proofs with such systems, for example G. Gonthier has formalized a proof of the 4-color theorem in Coq (see [28]).

This possibility of completely formalizing mathematical proofs in an electronic format and the fact that the constructive content of consistency proofs can be – in principle – automated has raised the question in how far it is possible to employ computers not only for the formalization but also for the *analysis* of mathematical proofs. The CERES-method for cut-elimination [8] has been developed by M. Baaz and A. Leitsch with this aim and it

[1] `http://mizar.org/`
[2] `http://www.cl.cam.ac.uk/research/hvg/Isabelle/`
[3] `http://coq.inria.fr/`

has also been implemented[4]. Another system with similar aims is minlog[5], developed by the group of H. Schwichtenberg.

The main proof-theoretical tool of the CERES-method is the extraction of a *characteristic clause set* from a formal proof with cuts. Any resolution refutation of this clause set can then serve as a skeleton for a cut-free proof. This thesis is an investigation of the potential of these kind of clause sets for characterizing the mathematical content and structure of a formal proof

After explaining the scientific background of this thesis in Chapter 2, we will in Chapter 3 define an improved variant of the original characteristic clause sets, the *profile* of a proof. We will show that the profile can completely replace the original characteristic clause sets: It is computationally superior in the sense that it will never generate longer proofs with CERES, i.e. if there is a resultion refutation of the characteristic clause set of length l then there is a resolution refutation of the profile of length $l' \leq l$. It is even better in detecting certain types of redundancies thus allowing a non-elementary speed-up, i.e. there is a sequence of proofs where the length of the refutation of the characteristic clause set cannot be bounded by an elementary function whereas there exists a refutation of the profile of constant length.

Chapter 4 is devoted to relating and comparing the profile to other methods for abstracting from concrete details of formal proofs: proof nets, Herbrand-disjunctions and logical flow graphs will be investigated. The profile has the nice theoretical property of being invariant under rule permutations which gives as immediate corollary that two proofs having the same proof net will also have the same profile and – in this sense – it constitutes a generalization of proof nets. Proof nets originate from J.-Y. Girard's work on linear logic [25] and can also be defined for classical logic as in [44]. An important tool for the analysis of mathematical proofs are Herbrand-disjunction, named after J. Herbrand whose famous theorem says that an existentially quantified first-order formula is valid iff there exists a finite disjunction of instances of these existential quantifiers which are a propositional tautology (see [29] and also [13]). Chapter 4 is mainly devoted to showing that the profile is intimately related to Herbrand-disjunctions: The profile has two dual parts corresponding to pruned versions of the two partial Herbrand-disjunctions that can be extracted from a proof with cuts: One being the instances of the end-sequent and one the instances of the cut-formulas. In a certain sense the profile can be seen as a combination of the techniques of first building an Herbrand-disjunction in order to abstract from concrete details of the proof and secondly of applying a normal form transformation to abstract from concrete details of the formulas in the proof.

In Chapter 5 we will give an analysis of the behavior of the profile under

[4] `http://www.logic.at/ceres/`

[5] `http://www.mathematik.uni-muenchen.de/~minlog/`

proof transformations. First we will show that cut-elimination does change the profile in a surprisingly simple and natural way. Then we will define a large class of proof transformations, containing e.g. the transformation of formulas to negation normal form. We will show that applying transformations from this class to the cut-formulas of a proof will leave the profile invariant. This class of proof transformations will be defined via a class of (simple) proofs and cut-elimination will be used as execution of these transformations.

Finally, in Chapter 6 we will perform a case study where two different proofs of a simple mathematical theorem are analyzed by characteristic clause sets. This analysis reveals that the characteristic clause set contains essential information not only about the proof itself but – more importantly – about *all* cut-free proofs that can be obtained from this one.

Chapter 2

Background

2.1 The Sequent Calculus

In his seminal work [23], Gentzen introduced the two formal systems which still today are the most prominent of proof theory: The sequent calculus and the calculus of natural deduction. In this paper he proved his famous Hauptsatz: the cut-elimination theorem. Gentzen's primary interest was the calculus of natural deduction, the sequent calculus has been introduced for the purpose of showing the cut-elimination theorem. As these two systems can be easily translated into each other, the cut-elimination theorem in the sequent calculus gave an indirect proof of the analogue theorem about natural deduction. A direct proof for natural deduction has only been obtained later in [42].

The calculi in [23] are designed in a way that is well-suited for both the formalization of classical and of intuitionistic first-order logic. This led to certain peculiarties of the form of inference rules and of the form of cut reduction rules. In this thesis we will deal with classical logic only, so we will not use Gentzen's original calculus but a more streamlined version. Our rules will be purely multiplicative which is well-suited for investigating proof transformations.

In order to distinguish different occurrences of the same formula in a sequent without having to introduce exchange or permutation rules to the calculus, we formally use sequents of indexed formulas. An indexed formula is pair consisting of a formula and an index from some countable infinite index set $\mathcal{I}$. A sequent is a pair of sets of indexed formulas. It is assumed that each index occurs at most once in a proof. So, formally, a formula occurrence is an index.

Definition 2.1 (**LK**-proof)**.** An **LK**-proof φ is a tree. The nodes of φ are labelled with sequents, the edges are labelled with rules and the leaves are

called axiom sequents.

1. Axiom sequents are of the form:

$$A \vdash A \quad \text{for an atomic formula } A$$

2. Logical Rules

$$\frac{\Gamma \vdash \Delta, A \quad \Pi \vdash \Lambda, B}{\Gamma, \Pi \vdash \Delta, \Lambda, A \wedge B} \wedge\text{: r} \qquad \frac{A, B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta} \wedge\text{: l}$$

$$\frac{A, \Gamma \vdash \Delta \quad B, \Pi \vdash \Lambda}{A \vee B, \Gamma, \Pi \vdash \Delta, \Lambda} \vee\text{: l} \qquad \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B} \vee\text{: r}$$

$$\frac{\Gamma \vdash \Delta, A \quad B, \Pi \vdash \Lambda}{A \to B, \Gamma, \Pi \vdash \Delta, \Lambda} \to : \text{l} \qquad \frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B} \to : \text{r}$$

$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta} \neg\text{: l} \qquad \frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \neg\text{: r}$$

$$\frac{A\{x \leftarrow t\}, \Gamma \vdash \Delta}{(\forall x)A, \Gamma \vdash \Delta} \forall\text{: l} \qquad \frac{\Gamma \vdash \Delta, A\{x \leftarrow \alpha\}}{\Gamma \vdash \Delta, (\forall x)A} \forall\text{: r}$$

$$\frac{\Gamma \vdash \Delta, A\{x \leftarrow t\}}{\Gamma \vdash \Delta, (\exists x)A} \exists\text{: r} \qquad \frac{A\{x \leftarrow \alpha\}, \Gamma \vdash \Delta}{(\exists x)A, \Gamma \vdash \Delta} \exists\text{: l}$$

For the variable α and the term t the following must hold:

(a) t must not contain a variable that occurs bound in A

(b) α is called an *eigenvariable* and must not occur in $\Gamma \cup \Delta \cup \{A\}$ (eigenvariable condition).

3. Structural Rules

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \text{ w} : \text{r} \qquad \frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \text{ w} : \text{l}$$

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \text{ c} : \text{l} \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A} \text{ c} : \text{r}$$

$$\frac{\Gamma \vdash \Delta, A \quad A, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda} \text{ cut}$$

In the above definition of the rules some formula occurrences are written down explicitly, e.g. A and $\neg A$ in the definition of the $\neg : r$-rule and some occur in the context Γ, Δ. For a concrete rule ρ in a proof, the formula occurrence written down explicitly in the definition of the rule in the sequent below the rule is called *main occurrence* of ρ. The formula occurrences written down explicitly in the sequents above ρ are called *auxiliary occurrences* of ρ. If an occurrence is auxiliary or main for a certain rule, it is said to be an *active occurrence* of this rule.

We define an ancestor-relation as follows: For formula occurrences μ and ν, μ is said to be an immediate ancestor of ν if either μ is an auxiliary occurrence of a rule whose main occurrence is ν or μ occurs in the context in a sequent above a rule and ν is the corresponding occurrence in the sequent below this rule. The ancestor-relation is then defined as the reflexive and transitive closure of the immediate ancestor-relation.

In order to keep track of ancestor occurrences in axioms we will consider proofs labelled in the following way: We fix a countable label set $\mathcal{L}$, e.g. $\mathcal{L} = \mathbb{N}$, and given a proof φ assign each axiom occurrence in φ a unique label. For a formula occurrence μ, the label set of μ, written as $\mathcal{L}(\mu)$, is defined as follows: If μ occurs in an axiom, its label set is the singleton set containing only the axiom's label. If μ does not occur in an axiom, its label set is the union of the label sets of all its immediate ancestors. For a rule ρ, the label set of ρ, written $\mathcal{L}(\rho)$, is the union of the label sets of its auxiliary occurrences. This way of assigning labels connects each formula occurrence and each rule in the proof with the axioms necessary for composing it.

There exist several extensions of the sequent calculus as presented above: For example, the calculus $\mathbf{LK_e}$ in [49] includes additional axioms for the handling of equality. Reflexivity and compatibility of $=$ are added as additional axiom sequents, symmetry and transitivity can be derived.

2.1.1 An Example

In this section we will give an example for the formalization of a mathematical proof in the sequent calculus. This is a very simple example from lattice theory (see e.g. [11]). There exist several equivalent definition of the notion of a lattice. We will formalize a proof that one such definition entails another one.

Definition (SL)**.** A *semi-lattice* is a non-empty set L together with a binary operation $\cdot$ s.t.

1. $x \cdot y = y \cdot x$ (commutativity)
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity)

3. $x \cdot x = x$ (idempotence)

Definition. Let $(L, \cdot)$ be a semi-lattice. The binary relation $\leq.$ on L is defined as

$$x \leq. y \iff x \cdot y = x$$

The two following definitions are equivalent.

Definition (L1)**.** Let $(L, \cap)$ and $(L, \cup)$ be semi-lattices. Then $(L, \cap, \cup)$ is a *lattice* if the following condition is fulfilled:

$$x \leq_\cap y \iff y \leq_\cup x$$

Definition (L2)**.** Let $(L, \cap)$ and $(L, \cup)$ be semi-lattices. Then $(L, \cap, \cup)$ is a *lattice* if the absorption laws

$$(x \cap y) \cup x = x \quad \text{and} \quad (x \cup y) \cap x = x$$

are fulfilled.

We will give a formal proof of the implication (L1) $\Rightarrow$ (L2).

Example 2.1. Let $\cdot$ be a binary operation, define the following abbreviations for formulas formalizing the properties above:

$$\begin{aligned}
\text{C.} &:= (\forall x)(\forall y)\ x \cdot y = y \cdot x \\
\text{A.} &:= (\forall x)(\forall y)(\forall z)\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \\
\text{I.} &:= (\forall x)\ x \cdot x = x \\
\text{SL.} &:= \text{C.} \wedge \text{A.} \wedge \text{I.} \\
D_1 &:= (\forall x)(\forall y)\ (x \leq_\cap y \to y \leq_\cup x) \\
D_2 &:= (\forall x)(\forall y)\ (x \leq_\cup y \to y \leq_\cap x) \\
A_1 &:= (\forall x)(\forall y)\ (x \cap y) \cup x = x \\
A_2 &:= (\forall x)(\forall y)\ (x \cup y) \cap x = x
\end{aligned}$$

The mathematical statement that every object satisfying definition (L1) also satisfies (L2) can now be formalized as the sequent $s =$

$$\text{SL}_\cup, \text{SL}_\cap, D_1 \wedge D_2 \vdash A_1 \wedge A_2$$

A formal proof of s in the sequent calculus is $\varphi =$

$$\dfrac{\dfrac{\dfrac{\dfrac{(\varphi_1) \qquad (\varphi_2)}{\text{SL}_\cup, \text{SL}_\cap, D_1 \wedge D_2 \vdash A_1 \quad \text{SL}_\cup, \text{SL}_\cap, D_1 \wedge D_2 \vdash A_2}\ \wedge\text{: r}}{\text{SL}_\cup, \text{SL}_\cup, \text{SL}_\cap, \text{SL}_\cap, D_1 \wedge D_2, D_1 \wedge D_2 \vdash A_1 \wedge A_2}\ \text{c : l}}{\text{SL}_\cup, \text{SL}_\cup, \text{SL}_\cap, \text{SL}_\cap, D_1 \wedge D_2 \vdash A_1 \wedge A_2}\ \text{c : l}}{\text{SL}_\cup, \text{SL}_\cup, \text{SL}_\cap, D_1 \wedge D_2 \vdash A_1 \wedge A_2}\ \text{c : l}}{\text{SL}_\cup, \text{SL}_\cap, D_1 \wedge D_2 \vdash A_1 \wedge A_2}\ \text{c : l}$$

where $\varphi_1 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\psi_1) \quad (\psi_2)}{\mathrm{SL}_\cap \vdash (\alpha \cap \beta) \cap \alpha = \alpha \cap \beta \quad \mathrm{SL}_\cup, \alpha \cup (\alpha \cap \beta) = \alpha \vdash (\alpha \cap \beta) \cup \alpha = \alpha}}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, (\alpha \cap \beta) \cap \alpha = \alpha \cap \beta \to \alpha \cup (\alpha \cap \beta) = \alpha \vdash (\alpha \cap \beta) \cup \alpha = \alpha}\,{\to}:\mathrm{l}}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, (\forall y)\ ((\alpha \cap \beta) \cap y = \alpha \cap \beta \to y \cup (\alpha \cap \beta) = y) \vdash (\alpha \cap \beta) \cup \alpha = \alpha}\,\forall:\mathrm{l}}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, (\forall x)(\forall y)\ (x \cap y = x \to y \cup x = y) \vdash (\alpha \cap \beta) \cup \alpha = \alpha}\,\forall:\mathrm{l}}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, (\forall x)(\forall y)\ (x \leq_\cap y \to y \leq_\cup x) \vdash (\alpha \cap \beta) \cup \alpha = \alpha}\,\forall:\mathrm{r}}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, (\forall x)(\forall y)\ (x \leq_\cap y \to y \leq_\cup x) \vdash (\forall y)\ (\alpha \cap y) \cup \alpha = \alpha}\,\forall:\mathrm{r}}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, (\forall x)(\forall y)\ (x \leq_\cap y \to y \leq_\cup x) \vdash (\forall x)(\forall y)\ (x \cap y) \cup x = x}$$

$$\dfrac{\dfrac{\mathrm{SL}_\cup, \mathrm{SL}_\cap, D_1 \vdash A_1}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, D_1, D_2 \vdash A_1}\,\mathrm{w}:\mathrm{l}}{\mathrm{SL}_\cup, \mathrm{SL}_\cap, D_1 \wedge D_2 \vdash A_1}\,\wedge:\mathrm{l}$$

where ψ_1 consists of trivial applications of associativity, commutativity and idempotence and ψ_2 consists of a single application of commutativity. The proof φ_2 is analogous to φ_1. Note that the proofs ψ_1 and ψ_2 have to be carried out in $\mathbf{LK_e}$ because reasoning with equality is needed.

2.2 Cut-Elimination

Gentzen's proof of the cut-elimination theorem works by shifting cuts upward in the proof until the logical complexity of the cut-formula can be reduced. This is repeated for the cuts newly created by the reduction of the logical complexity. A cut on a formula in an axiom can be deleted together with the axiom. We present this proof here in a variant that is inspired by term rewriting and computational interpretations of cut-elimination: We first give a general reduction relation $\to_\mathrm{G}$ between **LK**-proofs and then show that $\to_\mathrm{G}$ is weakly normalizing, i.e. that there exists a terminating strategy. The reduction relation works only on regular proofs. A proof is called regular if all eigenvariables are different, i.e. for each pair of strong quantifier rules, the respective eigenvariables are different.

Definition 2.2 ($\to_\mathrm{G}$)**.** We define the Gentzen-style cut-elimination as the reduction relation $\to_\mathrm{G}$ on regular **LK**-proofs which is the union of the reduction relations $\to_{\mathrm{G_p}}, \to_{\mathrm{G_q}}, \to_{\mathrm{G_a}}, \to_{\mathrm{G_w}}, \to_{\mathrm{G_c}}, \to_{\mathrm{G_r}}$ defined as follows:

Let φ be an **LK**-proof of the form:

$$\dfrac{\dfrac{(\varphi_1) \quad (\varphi_2)}{\Gamma \vdash \Delta, A \quad A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}$$

1. Reduction of propositional rules $\to_{\mathrm{G_p}}$:
   The cut formula is introduced by propositional rules on both sides immediately above the cut.

(a) $A = B \wedge C$, $\varphi =$

$$\dfrac{\dfrac{\overset{(\varphi_1')}{\Gamma_1 \vdash \Delta_1, B} \quad \overset{(\varphi_1'')}{\Gamma_2 \vdash \Delta_2, C}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, B \wedge C}\ \wedge\text{: r} \quad \dfrac{\overset{(\varphi_2')}{B, C, \Pi \vdash \Lambda}}{B \wedge C, \Pi \vdash \Lambda}\ \wedge\text{: l}}{\Gamma_1, \Gamma_2, \Pi \vdash \Delta_1, \Delta_2, \Lambda}\ \text{cut}$$

then $\varphi \to_{\mathrm{G_p}} \varphi' :=$

$$\dfrac{\overset{(\varphi_1'')}{\Gamma_2 \vdash \Delta_2, C} \quad \dfrac{\overset{(\varphi_1')}{\Gamma_1 \vdash \Delta_1, B} \quad \overset{(\varphi_2')}{B, C, \Pi \vdash \Lambda}}{C, \Gamma_1, \Pi \vdash \Delta_1, \Lambda}\ \text{cut}}{\Gamma_1, \Gamma_2, \Pi \vdash \Delta_1, \Delta_2, \Lambda}\ \text{cut}$$

(b) $A = B \vee C$: symmetric to case 1a.

(c) $A = B \to C$, $\varphi =$

$$\dfrac{\dfrac{\overset{(\varphi_1')}{B, \Gamma \vdash \Delta, C}}{\Gamma \vdash \Delta, B \to C}\ \to\text{: r} \quad \dfrac{\overset{(\varphi_2')}{\Pi_1 \vdash \Lambda_1, B} \quad \overset{(\varphi_2'')}{C, \Pi_2 \vdash \Lambda_2}}{B \to C, \Pi_1, \Pi_2 \vdash \Lambda_1, \Lambda_2}\ \to\text{: l}}{\Gamma, \Pi_1, \Pi_2 \vdash \Delta, \Lambda_1, \Lambda_2}\ \text{cut}$$

then $\varphi \to_{\mathrm{G_p}} \varphi' :=$

$$\dfrac{\dfrac{\overset{(\varphi_2')}{\Pi_1 \vdash \Lambda_1, B} \quad \overset{(\varphi_1')}{B, \Gamma \vdash \Delta, C}}{\Pi_1, \Gamma \vdash \Lambda_1, \Delta, C}\ \text{cut} \quad \overset{(\varphi_2'')}{C, \Pi_2 \vdash \Lambda_2}}{\Gamma, \Pi_1, \Pi_2 \vdash \Delta, \Lambda_1, \Lambda_2}\ \text{cut}$$

(d) $A = \neg B$, $\varphi =$

$$\dfrac{\dfrac{\overset{(\varphi_1')}{B, \Gamma \vdash \Delta}}{\Gamma \vdash \Delta, \neg B}\ \neg\text{: r} \quad \dfrac{\overset{(\varphi_2')}{\Pi \vdash \Lambda, B}}{\neg B, \Pi \vdash \Lambda}\ \neg\text{: l}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

then $\varphi \to_{\mathrm{G_p}} \varphi' :=$

$$\dfrac{\overset{(\varphi_2')}{\Pi \vdash \Lambda, B} \quad \overset{(\varphi_1')}{B, \Gamma \vdash \Delta}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

2. Reduction of quantifier rules $\to_{\mathrm{G_q}}$:
The cut formula is introduced by quantifier rules on both sides immediately above the cut.

(a) $A = (\forall x)B$, $\varphi =$

$$\dfrac{\dfrac{\begin{matrix}(\varphi_1')\\ \Gamma \vdash \Delta, B\{x \leftarrow \alpha\}\end{matrix}}{\Gamma \vdash \Delta, (\forall x)B}\ \forall\text{: r} \quad \dfrac{\begin{matrix}(\varphi_2')\\ B\{x \leftarrow t\}, \Pi \vdash \Lambda\end{matrix}}{(\forall x)B, \Pi \vdash \Lambda}\ \forall\text{: l}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

then $\varphi \rightarrow_{\mathrm{G_q}} \varphi' :=$

$$\dfrac{\begin{matrix}(\varphi_1'\{\alpha \leftarrow t\})\\ \Gamma \vdash \Delta, B\{x \leftarrow t\}\end{matrix} \quad \begin{matrix}(\varphi_2')\\ B\{x \leftarrow t\}, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

(b) $A = (\exists x)B$: symmetric to case 2a.

3. Reduction of axioms $\rightarrow_{\mathrm{G_a}}$:
The cut formula is introduced by an axiom on (at least) one of the two sides immediately above the cut.

(a) φ_1 is an axiom sequent, $\varphi =$

$$\dfrac{A \vdash A \quad \begin{matrix}(\varphi_2)\\ A, \Pi \vdash \Lambda\end{matrix}}{A, \Pi \vdash \Lambda}\ \text{cut}$$

then $\varphi \rightarrow_{\mathrm{G_a}} \varphi_2$

(b) φ_2 is an axiom sequent, then $\varphi \rightarrow_{\mathrm{G_a}} \varphi_1$

4. Reduction of weakening $\rightarrow_{\mathrm{G_w}}$:
The cut formula is introduced by weakening on (at least) one of the two sides immediately above the cut.

(a) φ_1 ends with $w : r$, $\varphi =$

$$\dfrac{\dfrac{\begin{matrix}(\varphi_1')\\ \Gamma \vdash \Delta\end{matrix}}{\Gamma \vdash \Delta, A}\ \text{w} : \text{r} \quad \begin{matrix}(\varphi_2)\\ A, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

then $\varphi \rightarrow_{\mathrm{G_w}} \varphi' :=$

$$\dfrac{\begin{matrix}(\varphi_1')\\ \Gamma \vdash \Delta\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{w} : *$$

(b) φ_2 ends with $w : l$: symmetric to case 3b.

5. The cut formula is introduced by a contraction on (at least) one of the two sides immediately above the cut.

(a) φ_1 ends with $c : r$, $\varphi =$

$$\dfrac{\dfrac{(\varphi_1')}{\Gamma \vdash \Delta, A, A}\ \mathrm{c:r} \qquad \dfrac{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}$$

then $\varphi \to_{\mathrm{G_c}} \varphi' :=$

$$\dfrac{\dfrac{\dfrac{(\varphi_1')}{\Gamma \vdash \Delta, A, A} \quad \dfrac{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda, A}\ \mathrm{cut} \qquad \dfrac{(\varphi_2')}{A, \Pi \vdash \Lambda}}{\dfrac{\Gamma, \Pi, \Pi \vdash \Delta, \Lambda, \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{c:*}}\ \mathrm{cut}$$

where φ_2' is a variant of φ_2, defined by renaming all eigenvariables in φ_2 by fresh ones (in order to keep the regularity of the proof).

(b) φ_2 ends with $c : l$: symmetric to case 5a

6. rank-reduction $\to_{\mathrm{G_r}}$:
The cut formula is *not* introduced immediately above the cut on (at least) one of the two sides.

(a) on the right side

i. φ_2 ends with a unary rule, $\varphi =$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{\dfrac{(\varphi_2')}{A, \Pi' \vdash \Lambda'}}{A, \Pi \vdash \Lambda}\ r}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}$$

Then $\varphi \to_{\mathrm{G_r}} \varphi' :=$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2')}{A, \Pi' \vdash \Lambda'}}{\dfrac{\Gamma, \Pi' \vdash \Delta, \Lambda'}{\Gamma, \Pi \vdash \Delta, \Lambda}\ r}\ \mathrm{cut}$$

which is a valid **LK**-proof. Note that regularity ensures that the eigenvariable condition cannot be violated.

ii. φ_2 ends with a binary rule μ

A. the ancestor of A is in the left premise of μ, $\varphi =$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{\dfrac{(\varphi_2')}{A, \Pi_1' \vdash \Lambda_1'} \quad \dfrac{(\varphi_2'')}{\Pi_2' \vdash \Lambda_2'}}{A, \Pi \vdash \Lambda}\ r}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}$$

Then $\varphi \to_{\mathrm{G_r}} \varphi' :=$

$$\dfrac{\dfrac{\overset{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \overset{(\varphi_2')}{A, \Pi_1' \vdash \Lambda_1'}}{\Gamma, \Pi_1' \vdash \Delta, \Lambda_1'}\ \text{cut} \quad \overset{(\varphi_2'')}{\Pi_2' \vdash \Lambda_2'}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ r$$

which is a valid **LK**-proof.

B. the ancestor of A is in the right premise of μ: symmetric to the previous case.

(b) on the left side: symmetric to case 6a

The above defined set of reduction rules is not strongly terminating, i.e. there exist infinite reduction sequences. The above set of reduction rules is also not confluent, i.e. one proof may have several normal forms.

Example 2.2. Consider the following proof (that can also be found in [22, 20, 50]): $\varphi :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \quad A \vdash A}{A \vee A \vdash A, A}\ \vee\text{: l}}{A \vee A \vdash A}\ \text{c : r} \quad \dfrac{\dfrac{\dfrac{A \vdash A \quad A \vdash A}{A, A \vdash A \wedge A}\ \wedge\text{: r}}{A \vdash A \wedge A}\ \text{c : l}}{A \vee A \vdash A \wedge A}\ \text{cut}$$

Applying the reduction rules $\to_{\mathrm{G}}$ with a strategy that always moves a cut to the left side results in the normal form $\varphi_1 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \quad A \vdash A}{A, A \vdash A \wedge A}\ \wedge\text{: r}}{A \vdash A \wedge A}\ \text{c : l} \quad \dfrac{\dfrac{\dfrac{A \vdash A \quad A \vdash A}{A, A \vdash A \wedge A}\ \wedge\text{: r}}{A \vdash A \wedge A}\ \text{c : l}}{A \vee A \vdash A \wedge A, A \wedge A}\ \vee\text{: l}}{A \vee A \vdash A \wedge A}\ \text{c : r}$$

If we instead apply the reduction rules with a strategy that favors the right side we obtain the normal form $\varphi_2 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \quad A \vdash A}{A \vee A \vdash A, A}\ \vee\text{: l}}{A \vee A \vdash A}\ \text{c : r} \quad \dfrac{\dfrac{\dfrac{A \vdash A \quad A \vdash A}{A \vee A \vdash A, A}\ \vee\text{: l}}{A \vee A \vdash A}\ \text{c : r}}{A \vee A, A \vee A \vdash A \wedge A}\ \wedge\text{: r}}{A \vee A \vdash A \wedge A}\ \text{c : l}$$

Moreover the proof φ does have an infinite reduction sequence and infinitely many normal forms. By applying one rank-reduction to the left side and

then a reduction of the upper cut to the right side we obtain the proof $\varphi' =$

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \quad A \vdash A}{A \vee A \vdash A, A}\vee\!:\mathrm{l} \quad \dfrac{\dfrac{A \vdash A \quad A \vdash A}{A \vee A \vdash A, A}\vee\!:\mathrm{l} \quad \dfrac{A \vdash A \quad A \vdash A}{A, A \vdash A \wedge A}\wedge\!:\mathrm{r}}{A \vee A, A \vdash A, A \wedge A}\,\mathrm{cut}}{A \vee A, A \vee A \vdash A, A, A \wedge A}\,\mathrm{cut}}{\dfrac{A \vee A \vdash A, A, A \wedge A}{A \vee A \vdash A, A \wedge A}\,\mathrm{c}:\mathrm{r}^\star}\,\mathrm{c}:\mathrm{l} \qquad \dfrac{\dfrac{A \vdash A \quad A \vdash A}{A, A \vdash A \wedge A}\wedge\!:\mathrm{r}}{A \vdash A \wedge A}\,\mathrm{c}:\mathrm{l}^\star}{\dfrac{A \vee A \vdash A \wedge A, A \wedge A}{A \vee A \vdash A \wedge A}\,\mathrm{c}:\mathrm{r}}\,\mathrm{cut}^\star$$

which contains – in the three rules marked with $\star$ – a variant of the starting configuration. Iterating this "reduction" one can generate normal forms of any size.

There exist several variants and refinements of the above and similar rewrite relations that are confluent and/or terminating: In Gentzen's original proof [23] an uppermost reduction strategy is employed that favors moving cuts up on the right side over the left side. This strategy is – as Gentzen shows – terminating. Another terminating strategy is to use a cut whose cut-formula has maximal logical complexity, see e.g. [48]. By annotating each subformula of a cut-formula with a preferred direction one essentially obtains a reduction relation that is confluent and terminating without imposing restrictions on the reductions strategy [20]. Another terminating procedure can be found in [50, 51].

The rest of this section is devoted to giving a proof of the cut-elimination theorem for the present calculus: Every provable sequent has a cut-free proof. The proof of this theorem in the present setting amounts to showing weak normalization of the above cut-reduction relation $\rightarrow_{\mathrm{G}}$. We will essentially use an uppermost reduction strategy.

Definition 2.3. Let μ and ν be formula occurrences. We write $\mu >^1 \nu$ if

1. μ is the direct ancestor of ν in the context of a rule or
2. μ is auxiliary occurrence and ν is main occurrences of a contraction rule ρ

We write $>$ for the reflexive and transitive closure of $>^1$.

Definition 2.4. A *formula interspace* I is a set of formula occurrences closed w.r.t. $>$, i.e. for all μ, ν with $\mu > \nu : \mu \in I \Leftrightarrow \nu \in I$.

Note that formula interspaces are trees and that every formula occurrence in a proof belongs to exactly one formula interspace. We write $\mathrm{I}(\mu)$ for the formula interspace containing μ. We write $\lfloor I \rfloor$ for the formula occurrence that is the root of the interspace I, i.e. $\forall \mu \in I \setminus \lfloor I \rfloor : \mu > \lfloor I \rfloor$. A formula occurrence $\mu \in I$ is called a leaf if $\nexists \nu \in I$ s.t. $\nu > \mu$.

Definition 2.5 (rank)**.**

1. Let I be a formula interspace. We define the *rank* of I as:

$$\mathrm{rank}(I) := |\{\mu \in I \mid \mu \text{ is a leaf and } \mu \neq \lfloor I \rfloor\}|$$

2. Let ω be a cut occurrence. We define

$$\mathrm{rank}(\omega) := \mathrm{rank}(\mathrm{I}(\omega))$$

3. Let ρ be a cut with positive cut occurrence ω^+ and negative cut occurrence ω^-. We define

$$\mathrm{lrank}(\rho) := \mathrm{rank}(\omega^+) \quad \mathrm{rrank}(\rho) := \mathrm{rank}(\omega^-)$$

$$\mathrm{rank}(\rho) := \mathrm{lrank}(\rho) + \mathrm{rrank}(\rho)$$

4. Let φ be a proof with cuts $\rho_1, \ldots, \rho_n$. We define

$$\mathrm{lrank}(\varphi) := \sum_{i=1}^{n} \mathrm{lrank}(\rho_i) \quad \mathrm{rrank}(\varphi) := \sum_{i=1}^{n} \mathrm{rrank}(\rho_i)$$

$$\mathrm{rank}(\varphi) := \mathrm{lrank}(\varphi) + \mathrm{rrank}(\varphi)$$

We will use $\to_{\mathrm{G_{rc}}}$ to denote the union $\to_{\mathrm{G_r}} \cup \to_{\mathrm{G_c}}$. For a proof φ and a rule ρ in φ we will write $\varphi \mid \rho'$ for the sub-proof of φ that ends with ρ.

Lemma 2.1. Let φ be an **LK**-proof of the form

$$\dfrac{\overset{(\varphi_1)}{\Gamma \vdash \Delta, A_{[\omega]}} \quad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}[\rho]$$

with $\mathrm{lrank}(\varphi_1) = \mathrm{lrank}(\varphi_2) = 0$ and $\mathrm{lrank}(\rho) = \mathrm{lrank}(\omega) > 0$. Then there is an **LK**-proof φ^* with $\varphi \to_{\mathrm{G_{rc}}} \varphi^*$ and $\mathrm{lrank}(\varphi^*) < \mathrm{lrank}(\varphi) = \mathrm{rank}(\omega)$.

Proof. Let μ be a leaf of $\mathrm{I}(\omega)$. We mark all formula occurrences on the path from μ to ω with a $\star$. Let $\star(\varphi)$ denote the number of occurrences in φ that are marked with $\star$. We proceed by induction on $\star(\varphi)$ doing a case distinction on the type of the last rule σ in φ_1:

1. If σ is a contraction working on ω then $\varphi =$

$$\dfrac{\dfrac{\overset{(\varphi_1')}{\Gamma \vdash \Delta, A, A^\star}}{\Gamma \vdash \Delta, A^\star}\ \mathrm{c:r} \quad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}[\rho]$$

and we reduce $\varphi \to_{\mathrm{G_c}} \varphi'$ where $\varphi' =$

$$\dfrac{\dfrac{\overset{(\varphi_1')}{\Gamma \vdash \Delta, A, A^\star_{[\omega']}} \quad \overset{(\varphi_2')}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda, A}\ \mathrm{cut}[\rho'] \quad \overset{(\varphi_2'')}{A, \Pi \vdash \Lambda}}{\dfrac{\Gamma, \Pi, \Pi \vdash \Delta, \Lambda, \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{c} : *}\ \mathrm{cut}[\rho'']$$

Then $\star(\varphi') = \star(\varphi) - 1$ and

$$\begin{aligned} \mathrm{lrank}(\varphi') &= \mathrm{lrank}(\rho') + \mathrm{lrank}(\rho'') + \mathrm{lrank}(\varphi_1') + \mathrm{lrank}(\varphi_2') + \mathrm{lrank}(\varphi_2'') \\ &= \mathrm{lrank}(\rho') + \mathrm{lrank}(\rho'') \\ &\leq \mathrm{lrank}(\rho) \end{aligned}$$

Now if φ_1' ends with a rule introducing ω' then $\mathrm{lrank}(\rho') = 0, \star(\varphi') = 1$ and $\mathrm{lrank}(\varphi') < \mathrm{lrank}(\varphi)$ which finished the induction, i.e. $\varphi^* = \varphi'$. If φ_1' does not end with such a rule then we can apply the induction hypothesis to the proof $\varphi' \mid \rho'$ to obtain a proof φ^* with $\mathrm{lrank}(\varphi^*) < \mathrm{lrank}(\varphi)$.

2. σ is a cut and the ancestor of ω occurs on the left side of σ. Then $\varphi =$

$$\dfrac{\dfrac{\overset{(\varphi_1^l)}{\Gamma_1 \vdash \Delta_1, A^\star, B_{[\omega']}} \quad \overset{(\varphi_1^r)}{B, \Gamma_2 \vdash \Delta_2}}{\Gamma \vdash \Delta, A^\star_{[\omega]}}\ \mathrm{cut}[\sigma] \quad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}[\rho]$$

As $\mathrm{lrank}(\varphi_1) = 0$, the last rule of φ_1' introduced ω', let this rule w.l.o.g. be unary. Then $\varphi =$

$$\dfrac{\dfrac{\dfrac{\overset{(\varphi_1^{l'})}{\Gamma_1' \vdash \Delta_1', A^\star, B'}}{\Gamma_1 \vdash \Delta_1, A^\star, B_{[\omega']}}\ \mathrm{r} \quad \overset{(\varphi_1^r)}{B, \Gamma_2 \vdash \Delta_2}}{\Gamma \vdash \Delta, A^\star_{[\omega]}}\ \mathrm{cut}[\sigma] \quad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}[\rho]$$

We reduce this proof by shifting ρ up with two rank-reductions: $\rho \to_{\mathrm{G_r}} \rho' \to_{\mathrm{G_r}} \rho''$ where $\rho'' =$

$$\dfrac{\dfrac{\dfrac{\overset{(\varphi_1^{l'})}{\Gamma_1' \vdash \Delta_1', A^\star_{[\omega'']}, B'} \quad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma_1', \Pi \vdash \Delta_1', \Lambda, B'}\ \mathrm{cut}[\rho']}{\Gamma_1, \Pi \vdash \Delta_1, \Lambda, B}\ \mathrm{r} \quad \overset{(\varphi_1^r)}{B, \Gamma_2 \vdash \Delta_2}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}[\sigma']$$

Then $\star(\varphi'') = \star(\varphi) - 2$ and

$$\begin{aligned}\mathrm{lrank}(\varphi'') &= \mathrm{lrank}(\varphi_1^{l'}) + \mathrm{lrank}(\varphi_2) + \mathrm{lrank}(\varphi_1^{r}) + \mathrm{lrank}(\rho') + \mathrm{lrank}(\sigma') \\ &= \mathrm{lrank}(\rho') \\ &\leq \mathrm{lrank}(\rho)\end{aligned}$$

If $\varphi_1^{l'}$ ends with a rule introducing ω'', then $\mathrm{lrank}(\rho') = 0$, $\star(\varphi'') = 1$ and $\mathrm{lrank}(\varphi'') < \mathrm{lrank}(\varphi)$ which finished the induction, i.e. $\varphi^* = \varphi''$. If $\varphi_1^{l'}$ does not end with such a rule then we can apply the induction hypothesis to the proof $\varphi'' \mid \rho'$.

3. σ is any other unary rule, then $\varphi =$

$$\dfrac{\dfrac{\overset{(\varphi_1')}{\Gamma' \vdash \Delta', A^\star}\,\mathrm{r}}{\Gamma \vdash \Delta, A^\star} \qquad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}[\rho]$$

and we reduce $\varphi \to_{\mathrm{G_r}} \varphi'$ with

$$\dfrac{\overset{(\varphi_1')}{\Gamma' \vdash \Delta', A^\star} \qquad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{\dfrac{\Gamma', \Pi \vdash \Delta', \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{r}}\,\mathrm{cut}[\rho']$$

We have $\star(\varphi') = \star(\varphi) - 1$ and $\mathrm{lrank}(\varphi') \leq \mathrm{lrank}(\varphi)$. If $\star(\varphi') = 1$, the induction is finished, if not we can apply the induction hypothesis to $\varphi' \mid \rho'$.

4. If σ is any other binary rule: proceed analogously to the previous case.

□

Corollary 2.1. Let φ be an **LK**-proof. Then there is an **LK**-proof φ^* with $\varphi \to_{\mathrm{G_{rc}}} \varphi^*$ and $\mathrm{lrank}(\varphi^*) = 0$.

Proof. By repeatedly applying the previous lemma to the uppermost cut with $\mathrm{lrank} > 0$. □

Lemma 2.2. Let φ be an **LK**-proof of the form

$$\dfrac{\overset{(\varphi_1)}{\Gamma \vdash \Delta, A} \qquad \overset{(\varphi_2)}{A_{[\omega]}, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}[\rho]$$

with $\mathrm{lrank}(\varphi) = 0, \mathrm{rrank}(\varphi_1) = \mathrm{rrank}(\varphi_2) = 0$ and $\mathrm{rrank}(\rho) = \mathrm{rank}(\omega) > 0$. Then there is an **LK**-proof φ^* with $\varphi \to_{\mathrm{G_{rc}}} \varphi^*$, $\mathrm{lrank}(\varphi^*) = 0$ and $\mathrm{rrank}(\varphi^*) < \mathrm{rrank}(\varphi) = \mathrm{rank}(\omega)$.

Proof. Let μ be a a leaf of $\mathrm{I}(\omega)$ and mark all formula occurrences on the path from μ to ω with $\star$. Let $\star(\varphi)$ denote the number of occurrences marked with $\star$. We proceed by induction on $\star(\varphi)$ doing a case distinction on the type of the last rule σ in φ_2.

1. If σ is a contraction, then $\varphi =$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2')}{\dfrac{A^\star, A, \Pi \vdash \Lambda}{A^\star, \Pi \vdash \Lambda}\,\mathrm{c}:\mathrm{l}}}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}[\rho]$$

   and we reduce $\varphi \to_{\mathrm{G_c}} \varphi'$ where $\varphi' =$

$$\dfrac{\dfrac{(\varphi_1'')}{\Gamma \vdash \Delta, A} \quad \dfrac{\dfrac{(\varphi_1')}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2')}{A^\star, A, \Pi \vdash \Lambda}}{A, \Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}[\rho']}{\dfrac{\Gamma, \Gamma, \Pi \vdash \Delta, \Delta, \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{c}:*}\,\mathrm{cut}[\rho'']$$

   Then $\star(\varphi') = \star(\varphi) - 1$, $\mathrm{lrank}(\varphi') = 0$, $\mathrm{rrank}(\varphi') = \mathrm{rrank}(\rho') + \mathrm{rrank}(\rho'') \leq \mathrm{rrank}(\rho)$ and we can apply the induction hypothesis on $\varphi' \mid \rho'$.

2. If σ is a cut and the ancestor of ω occurs on the left side of σ then $\varphi =$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2^l)}{A^\star, \Pi_1 \vdash \Lambda_1, B} \quad \dfrac{(\varphi_2^r)}{B, \Pi_2 \vdash \Lambda_2}\,\mathrm{cut}[\sigma]}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}[\rho]$$

   As $\mathrm{lrank}(\varphi) = 0$, φ_2' ends with a rule introducing B, let this rule w.l.o.g. be unary, then $\varphi =$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{\dfrac{(\varphi_2^{l'})}{A^\star, \Pi_1' \vdash \Lambda_1'}\,\mathrm{r}}{A^\star, \Pi_1 \vdash \Lambda_1, B} \quad \dfrac{(\varphi_2^r)}{B, \Pi_2 \vdash \Lambda_2}\,\mathrm{cut}[\sigma]}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}[\rho]$$

   We reduce this proof by shifting up ρ with two rank reductions: $\varphi \to_{\mathrm{G_r}} \varphi' \to_{\mathrm{G_r}} \varphi''$ where $\varphi'' =$

$$\dfrac{\dfrac{\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2^{l'})}{A^\star, \Pi_1' \vdash \Lambda_1'}\,\mathrm{cut}[\rho']}{\Gamma, \Pi_1' \vdash \Delta, \Lambda_1'}\,\mathrm{r}}{\Gamma, \Pi_1 \vdash \Delta, \Lambda_1, B} \quad \dfrac{(\varphi_2^r)}{B, \Pi_2 \vdash \Lambda_2}\,\mathrm{cut}[\sigma']}{\Gamma, \Pi \vdash \Delta, \Lambda}$$

   Then $\star(\varphi'') = \star(\varphi) - 2$ and $\mathrm{lrank}(\varphi^*) = 0$ and $\mathrm{rrank}(\varphi'') \leq \mathrm{rrank}(\varphi)$.

3. If σ is a cut and the ancestor of ω occurs on the right side of σ: symmetric to the previous case.

4. σ is any other unary rule, then $\varphi =$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2')}{A^\star, \Pi' \vdash \Lambda'}\,[\sigma]}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}[\rho]$$

   and we reduce $\varphi \to_{\mathrm{G_r}} \varphi'$ with $\varphi' =$

$$\dfrac{\dfrac{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2')}{A^\star, \Pi' \vdash \Lambda'}}{\dfrac{\Gamma, \Pi' \vdash \Delta, \Lambda'}{\Gamma, \Pi \vdash \Delta, \Lambda}\,[\sigma]}\,\mathrm{cut}$$

   We have $\star(\varphi') = \star(\varphi) - 1$, $\mathrm{lrank}(\varphi') = 0$ and $\mathrm{rrank}(\varphi') \leq \mathrm{rrank}(\varphi)$.

5. If σ is any other binary rule: analogous to the previous case.

□

Corollary 2.2. Let φ be an **LK**-proof. Then there is an **LK**-proof φ^* with $\varphi \to^*_{\mathrm{G_{rc}}} \varphi^*$ and $\mathrm{rank}(\varphi^*) = 0$.

Proof. From Corollary 2.1 we obtain a proof φ' with $\mathrm{lrank}(\varphi') = 0$. By repeatedly applying the previous lemma to an uppermost cut with $\mathrm{rrank} > 0$ we obtain a φ^* with $\mathrm{rank}(\varphi^*) = 0$. □

Definition 2.6 (degree)**.**

1. Let F be a formula. The degree $\deg(F)$ of F is defined as follows
   (a) If F is an atom: $\deg(F) := 0$
   (b) If $F = G \circ H$ for $\circ \in \{\wedge, \vee, \to\}$ then

$$\deg(F) := \deg(G) + \deg(H) + 1$$

   (c) If $F = \neg G$ then $\deg(F) := \deg(G) + 1$.
   (d) If $F = (Qx)G$ for $Q \in \{\forall, \exists\}$ then $\deg(F) := \deg(G) + 1$

2. Let ρ be a cut rule with cut formula F. We define

$$\deg(\rho) := \deg(F)$$

3. Let φ be a proof with cuts $\rho_1, \ldots, \rho_n$. We define $\deg(\varphi)$ as the multiset

$$\{\deg(\varphi_1), \ldots, \deg(\varphi_n)\}$$

Definition 2.7. Let $\succ$ be a binary relation on some set X.

1. $\succ$ is called *strict order*, if it is transitive and irreflexive, i.e. $\forall x, y, z \in X : x \succ y$ and $y \succ z$ implies $x \succ z$ and $\forall x \in X : x \not\succ x$
2. $\succ$ is called *well-founded* if there is no infinite sequence $x_1 \succ x_2 \succ \ldots$ with $x_i \in X$

Let X be a set. We write $\mathcal{M}(X)$ for the set of all multisets containing elements of X.

Definition 2.8. Let $\succ$ be a strict order on a set X, the corresponding *multiset order* $\succ_{\text{mul}}$ on $\mathcal{M}(X)$ is defined as follows:

$$M \succ_{\text{mul}} N \text{ iff } M \neq N \text{ and } \forall x^+ \in N \setminus M \; \exists x^- \in M \setminus N \text{ s.t. } x^- \succ x^+$$

The important point about multiset orders is that they preserve well-foundedness.

Theorem 2.1. The multiset order $\succ_{\text{mul}}$ is well-founded iff $\succ$ is well-founded

Proof. see [1, pp. 23–24]. □

We will use the multiset of cut-degrees as terminating measure for our cut-elimination strategy. We write $<$ for this multiset order.

Lemma 2.3. Let φ be an **LK**-proof of the form

$$\dfrac{\begin{matrix}(\varphi_1) & (\varphi_2) \\ \Gamma \vdash \Delta, A & A, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}[\rho]$$

where φ_1 and φ_2 are cut-free. Then there is a proof φ^* with $\varphi \to_{\text{G}}^* \varphi^*$ s.t. $\deg(\varphi^*) < \deg(\varphi)$.

Proof. By Corollary 2.2 there is a proof φ' with $\varphi \to_{\text{G}_{\text{rc}}}^* \varphi'$ and $\text{rank}(\varphi') = 0$. Let $\rho_1, \ldots, \rho_n$ be the cuts in φ', then as $\varphi \to_{\text{G}_{\text{rc}}}^* \varphi'$, $\deg(\rho_1) = \ldots = \deg(\rho_n) = \deg(\rho)$ and as $\text{rank}(\varphi') = 0$ all ρ_i can be reduced by one of $\to_{\text{G}_{\text{a}}}, \to_{\text{G}_{\text{w}}}, \to_{\text{G}_{\text{p}}}$ or $\to_{\text{G}_{\text{q}}}$. Applying these reductions (in any order) gives a proof φ^* with $\deg(\varphi^*) < \deg(\varphi) = \{\deg(\rho)\}$ because $\deg(\rho^*) < \deg(\rho)$ for each cut ρ^* in φ^*. □

Theorem 2.2. Let φ be an **LK**-proof. Then there exists a cut-free **LK**-proof φ^* with $\varphi \to_{\text{G}} \varphi^*$.

Proof. Let ρ be an uppermost cut, let $\psi := \varphi \mid \rho$. By Lemma 2.3 there is a ψ' with $\psi \to_{\mathrm{G}}^{*} \psi'$ and $\deg(\psi') < \deg(\psi)$. Define $\varphi' := \varphi[\psi]_\rho$ and observe that $\deg(\varphi') = \deg(\psi') \cup D < \deg(\psi) \cup D = \deg(\varphi)$. Iterating this operation ends in a cut-free proof φ^* by well-foundedness of the multiset ordering on degrees. □

Definition 2.9. A proof φ of a sequent s is said to have the *subformula property* if for every formula F occurring in φ there is a sub-formula G in s and a substitution σ s.t. $G\sigma = F$.

Corollary 2.3. For every **LK**-proof φ there exists a proof φ' of the same end-sequent that has the subformula property.

Proof. By the cut-elimination theorem there exists a cut-free proof φ' and all cut-free proofs have the subformula property (as can easily be checked by inspecting the rules). □

2.2.1 The Mathematical Meaning of Cut-Elimination

Cut-elimination has important applications in proof theory: It has been used in [23] to show the consistency of intuitionistic propositional logic. It also plays the key role of the finitary proof transformation in Gentzen's consistency proof of Peano Arithmetic [24] and in various similar consistency proofs (see e.g. [48]). Having a cut-elimination theorem, the consistency of a calculus is easily demonstrated as follows:

Corollary 2.4. LK is consistent, i.e. there is no formula A s.t. both $\vdash A$ and $\vdash \neg A$ are derivable.

Proof. Assume there are such proofs φ_1 and φ_2. Then $\varphi :=$

$$\dfrac{\dfrac{(\varphi_2)}{\vdash \neg A} \quad \dfrac{\dfrac{(\varphi_1)}{\vdash A}}{\neg A \vdash}\,\neg\text{: l}}{\vdash}\,\text{cut}$$

would be a proof of the empty sequent. But by the cut-elimination theorem there would exist a proof φ' of the empty sequent having the subformula property. This is a contradiction because a proof of the empty sequent cannot have the subformula property. □

The cut-elimination theorem however does not only provide a purely extensional proposition on the existence of proofs with certain properties, its proof contains an *algorithm* for *transforming* given proofs with cuts into proofs without cuts.

This proof transformation corresponds to the removal of lemmas and those mathematical notions present in the lemmas from a proof. The formal proof resulting from cut-elimination will enjoy the subformula property. Mathematically this means that only such notions will be used in the proof that also appear in the theorem itself. So cut-elimination allows – in principle – the automated generation of elementary proofs from arbitrary proofs and is therefore of fundamental mathematical importance. Whole branches of mathematics, like e.g. analytic number theory, are devoted to proving elementary statements with more advanced methods. It is often an important and difficult problem to find an elementary proof for a theorem where already other (non-elementary) proofs exist.

We will illustrate the potential of the application of cut-elimination methods on a concrete example continuing the lattice example of Section 2.1.1.

Definition (PO)**.** A *partially ordered set (poset)* is a non-empty set S with a binary relation $\leq$ s.t.

1. $x \leq x$ (reflexivity)
2. if $x \leq y$ and $y \leq x$ then $x = y$ (anti-symmetry)
3. if $x \leq y$ and $y \leq z$ then $x \leq z$ (transitivity)

The following definition (L3) of a lattice is equivalent to the definitions (L1) and (L2).

Definition (L3)**.** Let $(L, \leq)$ be a partially ordered set. If for each two elements $x, y \in L$ there exists a greatest lower bound $\mathrm{glb}(x, y)$ and a least upper bound $\mathrm{lub}(x, y)$ then $(L, \mathrm{glb}, \mathrm{lub})$ is a *lattice*.

Example 2.3. Let $\cdot$ be a binary operation and let $\lhd$ be a binary relation. We define the following formulas formalizing the properties above:

$$
\begin{aligned}
\mathrm{R}_{\lhd} &:= (\forall x)\ x \lhd x \\
\mathrm{AS}_{\lhd} &:= (\forall x)(\forall y)\ ((x \lhd y \wedge y \lhd x) \rightarrow x = y) \\
\mathrm{T}_{\lhd} &:= (\forall x)(\forall y)(\forall z)\ ((x \lhd y \wedge y \lhd z) \rightarrow x \lhd z) \\
\mathrm{PO}_{\lhd} &:= \mathrm{R}_{\lhd} \wedge \mathrm{AS}_{\lhd} \wedge \mathrm{T}_{\lhd} \\
\mathrm{GLB}^{\cdot}_{\lhd} &:= (\forall x)(\forall y)(x \cdot y \lhd x \wedge x \cdot y \lhd y \wedge \\
&\qquad (\forall z)((z \lhd x \wedge z \lhd y) \rightarrow z \lhd x \cdot y)) \\
\mathrm{LUB}^{\cdot}_{\lhd} &:= (\forall x)(\forall y)(x \lhd x \cdot y \wedge y \lhd x \cdot y \wedge \\
&\qquad (\forall z)((x \lhd z \wedge y \lhd z) \rightarrow x \cdot y \lhd z))
\end{aligned}
$$

$\mathrm{PO}_{\lhd}$ says that $\lhd$ is a partial order. $\mathrm{GLB}^{\cdot}_{\lhd}$ says that $\cdot$ is a function computing the greatest lower bound of two elements w.r.t. $\lhd$ and analogously for $\mathrm{LUB}^{\cdot}_{\lhd}$.

The definitions L1, L2 and L3 are expressed through the formulas

$$\begin{aligned} \text{L1} &= \text{SL}_\cap \wedge \text{SL}_\cup \wedge D_1 \wedge D_2 \\ \text{L2} &= \text{SL}_\cap \wedge \text{SL}_\cup \wedge A_1 \wedge A_2 \\ \text{L3} &= \text{PO}_\leq \wedge \text{GLB}^\cap_\leq \wedge \text{LUB}^\cup_\leq \end{aligned}$$

where the abbreviations used here refer to the formulas defined in the example in Section 2.1.1.

As all of these definitions are equivalent, there exist formal proofs ψ of $\text{L1} \vdash \text{L3}$ and ξ of $\text{L3} \vdash \text{L2}$. One can thus compose the proof $\chi :=$

$$\dfrac{\begin{matrix}(\psi) & (\xi) \\ \text{L1} \vdash \text{L3} & \text{L3} \vdash \text{L2}\end{matrix}}{\text{L1} \vdash \text{L2}}\ \text{cut}$$

which corresponds to the concatenation of the two arguments: "As L1 implies L3 and L3 implies L2 also L1 implies L2". The important point is that neither L1 nor L2 contains the notion of partially ordered set. Nevertheless our proof χ of the implication $\text{L1} \vdash \text{L2}$ makes use of this notion. But clearly this is not necessary, for example the proof φ defined in Example 2.1 does not use properties of partially ordered sets. By application of a cut-elimination algorithm to χ we can obtain a proof χ' of $\text{L1} \vdash \text{L2}$ *having the subformula property*. In the case of this end-sequent, a proof having the sub-formula property does not make any reference to the notion of partially ordered set nor to its properties. The proof χ' will be an argument working only with the semi-lattice axioms similarly to our original proof φ. This way we can eliminate mathematical notions (in this case: the *partially ordered set*) from proofs by applying cut-elimination to obtain an elementary proof.

2.3 The Resolution Calculus

The main purpose of the sequent calculus as introduced by Gentzen was to prove the cut-elimination theorem. For automated deduction, i.e. the search for proofs by computers, the sequent calculus is not very well-suited: In searching for a proof bottom-up, i.e. starting from the end-sequent important choices have to be made at the weak quantifier rules ($\forall : l$ and $\exists : r$). Here, a finite number of terms have to be chosen (out of an infinite totality) that allow to finish the proof. In [45] J. A. Robinson introduced a calculus that is much better suited for automated deduction: the resolution calculus. The key ingredient is the unification principle which allows to choose these terms in a more goal-directed way then in sequent calculus. The resolution calculus works in a restricted syntax: so called clause sets which are conjunctive normal forms of skolemized formulas which has additional benefits for the automation. In this section we will review a variant

of clause logic and of the resolution calculus as far as needed in this thesis. For a comprehensive presentation see [38].

2.3.1 Labelled Clause Logic

A literal is an atom or a negated atom. A clause is a multiset of literals. A labelled clause is a clause that is assigned a non-empty set of labels from $\mathcal{L}$. For a labelled clause c we write $\mathcal{L}(c)$ to denote this set. We will use the notation $\{L_1, \ldots, L_n\}_S$ for the clause $\{L_1, \ldots, L_n\}$ with the set of labels S. In writing down concrete labelled clauses (with concrete labels) we will sometimes omit the set braces of S to increase readability. We will sometimes also use a sequent notation for clauses, writing the clause $\{\neg A_1, \ldots, \neg A_n, B_1, \ldots, B_m\}$ as $A_1, \ldots, A_n \vdash B_1, \ldots B_m$ for atoms A_i, B_j. A labelled clause in sequent notation is written as $\Gamma \vdash^L \Delta$. Let $c = \{L_1, \ldots, L_k\}_S$ and $d = \{M_1, \ldots, M_n\}_T$ be labelled clauses. We define the *merge* of c and d as $c \circ d := \{L_1, \ldots, L_k, M_1, \ldots, M_n\}_{S \cup T}$. Let C, D be sets of labelled clauses. We define the *product* of C and D as $C \times D := \{c \circ d \mid c \in C, d \in D\}$. A *label selection formula* is a propositional formula built up from label sets as atoms and the connectives $\wedge, \vee, \neg$. For a clause c and a set of labels L we will say that c *is an* L*-clause* if there exists a label l that is both in L and $\mathcal{L}(c)$. The labels will be used in order to describe subsets of sets of labelled clauses as follows:

Definition 2.10. Let C be a set of labelled clauses and let F be a label selection formula. We define C^F as follows:

1. $C^L := \{c \in C \mid c \text{ is an } L\text{-clause}\}$ for a set of labels L.
2. $C^{\neg F} := C \setminus C^F$
3. $C^{F \wedge G} := C^F \cap C^G$
4. $C^{F \vee G} := C^F \cup C^G$

Example 2.4. Let $C := \{\{P\}_1; \{\neg P, R\}_{2,3}; \{\neg R\}_3; \{\neg P, Q\}_{2,3,4}; \{\neg Q\}_{3,4}\}$. Then

$$C^{\{4\} \vee \neg\{3\}} = C^{\{4\}} \cup (C \setminus C^{\{3\}}) = \{\{P\}_1 \,;\, \{\neg P, Q\}_{2,3,4} \,;\, \{\neg Q\}_{3,4}\}$$

Note that $C^{L_1 \wedge L_2} \neq C^{L_1 \cap L_2}$. Consider for example $C = \{\{\neg P, Q\}_{1,2}\}$. Then $C^{\{1\} \wedge \{2\}} = C$ but $C^{\{1\} \cap \{2\}} = C^{\emptyset} = \emptyset$. In contrast $C^{L_1 \vee L_2} = C^{L_1 \cup L_2}$ as can be easily verified.

Definition 2.11 (restricted product)**.** Let C, D be sets of labelled clauses and F be a label selection formula. We define the operation $\times_F$ as

$$C \times_F D := (C^F \times D^F) \cup C^{\neg F} \cup D^{\neg F}$$

Example 2.5. Let $C = \{\{\neg P\}_1 \,;\, \{\neg Q\}_2\}, D = \{\{P\}_3 \,;\, \{Q\}_4\}$. Then

$$\begin{aligned} C \cup D &= \{\{\neg P\}_1 \,;\, \{\neg Q\}_2 \,;\, \{P\}_3 \,;\, \{Q\}_4\}\} \\ C \times D &= \{\{\neg P, P\}_{1,3} \,;\, \{\neg P, Q\}_{1,4} \,;\, \{\neg Q, P\}_{2,3} \,;\, \{\neg Q, Q\}_{2,4}\} \\ C \times_{\{1,4\}} D &= \{\{\neg P, Q\}_{1,4} \,;\, \{\neg Q\}_2 \,;\, \{P\}_3\} \end{aligned}$$

The reader can easily convice himself that - under the usual interpretation of a clause set as a universally quantified conjunctive normal form - the logical meaning of the union ($\cup$) is conjunction, the meaning of the product ($\times$) is disjunction and that the restricted product is in-between in the sense that $C \cup D$ implies $C \times_L D$ which in turn implies $C \times D$ for all $L \subseteq \mathcal{L}$.

Definition 2.12 (closure)**.** Let F be a formula with the free variables $x_1, \ldots, x_n$. We write $(\forall^*)F$ for the universal closure $(\forall x_1) \ldots (\forall x_n)F$ and we write $(\exists^*)F$ for the existential closure $(\exists x_1) \ldots (\exists x_n)F$.

Definition 2.13 ($\forall$CNF, $\exists$DNF)**.** We define functions $\forall$CNF, $\exists$DNF mapping a clause set to a formula. Let $C = \{c_1, \ldots, c_n\}$ be a set of clauses where $c_i = \{L_{i,1}, \ldots L_{i,m_i}\}$ for $i = 1, \ldots, n$. Then

$$\begin{aligned} \forall\mathrm{CNF}(C) &:= (\forall^*) \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} L_{i,j} \\ \exists\mathrm{DNF}(C) &:= (\exists^*) \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} L_{i,j} \end{aligned}$$

Let M be a multiset. We write $\mathrm{set}(M)$ for the set that contains an element iff M contains it at least once. For a set of labelled clauses C we write $\mathrm{set}(C)$ for $\mathrm{set}(C')$ where C' is the multiset of non-labelled clauses obtained from C by dropping all labels.

A technique for avoiding redundancy used heavily for automated deduction is subsumption.

Definition 2.14 (subsumption)**.** Let C, D be sets of labelled clauses. Then C *subsumes* D, written as $C \leq_{ss} D$ if $\forall d \in D$ there is a $c \in C$ and a substition σ with $\mathrm{set}(c)\sigma \subseteq \mathrm{set}(d)$.

Definition 2.15 (propositional subsumption)**.** Let C, D be sets of labelled clauses. Then C *propositionally subsumes* D, written as $C \trianglelefteq D$ if $\forall d \in D \; \exists c \in C$ with $\mathrm{set}(c) \subseteq \mathrm{set}(d)$.

If C and D are clause sets with $C \trianglelefteq D$ then $\forall$CNF(C) implies $\forall$CNF(D) and $\exists$DNF(D) implies $\exists$DNF(C).

Definition 2.16. Let F, G, H be quantifier-free formulas. We define the rewrite rules:

$$\begin{array}{llll} \text{(I)} & F \to G \mapsto \neg F \vee G & \text{(DN)} & \neg\neg F \mapsto F \\ \text{(M1)} & \neg(F \wedge G) \mapsto \neg F \vee \neg G & \text{(M2)} & \neg(F \vee G) \mapsto \neg F \wedge \neg G \\ & \text{(C1)} & F \vee (G \wedge H) \mapsto (F \vee G) \wedge (F \vee H) & \\ & \text{(C2)} & (G \wedge H) \vee F \mapsto (G \vee F) \wedge (H \vee F) & \\ & \text{(D1)} & F \wedge (G \vee H) \mapsto (F \wedge G) \vee (F \wedge H) & \\ & \text{(D1)} & (G \vee H) \wedge F \mapsto (G \wedge F) \vee (H \wedge F) & \end{array}$$

Note that all these rewrite rules preserve logical equivalence. We define two rewrite relations: $\mapsto_{\text{CNF}}$ as the reflexive, transitive and compatible closure of $\{(\text{I}), (\text{DN}), (\text{M1}), (\text{M2}), (\text{C1}), (\text{C2})\}$ and $\mapsto_{\text{DNF}}$ as the reflexive, transitive and compatible closure of $\{(\text{I}), (\text{DN}), (\text{M1}), (\text{M2}), (\text{D1}), (\text{D2})\}$.

Definition 2.17. Let F be a quantifier-free formula, let $\bigwedge_{i=1}^{k} \bigvee_{j=1}^{l_i} L_{i,j}$ be a normal form of F under $\mapsto_{\text{CNF}}$ and let $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} M_{i,j}$ be a normal form of F under $\mapsto_{\text{DNF}}$. We define the clause sets

$$\text{CNF}(F) := \{\{L_{1,1}, \ldots, L_{1,l_1}\}, \ldots, \{L_{k,1}, \ldots, L_{k,l_k}\}\}$$

$$\text{DNF}(F) := \{\{M_{1,1}, \ldots, M_{1,m_1}\}, \ldots, \{M_{n,1}, \ldots, M_{n,m_n}\}\}$$

These clause sets are well-defined because both $\mapsto_{\text{CNF}}$ and $\mapsto_{\text{DNF}}$ are strongly normalizing and confluent up to commutativity of $\wedge$ and $\vee$.

Definition 2.18 (dualization)**.** Let L be a literal, then $\overline{L}$ denotes the dual of L, i.e. if $L = P(t_1, \ldots, t_n)$ then $\overline{L} = \neg P(t_1, \ldots, t_n)$ and if $L = \neg P(t_1, \ldots, t_n)$ then $\overline{L} = P(t_1, \ldots, t_n)$.
Let $c = \{L_1, \ldots, L_n\}_S$ be a clause with label set S, then $\overline{c} := \{\overline{L_1}, \ldots, \overline{L_n}\}_S$.
Let $C = \{c_1, \ldots, c_m\}$ be a clause set, then $\overline{C} := \{\overline{c_1}, \ldots, \overline{c_m}\}$.

Note that the dual of the empty clause is the empty clause and - similarly - the dual of the empty clause set is the empty clause set. Also note that for any literal L, any clause c and any clause set C: $\overline{\overline{L}} = L$, $\overline{\overline{c}} = c$ and $\overline{\overline{C}} = C$.

Lemma 2.4. Let C, D be sets of labelled clauses, let L be a set of labels and let F be a label selection formula. Then

1. $\overline{C \cup D} = \overline{C} \cup \overline{D}$
2. $\overline{C \times D} = \overline{C} \times \overline{D}$
3. $\overline{C^F} = \overline{C}^F$
4. $\overline{C \times_L D} = \overline{C} \times_L \overline{D}$.

Proof. by definition. □

2.3.2 Resolution

The resolution calculus works in a restricted syntax of first-order formulas: On universally quantified conjunctive normal forms. On the propositional level this means a transformation into a conjunction of disjunctions of literals. On the first-order level this means an elimination of one type of quantifier: The strong quantifiers which are – in the formulation of resolution as a refutational procedure – the existential quantifiers. These quantifiers are removed with a technique due to Th. Skolem which is therefore commonly called Skolemization [46]. There are different types of skolemizations which may strongly differ in the proof complexity of the transformed formula (see [6]). Below we define the structural skolemization operator sk.

Definition 2.19. Let B be a formula. If $(\forall x)$ occurs positively (negatively) in B then $(\forall x)$ is called a strong (weak) quantifier. If $(\exists x)$ occurs positively (negatively) in B then $(\exists x)$ is called a weak (strong) quantifier.

Definition 2.20 (skolemization)**.** sk is a function which maps closed formulas into closed formulas; it is defined in the following way: $sk(F) = F$ if F does not contain strong quantifiers, and

$$sk(F) = sk(F_{(Qy)}\{y \leftarrow f(x_1, \ldots, x_n)\})$$

if (Qy) is a strong quantifier and is in the scope of the weak quantifiers $(Q_1x_1), \ldots, (Q_nx_n)$ (appearing in this order) and $F_{(Qy)}$ denotes F after omission of (Qy) and f is a function symbol which does not occur in F (if $n = 0$ then f is a constant symbol).

A skolemized formula does not contain any strong quantifiers. The skolemization operator can be extended to skolemize also proofs, where a skolemized proof does not contains strong quantifiers in the end-sequent (and therefore also not in the ancestors of the end-sequent). The cut formulas cannot be skolemized, so the cut-formulas of a skolemized proof still contain strong and weak quantifiers. The skolemization of proofs roughly works by skolemizing the end-sequent and propagating these changes upwards in the proof – eigenvariables are replaced by skolem terms. For a complete definition see [7, Proposition 4.2].

The key technique underlying the resolution calculus is unification.

Definition 2.21 (unifier)**.** Let s and t be two terms.

A substition σ s.t. $s\sigma = t\sigma$ is called a *unifier* of s and t.

s and t are called *unifiable* if there exists a unifier.

A unifier θ is called *most general unifier* (mgu) if for all unifiers σ there exits a substitution τ s.t. $\theta\tau = \sigma$.

The notion of unifier is extended from pairs of terms to sets of terms, sets of atoms and sets of literals. The essential point is that unifiability is decidable and that whenever unification is possible there exists a most general unifier.

Theorem 2.3 (unification)**.** There is an algorithm taking two atoms A_1 and A_2 as input that has the following properties:

1. If A_1 and A_2 are unifiable, the algorithm computes a most general unifier of A_1 and A_2.
2. If A_1 and A_2 are not unifiable, the algorithm stops with failure.

Definition 2.22 (resolvent)**.** Let $c = \{L_1, \ldots, L_n\}, d = \{M_1, \ldots, M_k\}$ be variable-disjoint clauses.

If the two literals, L_1 and $\overline{M_1}$ are unifiable with mgu σ, then

$$\{L_2, \ldots, L_n, M_2, \ldots, M_k\}\sigma$$

is called *binary resolvent* of c and d.

Let σ be a mgu of some literals in c. Then the clause set set$(c\sigma)$ is called *factor* of c. Let c' and d' be factors of c and d. Then a binary resolvent of c' and d' is called *resolvent* of c and d.

Definition 2.23 (resolution refutation)**.** Let C be a set of clauses. A list of clauses $c_1, \ldots, c_n$ is called a *resolution refutation* of C if c_n is the empty clause and for all $i = 1, \ldots, n$:

1. c_i is a clause $c \in C$ modulo variable renaming or
2. c_i is a resolvent of clauses c_j, c_k with $j, k < i$.

A resolution refutation as defined above is a list of clauses. One can easily transform such a refutation in list form into one in tree form with resolution as binary rule and factorization as unary rule.

Theorem 2.4 (completeness)**.** If C is an unsatisfiable set of clauses, then there exists a resolution refutation of C.

Definition 2.24 (ground instance)**.** Let c be a clause and let σ be a substitution s.t. all variables of c are replaced by variable-free terms. Then $c\sigma$ is called *ground instance* of c.

Definition 2.25 (propositional resolvent)**.** Let $c = \{L_1, \ldots, L_n\}$, $d = \{M_1, \ldots, M_k\}$ be clauses s.t. $\overline{L_1} = M_1$, then

$$\{L_2, \ldots, L_n, M_1, \ldots, M_k\}$$

is called *propositional resolvent* of c and d.

Definition 2.26. Let C be a set of clauses. A list of clauses $c_1, \ldots, c_n$ is called a *ground resolution refutation* of C if c_n is the empty clause and for all $i = 1, \ldots, n$:

1. c_i is a ground instance of a clause $c \in C$ or
2. c_i is a propositional resolvent of clauses c_j, c_k with $j, k < i$.

Theorem 2.5. If γ is a resolution refutation of a clause set C then there exists a ground resolution refutation γ' of C.

Proof Sketch. By computing a global most general unifier. □

2.4 Cut-Elimination by Resolution (CERES)

Most cut-elimination methods, and in particular those based on the rewrite system $\rightarrow_{\mathrm{G}}$ described in Section 2.2, have one common property: Being based on syntactic reductions they preserve the ancestral structure of the proof. In this section we will describe a more liberal cut-elimination method that is based on a global logical analysis of a proof. The result of this first phase of analysis is a description of key properties of the proof in the form of a characteristic clause set. In a second phase a resolution refutation of this clause set is generated and then serves as a skeleton of the cut-free proof. This method: cut-elimination by resolution (CERES) has been introduced in [8] and further developed in [10, 9, 3, 4].

Definition 2.27. Let φ be a skolemized **LK**-proof and let M be a closed set of formula occurrences. We define the *characteristic clause set* $\mathrm{CL}(\varphi)$ of φ w.r.t. M as follows:

1. If φ is an axiom sequent s, then
$$\mathrm{CL}_M(\varphi) := \mathrm{S}(s, M)$$
2. If φ ends with a unary rule, let φ' be the sub-proof of φ and let M' be the subset of M that occurs in φ'. Then
$$\mathrm{CL}_M(\varphi) := \mathrm{CL}_{M'}(\varphi')$$
3. If φ ends with a binary rule ρ, let φ_1 and φ_2 be the immediate sub-proofs of φ and let M_1 and M_2 be the subsets of M that occur in φ_1 and φ_2 respectively.
   (a) If the auxiliary occurrences of ρ are in M then
$$\mathrm{CL}_M(\varphi) := \mathrm{CL}_{M_1}(\varphi_1) \cup \mathrm{CL}_{M_2}(\varphi_2)$$

(b) If the auxiliary occurrences of ρ are not in Ω then

$$\mathrm{CL}_M(\varphi) := \mathrm{CL}_{M_1}(\varphi_1) \times \mathrm{CL}_{M_2}(\varphi_2)$$

Let $\Omega(\varphi)$ denote the set of all ancestors of cut occurrences in φ. We define $\mathrm{CL}(\varphi) := \mathrm{CL}_{\Omega(\varphi)}(\varphi)$.

Example 2.6. Consider the following proof $\varphi =$

$$\dfrac{(\varphi_1) \quad (\varphi_2)}{(\forall x)(P(x) \to Q(x)) \vdash P(a) \to (\exists y)Q(y)}\ \text{cut}$$

where $\varphi_1 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \to Q(u) \vdash Q(u)}\ \to : \mathrm{l}}{P(u) \to Q(u) \vdash \neg P(u), Q(u)}\ \neg : \mathrm{l}}{P(u) \to Q(u) \vdash \neg P(u) \vee Q(u)}\ \vee : \mathrm{r}}{P(u) \to Q(u) \vdash (\exists y)(\neg P(u) \vee Q(y))}\ \exists : \mathrm{r}}{(\forall x)(P(x) \to Q(x)) \vdash (\exists y)(\neg P(u) \vee Q(y))}\ \forall : \mathrm{l}}{(\forall x)(P(x) \to Q(x)) \vdash (\forall x)(\exists y)(\neg P(x) \vee Q(y))}\ \forall : \mathrm{r}$$

and $\varphi_2 =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(a) \vdash P(a)}{P(a), \neg P(a) \vdash}\ \neg : \mathrm{l} \quad Q(v) \vdash Q(v)}{P(a), \neg P(a) \vee Q(v) \vdash Q(v)}\ \vee : \mathrm{l}}{P(a), \neg P(a) \vee Q(v) \vdash (\exists y)Q(y)}\ \exists : \mathrm{r}}{P(a), (\exists y)(\neg P(a) \vee Q(y)) \vdash (\exists y)Q(y)}\ \exists : \mathrm{l}}{P(a), (\forall x)(\exists y)(\neg P(x) \vee Q(y)) \vdash (\exists y)Q(y)}\ \forall : \mathrm{l}}{(\forall x)(\exists y)(\neg P(x) \vee Q(y)) \vdash P(a) \to (\exists y)Q(y)}\ \to : \mathrm{r}$$

Here

$$\begin{aligned} \mathrm{CL}(\varphi) &= (\{P(u) \vdash\} \times \{\vdash Q(u)\}) \cup (\{\vdash P(a)\} \cup \{Q(v) \vdash\}) \\ &= \{P(u) \vdash Q(u)\,;\, \vdash P(a)\,;\, Q(v) \vdash\} \end{aligned}$$

where the product $\times$ comes from the $\to :$ l-rule in φ_1, the right union comes from the $\vee$: l-rule in φ_2 and the left union comes from the cut.

Theorem 2.6. Let φ be a skolemized **LK**-proof. Then $\mathrm{CL}(\varphi)$ is unsatisfiable.

Proof. A direct proof can be found in [8]. For an alternative argument see Corollary 4.2. □

The above property of the unsatisfiability of CL(φ) is crucial: By the completeness of resolution (Theorem 2.4), there exists a refutation of CL(φ).

In addition to the unsatisfiability, the characteristic clause set has the property that for each clause $c \in \mathrm{CL}(\varphi)$ there exists a cut-free proof of $s \circ c$ where s is the end-sequent of φ. This proof is called the *projection* to c and can easily be constructed from φ. The projections prove weaker statements than φ as $\circ$ has the logical meaning of a disjunction, but they prove it without cuts. Structurally this process of building the characteristic clause set and the set of corresponding projections is a decomposition of the original proof into its cut-free parts. One clause corresponds exactly to one such cut-free part (the projection). Logically this clause is the difference between the full end-sequent and the weaker statement proved by the cut-free part.

Theorem 2.7. Let φ be a skolemized **LK**-proof of a sequent s and let $c \in \mathrm{CL}(\varphi)$. Then there exists a cut-free proof ψ of the sequent $s \circ c$.

Proof. see [8]. □

Theorem 2.8 (cut-elimination by CERES)**.** Let φ be a skolemized **LK**-proof. Then there exists an **LK**-proof φ' with only atomic cuts of the same end-sequent.

Proof. By the unsatisfiability of CL(φ) and the completeness of resolution there exists a resolution refutation γ of CL(φ). By Theorem 2.5 there exists a ground resolution refutation γ' corresponding to γ. Interpreting γ' in **LK** by replacing resolution by atomic cuts yields an **LK**-proof γ'' of the empty sequent with clauses $d_1, \ldots, d_n$ as initial sequents. But for each $i = 1, \ldots, n$ there is a substitution σ_i and a clause $c_i \in \mathrm{CL}(\varphi)$ s.t. $c_i\sigma_i = d_i$. By replacing these initial sequents of γ'' by their respective projections $\psi_{c_i}\sigma_i$ we obtain a proof of $s \circ \ldots \circ s$ with only atomic cuts. By applying contractions to the end of this proof we obtain the end-sequent s. □

The output of the CERES-method is proof that has only atomic cuts: an *atomic cut normal form*. In the calculus used in this thesis, these atomic cuts could easily be eliminated by employing the cut-reduction rules $\rightarrow_{\mathrm{G}}$. The proof projections have the property that no weakenings and no contractions are applied to ancestors of the clause. Hence $\rightarrow_{\mathrm{G}}$ on the atomic cut normal forms is strongly normalizing and confluent modulo rule permutations. Furthermore the size of the proof strictly decreases. An atomic cut normal form is therefore just another notation of a cut-free proof. Moreover, the elimination of atomic cuts is – in principle – not possible in other (more sophisticated) calculi. For example, the calculus $\mathbf{LK_e}$ in [49] axiomatizes equality by including atomic axiom sequents for the reflexivity and compatibility of $=$ (symmetry and transitivity can be derived). In $\mathbf{LK_e}$ only

such cuts can be eliminated whose cut-formula is not of the form $s = t$. Another example is the extension of the CERES-method in [4] to a calculus **LKDe** which axiomatizes equality and the use of definitions – two forms of reasoning that are very important for the formalization of mathematical proofs.

One important advantage of the CERES-method is its high flexibility concerning syntactic details of the calculus. The definition of the characteristic clause set as well as the construction of the projections is not dependent on wether the rules are multiplicative or additive, on wether weakening and contraction are implicit or explicit, on wether a sequent is a pair of sets, multisets or sequences, etc. It is even possible to eliminate *pseudo-cuts*:

$$\frac{\Gamma \vdash \Delta, A \quad B, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{pscut}$$

where $A \models B$. In this case the resolution refutation will "fill up the gap" between A and B.

Another advantage of the CERES-method is that the underlying calculus (resolution) is very redundancy-free (compared to the sequent calculus). There exist powerful techniques for redundancy deletion in clause logic like subsumption and tautology-deletion which proved very useful in automated theorem proving.

In [10] it has been shown that every atomic cut normal form calculated by a syntactic cut-elimination procedure is subsumed by one calculated by CERES. Thus CERES is a generalization of syntactic cut-elimination à la Gentzen. This is shown by analyzing the development of the characteristic clause set under cut-elimination: If φ reduces to φ', the characteristic clause set $\mathrm{CL}(\varphi)$ subsumes $\mathrm{CL}(\varphi')$.

Note that the projections are strictly smaller than the original proof and that the size of the characteristic clause set is at most exponential in the number of binary rules that work on ancestors of the end-sequent. It is a well-known result that cut-elimination in first-order logic can yield a non-elementary expansion of the size of the proof (see [47, 41, 43]). So the main complexity of the method lies in finding a resolution refutation of the characteristic clause set.

Chapter 3

The Proof Profile

In this chapter we will define the profile of a proof. It consists of four components, each of them a clause set, which are closely related. The profile is a refined and improved variant of the characteristic clause sets of the CERES-method.

3.1 Definition of the Proof Profile

The four components of the profile will be called $\Omega, \Omega\mathrm{T}, \Sigma$ and $\Sigma\mathrm{T}$ where Ω refers to the part of the proof consisting of ancestors of cut-formulas, Σ refers to the part of the proof consisting of ancestors of the end-sequent and the respective T-versions contain some additional tautological clauses.

Before defining the profile, we need some more technical notions for talking about **LK**-proofs. For a proof φ an occurrence of a formula in the end-sequent will be called *end occurrence*, an auxiliary occurrence of a cut-rule will be called *cut occurrence* and if μ is either an end occurrence or a cut occurrence it will be called *terminal occurrence*. Note that each occurrence is ancestor of exactly one terminal occurrence.

Let M be a set of formula occurrences. M is called *ancestor-closed* if $\mu \in M \Leftrightarrow$ all ancestors of μ are in M. M is called *cut-closed* if for each instance of the cut rule either both cut occurrences are in M or both are not in M. M is called *closed* if it is ancestor-closed and cut-closed. If M is a closed set of formula occurrence then for each rule ρ either all active occurrences are in M or none of the active occurrences is in M - we say ρ *operates on* M in the first case and ρ *does not operate on* M in the second. For a non-empty set of formula occurrences M, the *ancestor-closure* of M, written as $\langle M \rangle$ is defined as the set of all ancestors of occurrences from M.

Definition 3.1 (Ω-proof profiles)**.** Let φ be an **LK**-proof, let M be a closed set of formula occurrences. We define the proof profiles $\mathrm{P}^{\Omega}_{M}(\varphi)$ and $\mathrm{P}^{\Omega\mathrm{T}}_{M}(\varphi)$

by induction on φ as the following sets of labelled clauses:

1. φ is an axiom α with label l. Let $\mu_1, \ldots, \mu_m$ be the literals in $S(\alpha, M)$:

$$\mathrm{P}^{\Omega\mathrm{T}}_M(\varphi) := \{\{\mu_1, \ldots, \mu_m\}_{\{l\}}\}$$

$$\mathrm{P}^{\Omega}_M(\varphi) := \begin{cases} \emptyset \text{ if } S(\alpha, M) = \alpha \\ \mathrm{P}^{\Omega\mathrm{T}}_M(\varphi) \text{ otherwise} \end{cases}$$

For the rest of this definition let $X \in \{\Omega, \Omega\mathrm{T}\}$ to abbreviate the notation.

2. φ ends with a unary rule. Let φ' be the immediate sub-proof of φ and let M' be the subset of M that occurs in φ'. Then

$$\mathrm{P}^X_M(\varphi) := \mathrm{P}^X_{M'}(\varphi')$$

3. φ ends with a binary rule ρ. Let φ_1 and φ_2 be the immediate sub-proofs of φ. Let M_1 and M_2 be the subsets of M that occur in φ_1 and φ_2 respectively. We distinguish two cases

   (a) ρ operates on M. Then

$$\mathrm{P}^X_M(\varphi) := \mathrm{P}^X_{M_1}(\varphi_1) \cup \mathrm{P}^X_{M_2}(\varphi_2)$$

   (b) ρ does not operate on M. Then

$$\mathrm{P}^X_M(\varphi) := \mathrm{P}^X_{M_1}(\varphi_1) \times_{\mathcal{L}(\rho)} \mathrm{P}^X_{M_2}(\varphi_2)$$

Definition 3.2 (Σ-proof profiles)**.** Let φ be an **LK**-proof, let N be a closed set of formula occurrences. We define the proof profiles $\mathrm{P}^{\Sigma}_N(\varphi)$ and $\mathrm{P}^{\Sigma\mathrm{T}}_N(\varphi)$ of φ by induction on φ as the following sets of labelled clauses:

1. φ is an axiom α with label l. Let $\nu_1, \ldots, \nu_n$ be the literals in $S(\alpha, N)$.:

$$\mathrm{P}^{\Sigma\mathrm{T}}_N(\varphi) := \{\{\nu_1\}_{\{l\}}, \ldots, \{\nu_n\}_{\{l\}}\}$$

$$\mathrm{P}^{\Sigma}_N(\varphi) := \begin{cases} \{\emptyset_{\{l\}}\} \text{ if } S(\alpha, N) = \alpha \\ \mathrm{P}^{\Sigma\mathrm{T}}_N(\varphi) \text{ otherwise} \end{cases}$$

For the rest of this definition let $X \in \{\Sigma, \Sigma\mathrm{T}\}$ to abbreviate the notation.

2. φ ends with a unary rule. Let φ' be the immediate sub-proof of φ. Let N' be the subset of N that occurs in φ'. Then

$$\mathrm{P}^X_N(\varphi) := \mathrm{P}^X_{N'}(\varphi')$$

3. φ ends with a binary rule ρ. Let φ_1 and φ_2 be the immediate subproofs of φ and let N_1 and N_2 be the subsets of N that occur in φ_1 and φ_2 respectively. We distinguish two cases

   (a) ρ operates on N. Then

   $$\mathrm{P}^X_N(\varphi) := \mathrm{P}^X_{N_1}(\varphi_1) \times_{\mathcal{L}(\rho)} \mathrm{P}^X_{N_2}(\varphi_2)$$

   (b) ρ does not operate on N. Then

   $$\mathrm{P}^X_N(\varphi) := \mathrm{P}^X_{N_1}(\varphi_1) \cup \mathrm{P}^X_{N_2}(\varphi_2)$$

Note that these sets are indeed clause sets because the axioms consist only of atomic formulas. We will interpret the Ω-Profiles as universally quantified conjunctive normal forms while the Σ-Profiles will be interpreted as existentially quantified disjunctive normal forms. For a proof φ we will denote with $\Omega(\varphi)$ the closure of the set of cut occurrences and with $\Sigma(\varphi)$ the closure of the set of end occurrences. We will abbreviate $\mathrm{P}^\Omega(\varphi) := \mathrm{P}^\Omega_{\Omega(\varphi)}(\varphi)$, $\mathrm{P}^{\Omega\mathrm{T}}(\varphi) := \mathrm{P}^{\Omega\mathrm{T}}_{\Omega(\varphi)}(\varphi)$, $\mathrm{P}^\Sigma(\varphi) := \mathrm{P}^\Sigma_{\Sigma(\varphi)}(\varphi)$ and $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) := \mathrm{P}^{\Sigma\mathrm{T}}_{\Sigma(\varphi)}(\varphi)$. Note that $\mathrm{P}^\Omega(\varphi)$ (as $\mathrm{CL}(\varphi)$) has the important property of being unsatisfiable - a fact that is at the core of the cut-elimination method CERES.

3.1.1 Duality

Definition 3.3 (proper partition)**.** An ordered pair $(M; N)$ of sets of formula occurrences from a proof φ is called *proper partition* of φ if

1. $M = \langle M' \rangle, N = \langle N' \rangle$ and
2. $M' \cup N'$ contains all terminal occurrences and
3. N contains only end occurrences.

We will notate proper partitions also as $M \uplus N$ instead of $(M; N)$.

Proposition 3.1. Let φ be an **LK**-proof. Then

$$\overline{\mathrm{P}^\Omega(\varphi)} = \mathrm{P}^\Sigma(\varphi) \text{ and } \overline{\mathrm{P}^\Sigma(\varphi)} = \mathrm{P}^\Omega(\varphi)$$

Proof. We will show the following stronger statement by induction on φ: Let $M \uplus N$ be a proper partition of φ. Then

$$\overline{\mathrm{P}^\Omega_M(\varphi)} = \mathrm{P}^\Sigma_N(\varphi) \text{ and } \overline{\mathrm{P}^\Sigma_N(\varphi)} = \mathrm{P}^\Omega_M(\varphi)$$

If φ is an axiom α with label l there are three cases: (1) If $N = \emptyset$ then $\mathrm{P}^\Sigma_N(\varphi) = \emptyset$ and $\mathrm{P}^\Omega_M(\varphi) = \emptyset$. (2) If $M = \emptyset$ then $\mathrm{P}^\Omega_M(\varphi) = \{\emptyset_{\{l\}}\}$ and

$\mathrm{P}^{\Sigma}_{N}(\varphi) = \{\emptyset_{\{l\}}\}$. (3) If both $M \neq \emptyset$ and $N \neq \emptyset$ then there is a literal L s.t. $\mathrm{P}^{\Omega}_{M}(\varphi) = \{\{L\}_{\{l\}}\}$ and $\mathrm{P}^{\Sigma}_{N}(\varphi) = \{\{\overline{L}\}_{\{l\}}\}$.

If φ ends with a unary rule, the result follows immediately by the induction hypothesis. If φ ends with a binary rule ρ, let φ_1 and φ_2 be the immediate sub-proofs of φ and let $M_1(M_2)$ and $N_1(N_2)$ be the subsets of M and N occurring in $\varphi_1(\varphi_2)$. As $M \uplus N$ is a proper partition ρ either operates on M or on N, so either

$$\mathrm{P}^{\Omega}_{M}(\varphi) = \mathrm{P}^{\Omega}_{M_1}(\varphi_1) \cup \mathrm{P}^{\Omega}_{M_2}(\varphi_2) \quad \text{and} \quad \mathrm{P}^{\Sigma}_{N}(\varphi) = \mathrm{P}^{\Sigma}_{N_1}(\varphi_1) \cup \mathrm{P}^{\Sigma}_{N_2}(\varphi_2)$$

or

$$\mathrm{P}^{\Omega}_{M}(\varphi) = \mathrm{P}^{\Omega}_{M_1}(\varphi_1) \times_{\mathcal{L}(\rho)} \mathrm{P}^{\Omega}_{M_2}(\varphi_2) \quad \text{and} \quad \mathrm{P}^{\Sigma}_{N}(\varphi) = \mathrm{P}^{\Sigma}_{N_1}(\varphi_1) \times_{\mathcal{L}(\rho)} \mathrm{P}^{\Sigma}_{N_2}(\varphi_2)$$

In both cases the induction hypothesis can be applied because $M_1 \uplus N_1$ is a proper partition of φ_1 and $M_2 \uplus N_2$ is a proper partition of φ. The result then follows from Lemma 2.4. □

Definition 3.4. We define the profile $\mathrm{P}(\varphi)$ of the proof φ as the ordered pair $(\mathrm{P}^{\Omega}(\varphi); \mathrm{P}^{\Sigma}(\varphi))$.

Lemma 3.1. Let C and D be clause sets, F be a label selection formula, let π be a permutation on labels and variables and let σ be a substitution. Then dualization of clause sets has the following compatibility properties:

1. $\overline{C \cup D} = \overline{C} \cup \overline{D}$
2. $\overline{C \times D} = \overline{C} \times \overline{D}$
3. $\overline{C^F} = \overline{C}^F$
4. $\overline{C \times_F D} = \overline{C} \times_F \overline{D}$
5. $\overline{C\sigma} = \overline{C}\sigma$
6. $\overline{C\pi} = \overline{C}\pi$

The above lemma shows that these operations can be performed on the pair $\mathrm{P}(\varphi)$ by performing it on a single component and then calculating the other component by dualization.

3.2 Basic Properties

3.2.1 The Relation between the Ω-Sets

In this section we will show that $\mathrm{P}^{\Omega}(\varphi)$ and $\mathrm{P}^{\Omega\mathrm{T}}(\varphi)$ differ only by tautologies and are thus logically equivalent.

Definition 3.5 (tautology-deletion)**.** Let C and D be sets of clauses. We write $C \leq^{\mathrm{T}} D$ if

1. $C \subseteq D$ and
2. $\forall c \in D \setminus C$ there is a literal L s.t. $\{L, \overline{L}\} \subseteq c$.

For $C \leq^{\mathrm{T}} D$, the formulas $\forall\mathrm{CNF}(C)$ and $\forall\mathrm{CNF}(D)$ as well as $\exists\mathrm{DNF}(C)$ and $\exists\mathrm{DNF}(D)$ are logically equivalent because $D \setminus C$ contains only tautology clauses.

Lemma 3.2 (compatibility of $\leq^{\mathrm{T}}$)**.** Let C, C', D, D' be sets of clauses with $C \leq^{\mathrm{T}} C'$ and $D \leq^{\mathrm{T}} D'$ and let F be a label selection formula. Then

1. $C \cup D \leq^{\mathrm{T}} C' \cup D'$
2. $C \times D \leq^{\mathrm{T}} C' \times D'$
3. $C^F \leq^{\mathrm{T}} (C')^F$
4. $C \times_F D \leq^{\mathrm{T}} C' \times_F D'$

Proof.

1. As both $C' \setminus C$ and $D' \setminus D$ contain only tautologies, so does $(C' \cup D') \setminus (C \cup D)$ because $(C' \cup D') \setminus (C \cup D) \subseteq (C' \setminus C) \cup (D' \setminus D)$.
2. Let $c \circ d \in (C' \times D') \setminus (C \times D)$. Then $c \in C' \setminus C$ or $d \in D' \setminus D$ (or both). Assume w.l.o.g. $c \in C' \setminus C$. Then - as $C \leq^{\mathrm{T}} C'$ - there is a literal L s.t. $\{L, \overline{L}\} \subseteq c$, so $\{L, \overline{L}\} \subseteq c \circ d$. Therefore $C \times D \leq^{\mathrm{T}} C' \times D'$
3. As every $c \in C' \setminus C$ is a tautology, so is every $d \in (C')^F \setminus C^F$ because $(C')^F \setminus C^F = (C' \setminus C)^F \subseteq C' \setminus C$.
4. Follows from 1-3.

□

Proposition 3.2. Let φ be an **LK**-proof and let M be a closed set of formula occurrences. Then

$$\mathrm{P}^{\Omega}_{M}(\varphi) \leq^{\mathrm{T}} \mathrm{P}^{\Omega\mathrm{T}}_{M}(\varphi)$$

Proof. By induction on φ: If φ is an axiom sequent α then $\mathrm{P}^{\Omega}_{M}(\varphi) = \mathrm{P}^{\Omega\mathrm{T}}_{M}(\varphi)$ except if $S(\alpha, M) = \alpha$. In this case $\mathrm{P}^{\Omega}_{M}(\varphi) = \emptyset$ and $\mathrm{P}^{\Omega\mathrm{T}}_{M}(\varphi) = \{\alpha\}$, but then clearly $\mathrm{P}^{\Omega}_{M}(\varphi) \leq^{\mathrm{T}} \mathrm{P}^{\Omega\mathrm{T}}_{M}(\varphi)$. If φ ends with a unary rule the result follows directly from the induction hypothesis. If φ ends with a binary rule, the result follows from the induction hypothesis and Lemma 3.2 in both cases. □

3.2.2 The Relation between the Σ-Sets

In this section we show that $\mathrm{P}^{\Sigma}(\varphi)$ and $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi)$ differ only by a simple kind of redundancy are are thus also logically equivalent.

Definition 3.6 (redundancy-elimination)**.** Let C and D be sets of labelled clauses. We write $C \leq^{\mathrm{R}^1} D$ if there are clauses $c \in C, d_1, d_2 \in D$ with $d_1 = c \cup \{A\}, d_2 = c \cup \{\neg A\}$ and a set of labelled clauses E with $C = E \uplus \{c\}, D = E \uplus \{d_1, d_2\}$. We write $\leq^{\mathrm{R}}$ for the reflexive and transitive closure of $\leq^{\mathrm{R}^1}$.

For $C \leq^{\mathrm{R}} D$ the formulas $\forall\mathrm{CNF}(C)$ and $\forall\mathrm{CNF}(D)$ as well as $\exists\mathrm{DNF}(C)$ and $\exists\mathrm{DNF}(D)$ are logically equivalent. For technical reasons we introduce the following relation describing a labelled redundancy-elimination.

Definition 3.7 (labelled redundancy-elimination)**.** Let C and D be sets of labelled clauses. We write $C \leq^{\mathrm{R}^1_{\mathrm{L}}} D$ if there is an unlabeled clause γ, a label l, a label set L and labelled clauses $c \in C, d_1, d_2 \in D$ s.t. $c = \gamma_{L\cup\{l\}}, d_1 = \gamma_L \cup \{A\}_{\{l\}}, d_2 = \gamma_L \cup \{\neg A\}_{\{l\}}$ and $C = E \uplus \{c\}, D = E \uplus \{d_1, d_2\}$ for some clause set E. We again write $\leq^{\mathrm{R}_{\mathrm{L}}}$ for the reflexive and transitive closure of $\leq^{\mathrm{R}^1_{\mathrm{L}}}$.

Lemma 3.3. Let C, C', D, D' be sets of clauses with $C \leq^{\mathrm{R}_{\mathrm{L}}} C'$ and $D \leq^{\mathrm{R}_{\mathrm{L}}} D'$ and let F be a label selection formula. Then

1. $C \cup D \leq^{\mathrm{R}_{\mathrm{L}}} C' \cup D'$
2. $C \times D \leq^{\mathrm{R}_{\mathrm{L}}} C' \times D'$
3. $C^F \leq^{\mathrm{R}_{\mathrm{L}}} (C')^F$
4. $C \times_F D \leq^{\mathrm{R}_{\mathrm{L}}} C' \times_F D'$

Proof. It suffices to show 1-4 with the assumption $C \leq^{\mathrm{R}^1_{\mathrm{L}}} C'$ and $D = D'$. The full result follows by induction and commutativity of $\cup, \times$ and $\times_L$. So we assume that there is an unlabeled clause γ, a label l, a label set L and clauses $c \in C, c_1, c_2 \in C'$ with $c = \gamma_{L\cup\{l\}}, c_1 = \gamma_L \cup \{A\}_{\{l\}}$ and $c_2 = \gamma_L \cup \{A\}_{\{l\}}$.

1. Clearly also $c \in C \cup D$ and $c_1, c_2 \in C' \cup D$.
2. For any $d \in D$ we have $c \circ d \in C \times D$ and $c_1 \circ d, c_2 \circ d \in C' \times D$, so $C \times D \leq^{\mathrm{R}_{\mathrm{L}}} C' \times D$.
3. As $\mathcal{L}(c) = \mathcal{L}(c_1) = \mathcal{L}(c_2)$ either $c \in C^F$ and $c_1, c_2 \in (C')^F$ and thus $C^F \leq^{\mathrm{R}^1_{\mathrm{L}}} (C')^F$ or $c \notin C^F$ and $c_1 \notin (C')^F$ and $c_2 \notin (C')^F$ and thus $C^F = (C')^F$.

4. follows from 1-3.

□

Proposition 3.3. Let φ be an **LK**-proof and let N be a closed set of formula occurrences. Then

$$\mathrm{P}^{\Sigma}_{N}(\varphi) \leq^{\mathrm{R}} \mathrm{P}^{\Sigma\mathrm{T}}_{N}(\varphi)$$

Proof. We will show $\mathrm{P}^{\Sigma}_{N}(\varphi) \leq^{\mathrm{R_L}} \mathrm{P}^{\Sigma\mathrm{T}}_{N}(\varphi)$ by induction on φ: If φ is an axiom sequent α then $\mathrm{P}^{\Sigma}_{N}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}_{N}(\varphi)$ except if $\mathrm{S}(\alpha, N) = \alpha$. In this case $\mathrm{P}^{\Sigma}_{N}(\varphi) = \{\emptyset_{\{l\}}\}, \mathrm{P}^{\Sigma\mathrm{T}}_{N}(\varphi) = \{\{A\}_{\{l\}}, \{\neg A\}_{\{l\}}\}$ and $\mathrm{P}^{\Sigma}_{N}(\varphi) \leq^{\mathrm{R^1_L}} \mathrm{P}^{\Sigma\mathrm{T}}_{N}(\varphi)$. If φ ends with a unary rule, the result follows directly from the induction hypothesis. If φ ends with a binary rule, the result follows from the induction hypothesis and Lemma 3.3. □

3.3 CERES with the Proof Profile

In this section we will show that the proof profile P^{Ω} can replace the characteristic clause set CL in the cut-elimination method CERES. This replacement is an improvement of CERES in several respects: The clause set P^{Ω} always subsumes CL hence for each resolution refutation of CL of length l there will exist one of P^{Ω} of a length $l' \leq l$. Furthermore also the projections to the clauses in P^{Ω} will be at most as large as those to the clauses of CL. Moreover, there exist proof sequences that have a constant size normal form with CERES with P^{Ω} while all normal forms of CERES with CL are of non-elementary size.

3.3.1 Subsumption

We will now show that the profile $\mathrm{P}^{\Omega\mathrm{T}}(\varphi)$ propositionally subsumes the characteristic clause set $\mathrm{CL}(\varphi)$.

Proposition 3.4. Let φ be an **LK**-proof. Then $\mathrm{P}^{\Omega\mathrm{T}}(\varphi) \trianglelefteq \mathrm{CL}(\varphi)$

Proof. By induction on the structure of φ we show the stronger statement that $\mathrm{P}^{\Omega\mathrm{T}}_{M}(\varphi) \trianglelefteq \mathrm{CL}_{M}(\varphi)$ for any closed set of formula occurrences M. The only non-trivial case in proving this is the product case of the definitions of these clause sets. But here the claim follows directly from the observation that $C \times_L D \trianglelefteq C \times D$ for all sets of labelled clauses C and D and for all label sets L. □

Corollary 3.1. Let φ be an **LK**-proof. Then $\mathrm{P}^{\Omega}(\varphi) \trianglelefteq \mathrm{CL}(\varphi)$.

Proof. By Proposition 3.2 we have $\mathrm{P}^{\Omega}(\varphi) \leq^{\mathrm{T}} \mathrm{P}^{\Omega\mathrm{T}}(\varphi)$ so in particular $\mathrm{P}^{\Omega}(\varphi) \subseteq \mathrm{P}^{\Omega\mathrm{T}}(\varphi)$ which entails $\mathrm{P}^{\Omega}(\varphi) \trianglelefteq \mathrm{CL}(\varphi)$. □

3.3.2 Projections

In order to describe the end-sequents produced by the projections (which are all sub-sequents of the original end-sequent) we introduce a description of sub-sets of the end-sequent based on clauses from the profile.

Definition 3.8 (restriction)**.** Let N be a set of formula occurrences and let L be a set of labels. We define the *L-restriction* of N as

$$\mathrm{R}_L(N) := \{\nu \in N \mid \mathcal{L}(\nu) \cap L \neq \emptyset\}$$

Let φ be an **LK**-proof and let $M \uplus N$ be a proper partition of φ. Then for every $c \in \mathrm{P}^{\Omega}_M(\varphi)$ we define

$$\mathrm{R}_c(N) := \mathrm{R}_{\mathcal{L}(c)}(N)$$

So the c-restriction R_c will only contain those formula occurrences in a proof that are connected to c via an axiom. The projection of φ to the clause c will only contain formulas that occur in the c-restriction. This restriction ensures that rules can either be applied fully or not at all which is crucial in the proof below.

Theorem 3.1. Let φ be a skolemized **LK**-proof, let $M \uplus N$ be a proper partition of φ. Then $\forall c \in \mathrm{P}^{\Omega}_M(\varphi)\ \exists \psi$ s.t.

I) ψ is cut-free

II) ψ is a proof of $\mathrm{S}(s, \mathrm{R}_c(N)) \circ c$

Proof.

1. If φ is an axiom, define
$$\psi := \varphi = s$$
I) is obvious, for II) consider that $\mathrm{P}^{\Omega}_M(\varphi) = \{c\}$ with $c = \mathrm{S}(s, M)$, that $\mathrm{R}_c(N) = N$ and that $s = \mathrm{S}(s, M) \circ \mathrm{S}(s, N)$.

2. If φ ends with a unary rule ρ, let φ' be φ without ρ and let M', N' be the subsets of M, N occurring in φ', let s' be the end-sequent of φ'. For $c \in \mathrm{P}^{\Omega}_M(\varphi)$ we also have $c \in \mathrm{P}^{\Omega}_{M'}(\varphi')$.

(a) ρ does not operate on $\mathrm{R}_c(N)$. Then by the induction hypothesis there is a ψ' deriving $\mathrm{S}(s', \mathrm{R}_c(N')) \circ c$. Define

$$\psi := \psi'$$

which I) is cut-free. As ρ does not operate on $\mathrm{R}_c(N)$, $\mathrm{S}(s, \mathrm{R}_c(N)) = \mathrm{S}(s', \mathrm{R}_c(N'))$. and II) ψ is a proof of $\mathrm{S}(s, \mathrm{R}_c(N)) \circ c$.

(b) ρ operates on $\mathrm{R}_c(N)$. Let $\nu \in \mathrm{R}_c(N)$ be the main formula of ρ. We know that ρ is not a weakening (assume it would be, then ν would not have any ancestor axiom and thus could not be in $\mathrm{R}_c(N)$). Furthermore, we know that ρ cannot be a strong quantifier rule by the assumption that φ is skolemized. We make a case distinction on the number of immediate ancestors of ν which must be 1 or 2:

i. ν has exactly one immediate ancestor. This means that every $\nu_0 \in N$ has exactly one ancestor $\nu_0' \in N$ and that furthermore $\mathcal{L}(\nu_0) = \mathcal{L}(\nu_0')$. By the induction hypothesis there is an **LK**-proof ψ' of $\mathrm{S}(s', \mathrm{R}_c(N'))$. Define

$$\psi := \dfrac{\psi'}{\rho}$$

which is I) cut-free and II) applying ρ to $\mathrm{S}(s', \mathrm{R}_c(N'))$ gives the conclusion sequent $\mathrm{S}(s, R_c(N)) \circ c$.

ii. ν has exactly two immediate ancestors, call them ν_1 and ν_2. As ν shares an ancestor axiom with c, we know that at least one of ν_1 and ν_2 share an ancestor axiom with c, let w.l.o.g. this be ν_1. We make a case distinction on wether ν_2 share an ancestor axiom with c.

A. ν_2 shares an ancestor axiom with c. By induction hypothesis there is an **LK**-proof ψ' of $\mathrm{S}(s', \mathrm{R}_c(N')) \circ c$. Define

$$\psi := \dfrac{\psi'}{\rho}$$

which I) is cut-free. Both ν_1 and ν_2 are in $\mathrm{R}_c(N')$ so we can apply ρ to $\mathrm{S}(s', \mathrm{R}_c(N')) \circ c$ and II) obtain $\psi : \mathrm{S}(s, \mathrm{R}_c(N))$ because the context formulas $\nu_0 \in \mathrm{R}_c(N)$ each have exactly one ancestor $\nu_0' \in N'$ which is also in $\mathrm{R}_c(N')$.

B. ν_2 does not share an ancestor axiom with c. By induction hypothesis there is a proof ψ' of $\mathrm{S}(s', \mathrm{R}_c(N')) \circ c$. Let ω be a weakening rule that adds the formula of ν_2 and define

$$\psi := \dfrac{\psi'}{\omega}$$

which I) is cut-free. As ψ' derives $\mathrm{S}(s', \mathrm{R}_c(N')) \circ c$, ψ' with ω derives $\mathrm{S}(s', \mathrm{R}_c(N')) \circ c \circ [\nu_2]$. As ν_1 shares an ancestor axiom with c, it is in $\mathrm{R}_c(N')$ and application of ρ gives II) the proof ψ of $\mathrm{S}(s, \mathrm{R}_c(N)) \circ c$

3. If φ ends with a binary rule ρ, let s_1, s_2 be the end-sequents of the immediate sub-proofs φ_1, φ_2 of φ and let M_1, M_2 and N_1, N_2 be the subsets of M and N occurring in φ_1, φ_2.

   (a) ρ does not operate on $\mathrm{R}_c(N)$. Then either ρ operates on M in which case $c \in \mathrm{P}^{\Omega}_{M_1}(\varphi_1) \cup \mathrm{P}^{\Omega}_{M_2}(\varphi_2)$ or it operates on $N \setminus \mathrm{R}_c(N)$ in which case even $c \in \mathrm{P}^{\Omega}_{M_1}(\varphi_1)^{\neg\mathcal{L}(\rho)} \cup \mathrm{P}^{\Omega}_{M_2}(\varphi_2)^{\neg\mathcal{L}(\rho)}$. In any case let w.l.o.g. be $c \in \mathrm{P}^{\Omega}_{M_1}(\varphi_1)$. By induction hypothesis there is a ψ_1' deriving $\mathrm{S}(s_1', \mathrm{R}_c(N_1)) \circ c$. Define

   $$\psi := \psi_1'$$

   which I) is cut-free. For II) observe that $\mathrm{R}_c(N)$ does not contain the main and auxiliary formulas of ρ. Furthermore, as $c \in \mathrm{P}^{\Omega}_{M_1}(\varphi_1)$ the ancestor axioms of c are all from φ_1 so c cannot have an ancestor axiom in common with any formula from φ_2. Therefore $\mathrm{S}(s_1, \mathrm{R}_c(N_1)) = \mathrm{S}(s, \mathrm{R}_c(N))$ and hence ψ derives $\mathrm{S}(s, \mathrm{R}_c(N)) \circ c$.

   (b) ρ operates on $\mathrm{R}_c(N)$. This means that c is a ρ-clause, so $c = c_1 \circ c_2$ where both, c_1 and c_2 are ρ-clauses. By induction hypothesis we have $\psi_1 : s_1 \backslash \mathrm{R}_{c_1}(N_1) \circ c_1$ and $\psi_2 : s_2 \backslash \mathrm{R}_{c_2}(N_2) \circ c_2$. Define

   $$\psi := \frac{\psi_1' \quad \psi_2'}{} \; \rho$$

   which I) is cut-free because N contains no cut-occurrences and ρ operates on N. As c_1, c_2 are ρ-clauses we know that $\mathrm{R}_{c_1}(N_1)$ and $\mathrm{R}_{c_2}(N_2)$ contain the auxiliary formulas of ρ. So we can form ψ which II) derives $\mathrm{S}(s, \mathrm{R}_c(N)) \circ c$ because $c = c_1 \circ c_2$, the merging of the context formulas from $\mathrm{R}_{c_1}(N_1)$ and $\mathrm{R}_{c_2}(N_2)$ gives the context formulas in $\mathrm{R}_c(N)$ and the main formula of ρ is in $\mathrm{R}_c(N)$ and can be derived by ρ because both auxiliary formulas are in $\mathrm{R}_{c_1}(N_1)$ and $\mathrm{R}_{c_2}(N_2)$.

□

In comparing the profile to the characteristic clause set it is obvious that the refutations of the profile have at most the size of those of the characteristic clause sets by the subsumption result Corollary 3.1. Furthermore, by analyzing the construction of the projections in the above proof one can

also see that the projections to the clauses from the profile are at most the size of those to the clauses from the characteristic clause set (the addition of weakening rules is compensated by the fact that the formula we add by weakening in the profile-projections has to be derived in the characteristic clause set-projection)

3.3.3 Speed-Up

We will now show that using the profile can even result in a non-elementary speed-up of the CERES method w.r.t. using the characteristic clause set. The reason is that certain redundancies which are automatically detected in the construction of the profile remain unnoticed in the construction of the characteristic clause set.

Example 3.1. Let (ψ_n) be a sequence of proofs with non-elementary cut-elimination (for examples of such sequences see [47, 41, 43]), let $X_n := \mathrm{CL}(\psi_n)$ and consider the following proof sequence $\varphi_n =$

$$\dfrac{A \vdash A \qquad \dfrac{\dfrac{A \vdash A}{C, A \vdash A}\ \mathrm{w:l} \qquad \dfrac{(\psi_n, X_n)}{\vdash F}}{C \vee D, A \vdash A, F}\ \vee\mathrm{:l}[\rho]}{A, C \vee D \vdash A, F}\ \mathrm{cut}$$

Then

$$\mathrm{CL}(\varphi_n) = (X_n \times \{A \vdash\}) \cup \{\vdash A\}$$

and

$$\mathrm{P}^{\Omega}(\varphi_n) = (Y_n \times_{\mathcal{L}(\rho)} \{A \vdash\}) \cup \{\vdash A\} = Y_n \cup \{A \vdash\} \cup \{\vdash A\}$$

for some Y_n with $Y_n \trianglelefteq X_n$. Then $\mathrm{CL}(\varphi_n)$ has only refutations of non-elementary length whereas $\mathrm{P}^{\Omega}(\varphi_n)$ has a refutation consisting of a single resolution step. The restricted product $\times_{\mathcal{L}(\rho)}$ becomes a pure union because neither Y_n nor $\{A \vdash\}$ contain ρ-clauses.

Chapter 4

Static Properties of the Profile

In this chapter we will investigate the relation of the profile to various other techniques for abstracting from details of formal proofs. We will investigate proof nets, Herbrand-disjunctions and logical flow graphs.

4.1 The Relation to Proof Nets

The following analysis will be carried out for pseudo-proofs which are used in Chapter 5 in the investigation of proofs transformations.

Definition 4.1 (pseudo-**LK**-proof)**.** A pseudo-**LK**-proof (also called an **LKps**-proof) is an **LK**-proof where the following rules are replaced:

1. Contraction by pseudo-contraction:

$$\frac{A, B, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ \text{psc} : \text{l} \qquad \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A}\ \text{psc} : \text{r}$$

   if A and B are logically equivalent (in first-order logic).

2. Cut by pseudo-cut:

$$\frac{\Gamma \vdash \Delta, A \quad B, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{pscut}$$

   if A and B are logically equivalent (in first-order logic).

We need the technical notion of pseudo-LK-proofs, as many useful proof transformations destroy the proof property in intermediary steps, but keep this of a pseudo-proof. Moreover the analysis of proofs via profiles and

characteristic clause sets can be generalized to pseudo-proofs without any problems. The reduction relation $\rightarrow_{\mathrm{G_r}}$ can be carried over to **LKps**-proofs; however $\rightarrow_{\mathrm{G_r}}$ is not capable of eliminating all cuts in **LKps**-proofs (in contrast to the CERES-method [8] which also eliminates pseudo-cuts).

From now on, we will also sometimes use another notation for the profile which is more convenient for writing about sub-proofs.

Definition 4.2. Let $\chi[\varphi]_\mu$ be an **LK**-proof. Let M be the subset of $\Omega(\chi)$ that occurs in φ and let N be the subset of $\Sigma(\chi)$ that occurs in φ. We define

$$\mathrm{P}^\Omega(\chi).\mu := \mathrm{P}^\Omega_M(\varphi), \quad \mathrm{P}^\Sigma(\chi).\mu := \mathrm{P}^\Sigma_N(\varphi) \text{ and}$$

$$\mathrm{P}(\chi).\mu := (\mathrm{P}^\Omega(\chi).\mu; \mathrm{P}^\Sigma(\chi).\mu)$$

Lemma 4.1 (compatibility of P)**.** Let $\chi[\varphi]_\mu$ be an **LKps**-proof, let φ' be another **LK**-proof with the same end-sequent as φ. Let $\sigma_1, \ldots, \sigma_n$ be the formula occurrences in the end-sequent of φ and let $\sigma'_1, \ldots, \sigma'_n$ be the corresponding formula occurrences in the end-sequent of φ'. Let θ be a substitution whose domain is included in the set of eigenvariables of φ. We write χ' for $\chi[\varphi']_\mu$. If

1. $\mathrm{P}(\chi').\mu = (\mathrm{P}(\chi).\mu)\theta$ and
2. for $i = 1, \ldots, n : \mathcal{L}(\sigma'_i) \cap \mathcal{L}(\mathrm{P}(\chi').\mu) = \mathcal{L}(\sigma_i) \cap \mathcal{L}(\mathrm{P}(\chi).\mu)$

then

$$\mathrm{P}(\chi') = \mathrm{P}(\chi)\theta$$

Proof. Note that by 1 we have $\mathcal{L}(\mathrm{P}(\chi').\mu) = \mathcal{L}(\mathrm{P}(\chi).\mu)$. Let ν be a formula occurrence in χ that is not in φ, let ν' be the corresponding formula occurrence in χ'. If ν is not on the path between μ and the end-sequent then we clearly have $\mathcal{L}(\nu') = \mathcal{L}(\nu)$. If it is then by induction on the length of this path and by using 2 we have $\mathcal{L}(\nu') \cap \mathcal{L}(\mathrm{P}(\chi).\nu) = \mathcal{L}(\nu) \cap \mathcal{L}(\mathrm{P}(\chi).\nu)$.

Now, using $\mathcal{L}(\nu') \cap \mathcal{L}(\mathrm{P}(\chi).\nu) = \mathcal{L}(\nu) \cap \mathcal{L}(\mathrm{P}(\chi).\nu)$ we proceed by induction on the length of the path between μ and the end-sequent. If the last rule is unary then the induction step obviously extends to give $\mathrm{P}(\chi') = \mathrm{P}(\chi)\theta$. If the last rule is binary, observe that θ cannot change variables of the part that does not contain μ because its domain is restricted to the eigenvariables of φ and the proof is regular, so also $\mathrm{P}(\chi') = \mathrm{P}(\chi)\theta$. □

It is a well-known fact about the sequent calculus that the order of rule applications can be permuted up to a high degree (see e.g. [33]). In this section we will formally define these rule permutations and show that the proof profile is not changed by permuting rules.

Definition 4.3 (adjacent)**.** Two rules in an **LKps**-proof are said to be *adjacent* if one occurs immediately above the other.

Definition 4.4 (independent)**.** Two adjacent rules in an **LKps**-proof are said to be *independent* if neither

1. the main occurrence of the upper rule is an auxiliary occurrence of the lower rule, nor
2. the lower rule is unary with two auxiliary occurrences that are split by the binary upper rule, nor
3. the lower rule is a strong quantifier rule and the upper rule is a weak quantifier rule introducing a term that contains the eigenvariable of the lower rule

Definition 4.5 (permutation of independent rules)**.** Let φ be an **LKps**-proof whose last two rules are independent. Let φ' be the proof that differs from φ only by swapping the order of the last two rules. Then we write $\varphi \sim_\pi \varphi'$.

We will denote with $\approx_\pi$ the reflexive, transitive and compatible closure of the rule swapping relation $\sim_\pi$.

The main result of this section is that proofs that are equivalent modulo $\approx_\pi$ have the same profile. In order to show this we need a lemma on the algebraic behavior of the restricted product $\times_L$: Under certain circumstances it acts in an associative way.

Lemma 4.2. Let C, D, E be sets of labelled clauses and let $L_1, L_2 \subseteq \mathcal{L}$ s.t. C contains no L_2-clauses and E contains no L_1-clauses. Then

$$C \times_{L_1} (D \times_{L_2} E) = (C \times_{L_1} D) \times_{L_2} E$$

Proof. We start with the left-hand side of the equation:

$$\begin{aligned} C \times_{L_1} (D \times_{L_2} E) \quad = \quad & (C^{L_1} \times ((D^{L_2} \times E^{L_2}) \cup D^{\neg L_2} \cup E^{\neg L_2})^{L_1}) \cup \\ & C^{\neg L_1} \cup ((D^{L_2} \times E^{L_2}) \cup D^{\neg L_2} \cup E^{\neg L_2})^{\neg L_1} \end{aligned}$$

by definition. Note that $(X \cup Y)^L = X^L \cup Y^L$ for all sets of labelled clauses X, Y and all label sets L, so we have:

$$\begin{aligned} & (C^{L_1} \times ((D^{L_2} \times E^{L_2})^{L_1} \cup D^{L_1 \wedge \neg L_2} \cup E^{L_1 \wedge \neg L_2})) \cup \\ & C^{\neg L_1} \cup (D^{L_2} \times E^{L_2})^{\neg L_1} \cup D^{\neg L_1 \wedge \neg L_2} \cup E^{\neg L_1 \wedge \neg L_2} \end{aligned}$$

Distributing $\times$ over $\cup$ we get:

$$\begin{aligned} (C^{L_1} \times (D^{L_2} \times E^{L_2})^{L_1}) \cup (C^{L_1} \times D^{L_1 \wedge \neg L_2}) \cup (C^{L_1} \times E^{L_1 \wedge \neg L_2}) \cup \\ C^{\neg L_1} \cup (D^{L_2} \times E^{L_2})^{\neg L_1} \cup D^{\neg L_1 \wedge \neg L_2} \cup E^{\neg L_1 \wedge \neg L_2} \end{aligned}$$

As E contains no L_1-clauses we can write $(D^{L_2} \times E^{L_2})^{L_1} = D^{L_1 \wedge L_2} \times E^{L_2}$ and $(D^{L_2} \times E^{L_2})^{\neg L_1} = D^{\neg L_1 \wedge L_2} \times E^{L_2}$ and obtain:

$$(C^{L_1} \times (D^{L_1 \wedge L_2} \times E^{L_2})) \cup (C^{L_1} \times D^{L_1 \wedge \neg L_2}) \cup (C^{L_1} \times E^{L_1 \wedge \neg L_2}) \cup C^{\neg L_1} \cup (D^{\neg L_1 \wedge L_2} \times E^{L_2}) \cup D^{\neg L_1 \wedge \neg L_2} \cup E^{\neg L_1 \wedge \neg L_2}$$

As E does not contain L_1-clauses, i.e. $E^{L_1} = \emptyset$ also $C^{L_1} \times E^{L_1 \wedge \neg L_2} = \emptyset$. Furthermore we can write $E = E^{\neg L_1}$ and - as C does not contain L_2-clauses - also $C = C^{\neg L_2}$. We obtain

$$(C^{L_1 \wedge \neg L_2} \times (D^{L_1 \wedge L_2} \times E^{\neg L_1 \wedge L_2})) \cup (C^{L_1 \wedge \neg L_2} \times D^{L_1 \wedge \neg L_2}) \cup (D^{\neg L_1 \wedge L_2} \times E^{\neg L_1 \wedge L_2}) \cup C^{\neg L_1 \wedge \neg L_2} \cup D^{\neg L_1 \wedge \neg L_2} \cup E^{\neg L_1 \wedge \neg L_2}$$

The right-hand side can be rewritten to the same expression in an analogous way. □

Proposition 4.1 (invariance under $\approx_\pi$)**.** Let χ, χ' be two **LKps**-proofs with $\chi \approx_\pi \chi'$. Then

$$\mathrm{P}(\chi') = \mathrm{P}(\chi)$$

Proof. By duality it suffices to show $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi)$ and by transitivity of $=$, it suffices to show the invariance of P^Ω for a single rule swapping. Let μ be the position in χ where the rule swapping occurs, so we have $\varphi \sim_\pi \varphi'$ with $\chi = \chi[\varphi]_\mu$ and $\chi' = \chi[\varphi']_\mu$.

We will first show $\mathrm{P}^\Omega(\chi').\mu = \mathrm{P}^\Omega(\chi).\mu$.

If both swapped rules are unary rules, then we simply have

$$\mathrm{P}^\Omega(\chi).\mu = C = \mathrm{P}^\Omega(\chi').\mu$$

For some clause set C.

If one of the swapped rules is a unary rule and one a binary rule, we have

$$\mathrm{P}^\Omega(\chi).\mu = C \circ D$$

where $\circ = \cup$ or $\circ = \times_{\mathcal{L}(\rho)}$ where ρ is the binary rule. In both cases also

$$\mathrm{P}^\Omega(\chi').\mu = C \circ D$$

because $\mathcal{L}(\rho)$ clearly is not changed by the swapping of two rules.

If both rules are binary then the last rules ρ_1 and ρ_2 of φ, φ' have the form (omitting the sequents and concrete rule types):

$$\dfrac{(\varphi_1, C) \quad \dfrac{(\varphi_2, D)}{\rho_1} \quad (\varphi_3, E)}{\rho_2} \qquad \text{and} \qquad \dfrac{(\varphi_1, C) \quad \dfrac{(\varphi_2, D) \quad (\varphi_3, E)}{\rho_1}}{\rho_2}$$

From the existence of the left proof one can deduce that E does not contain any clauses with labels from $\mathcal{L}(\rho_1)$ because all labels in E refer to axioms in φ_3 and $\mathcal{L}(\rho_1)$ cannot contain any labels from axioms in φ_3 because it is parallel to it. Symmetrically from the right proof one can deduce that C does not contain any clauses with labels from $\mathcal{L}(\rho_2)$.

For the profiles at μ we have

$$\mathrm{P}^{\Omega}(\chi).\mu = (C \circ_1 D) \circ_2 E \qquad \text{and} \qquad \mathrm{P}^{\Omega}(\chi').\mu = C \circ_1 (D \circ_2 E)$$

for operators $\circ_1, \circ_2$ associated to the rules ρ_1 and ρ_2.

If both $\circ_1 = \cup$ and $\circ_2 = \cup$ then $\mathrm{P}^{\Omega}(\chi).\mu = O\mathrm{P}(\chi').\mu$ follows from associativity of $\cup$. If $\circ_1 = \times_{\mathcal{L}}(\rho_1)$ and $\circ_2 = \times_{\mathcal{L}}(\rho_2)$ then with the observation above we can apply Lemma 4.2 to obtain $\mathrm{P}^{\Omega}(\chi).\mu = \mathrm{P}^{\Omega}(\chi').\mu$.

Now, let $\circ_1 = \times_{\mathcal{L}(\rho_1)}$ and $\circ_2 = \cup$. Then – abbreviating $\mathcal{L}(\rho_1)$ as L – we have

$$\begin{aligned} C \times_L (D \cup E) &= (C^L \times (D \cup E)^L) \cup C^{\neg L} \cup (D \cup E)^{\neg L} \\ &= (C^L \times (D^L \cup E^L)) \cup C^{\neg L} \cup D^{\neg L} \cup E^{\neg L} \end{aligned}$$

but as E does not contain labels from L, $E^L = \emptyset$ and $E^{\neg L} = E$ and so

$$\begin{aligned} &= (C^L \times D^L) \cup C^{\neg L} \cup D^{\neg L} \cup E \\ &= (C \times_L D) \cup E \end{aligned}$$

If $\circ_1 = \cup$ and $\circ_2 = \times_{\mathcal{L}(\rho_2)}$ the proof proceeds analogously using the observation that C does not contain labels from $\mathcal{L}(\rho_2)$.

Condition 2 of Lemma 4.1 is fulfilled, because rule swappings do not change the ancestor relation in the proof, so we can apply Lemma 4.1 and conclude $\mathrm{P}(\chi') = \mathrm{P}(\chi)$. □

In [44] E. Robinson defines proof nets for classical propositional logic and shows [44, Proposition 6.2]:

Proposition 4.2. Two **LK**-proofs φ and φ' (for classical propositional logic) induce isomorphic proof nets iff $\varphi \approx_\pi \varphi'$.

Building on this and Proposition 4.1 we can easily conclude

Corollary 4.1. If two **LK**-proofs φ and φ' (for classical propositional logic) induce isomorphic proof nets then $\mathrm{P}(\varphi) = \mathrm{P}(\varphi')$.

R. McKinley defines in his PhD thesis [40] an extension of Robinson's proof nets to first-order classical logic by treating quantifiers with boxes. We conjecture that the result of Corollary 4.1 also extends to this notion of proof net.

4.2 The Relation to Herbrand-Disjunctions

One of the most important results about first-order classical logic is Herbrand's Theorem: In its simplest version it says that if F is a quantifier-free formula and if $(\exists x)F$ is a tautology, then there exists a finite disjunction of instances of F that is also a tautology. There are other variants and generalizations of this theorem (see e.g. [13]), in particular Gentzen's proof-theoretic version of it: the mid-sequent theorem which says that each cut-free proof of a prenex sequent can be transformed into one s.t. no quantifier rule appears above a propositional rule: The proof is divided into an upper propositional part and a lower quantifier part. The sequent between these two parts is called mid-sequent and is the generalization of the Herbrand-disjunction. A mid-sequent has thus two main properties: 1) it is a propositional tautology and 2) it consits only of instances of the end-sequent.

For the analysis of concrete mathematical proofs in first-order logic the mid-sequent is of high significance because it contains the *term instances* used in the proof and it is in choosing these instances where the mathematical creativity of a proof lies. From this point of view, the first property of mid-sequents is less important than the second: In order to understand how a concretely given proof establishes the truth of a theorem, understanding which instances of quantified formulas are used is enough. The possibility of isolating a list of such instances which form a *propositional* tautology (as opposed to a first-order tautology) is secondary.

We will partition a proof containing cuts into two parts: one part containing all the rules working on (ancestors of) the end-sequent and the other part containing all the rules working on (ancestors of) cut formulas. For each of the two parts we will show an analogue of the mid-sequent theorem, i.e. we will give a construction of a formula that consists only of instances of the end-sequent formulas (resp. cut-formulas) that occur in the proof and that is a *first-order* tautology for the end-sequent part and unsatisfiable for the cut-formulas part. It is not possible - in principle - to extract such a propositional tautology from a proof with cuts. See [47, 41, 43] for examples of sequences of proofs with cuts where the smallest such propositional tautology is of a size that is not elementary in the size of the original proof. These constructions are carried out by using the proof profile.

Definition 4.6 ($\mathbf{LK^j}$-proof)**.** An $\mathbf{LK^j}$-proof is an **LK**-proof where in addition the following rule of *juxtaposition* can occur:

$$\frac{\Gamma \vdash \Delta \quad \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{j}(L)$$

where L is a set of labels.

If σ is a sequent occurrence in a proof and M is a set of formula occurrences, then $\mathrm{S}(\sigma, M)$ denotes the sub-sequent of σ consisting of the formula

occurrences from M.

A formula is called *prenex* if no quantifier appears below a propositional connective. A sequent is called prenex if all its formulas are prenex. A proof is called prenex if all its sequents are prenex. The mid-sequent theorem is a proof-theoretic version of Herbrand's theorem and has first been shown by Gentzen in [23].

Theorem 4.1 (mid-sequent theorem)**.** Let φ be a cut-free prenex **LK**-proof. Then there is a proof φ' of the same end-sequent s.t. no quantifier rule occurs above a propositional rule.

We will now give a proof of the mid-sequent theorem that is adapted to $\mathbf{LK^j}$ and will also allow to define a unique mid-sequent (which we will call Herbrand-sequent) of a cut-free prenex $\mathbf{LK^j}$-proof.

Definition 4.7 (depth)**.** Let ρ be a quantifier rule in an $\mathbf{LK^j}$-proof φ. Then the *depth* of ρ, $|\rho|$ is defined as the number of propositional, cut and juxtaposition rules on the path from ρ to the root of φ.

Definition 4.8 (associated contraction)**.** Let φ be an $\mathbf{LK^j}$-proof containing a quantifier rule ρ with main occurrence μ. Every contraction rule below ρ that has an auxiliary occurrence ν s.t. μ is ancestor of ν and the only active formula occurrences this ancestor path passes through are active formula occurrences of contraction rules is said to be *associated to* ρ.

Definition 4.9 (mid-sequent reduction)**.** Let φ be a regular cut-free prenex $\mathbf{LK^j}$-proof. We define the transformation $\rightarrow_{\mathcal{M}}$ permuting a quantifier rule ρ with $|\rho| > 0$ downwards.

1. ρ is a $\forall : r$-rule. Let τ be the first propositional or juxtaposition rule below ρ and assume that there is no quantifier rule between ρ and τ (If this is not the case, choose the quantifier rule that is in-between as ρ).

   (a) τ is a unary propositional rule. Then the subproof χ of φ at τ has the following form: $\chi =$

$$\dfrac{\dfrac{\dfrac{(\psi)}{\Gamma \vdash \Delta, F\{x \leftarrow \alpha\}}\ \forall\text{: r}[\rho]}{\Gamma \vdash \Delta, (\forall x)F}}{\dfrac{\Gamma' \vdash \Delta', (\forall x)F}{\Gamma'' \vdash \Delta'', (\forall x)F}\ [\tau]}\ \text{c} : *, \text{w} : *[\sigma]$$

   The premise of τ contains $(\forall x)F$ (as a descendant of the main occurrence of ρ) because neither contraction nor weakening can remove it. The propositional rule τ does not have this $(\forall x)F$ as

auxiliary formula (assume it has, then the main formula G of τ would not be prenex), so also the conclusion of τ contains this $(\forall x)F$.

Let σ' be the contractions in σ that are associated to ρ and let Π be the multiset that contains the formula $(\forall x)F$ exactly n times where n is the number of contractions in σ'.

We define $\chi \to_{\mathcal{M}} \chi'$ with $\chi' =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\psi)}{\Gamma \vdash \Delta, F\{x \leftarrow \alpha\}}}{\Gamma' \vdash \Delta', \Pi, F\{x \leftarrow \alpha\}}\ \mathrm{c} : *, \mathrm{w} : *[\sigma \setminus \sigma']}{\Gamma'' \vdash \Delta'', \Pi, F\{x \leftarrow \alpha\}}\ [\tau]}{\Gamma'' \vdash \Delta'', \Pi, (\forall x)F}\ \forall\mathrm{:\ r}[\rho]}{\Gamma'' \vdash \Delta'', (\forall x)F}\ \mathrm{c} : \mathrm{r} * [\sigma']$$

The eigenvariable condition (of ρ in χ') is fulfilled because α does not occur in Γ, Δ and not in Γ', Δ' (in particular it is not added by a weakening in σ because the proof is regular).

(b) ν is a binary rule: analogous to 1a) because we use a multiplicative sequent calculus.

2. ρ is a $\forall : l$-rule: analogous to 1)
3. ρ is a $\exists : r$-rule: analogous to 1)
4. ρ is a $\exists : l$-rule: analogous to 1)

With $\to^*_{\mathcal{M}}$ we will denote the reflexive and transitive closure of $\to_{\mathcal{M}}$. We say that a cut-free prenex proof φ is in mid-sequent normal form (abbreviated $\mathcal{M}$-NF) if there is no φ' s.t. $\varphi \to_{\mathcal{M}} \varphi'$. A proof in $\mathcal{M}$-NF has $|\rho| = 0$ for all quantifier rules ρ, i.e. there is no propositional or juxtaposition rule below a quantifier rule: Such a proof can be split into two parts: An upper part containing only propositional and structural rules (including juxtaposition) and a lower part containing only quantifier rules, weakenings and contractions (and neither juxtaposition nor propositional rules). However this splitting is not unique: We can split the proof at any position between the lowest propositional or juxtaposition rule and the highest quantifier rule. Between these two rules is a sequence of contractions and weakenings. In order to give a definition of a unique mid-sequent of a proof in $\mathcal{M}$-NF we employ usedness to take care of weakening and set-normalization to take care of contraction.

A formula occurrence μ is called *used* if it has an ancestor in an axiom. For a set of formula occurrences M we write $\mathrm{U}(M)$ for the subset of M that is used. Note that a formula occurrence is not used iff all its ancestor paths end in main occurrences of weakening rules.

Definition 4.10 (Herbrand-sequent)**.** Let φ be a cut-free prenex $\mathbf{LK^j}$-proof in $\mathcal{M}$-NF. Then φ has a lowest propositional rule ρ, i.e. ρ is on the path between the end-sequent and any other propositional rule. Let s be the conclusion sequent of ρ. We define the *Herbrand-Sequent*

$$\mathcal{H}(\varphi) := \mathrm{set}(\mathrm{U}(s))$$

The Herbrand-sequent contains essential information about the cut-free proof. Herbrand sequents have for example been used in [39] to extract explicit bounds from proofs.

4.2.1 Global Characterization of Herbrand Sequents

Using U and set-normalization we have given a unique definition of the mid-sequent of a proof in $\mathcal{M}$-NF. But $\mathcal{M}$-reduction is not confluent, so it is a-priori not clear how to uniquely define the mid-sequent of a proof which is not in $\mathcal{M}$-NF. But in this section we will show that $\mathcal{M}$-reduction is confluent w.r.t. the Herbrand-sequent (i.e. all $\mathcal{M}$-NFs of a certain proof have the same Herbrand-sequent). This will allow us to speak about *the* Herbrand-sequent of a cut-free prenex proof which is *not* in $\mathcal{M}$-NF.

Definition 4.11. Let φ be an $\mathbf{LK^j}$-proof.

With $\mathrm{Q}(\varphi)$ we denote the set of quantifier rules in φ.

Let R be a set of rules. With $\mathrm{A}(R)$ we denote the set of auxiliary occurrences of the rules in R.

Let M be a set of formula occurrences. With $\mathrm{S}(M)$ we denote the sequent that is created from merging all formula occurrences from M.

Let s be a sequent. With $\mathrm{P}(s)$ we denote the sequent that contains exactly the quantifier-free formulas of s.

Definition 4.12. Let φ be a cut-free prenex $\mathbf{LK^j}$-proof. We define the sequent

$$\mathcal{Q}_\mathrm{p}(\varphi) := \mathrm{P}(\mathrm{S}(\mathrm{U}(\mathrm{A}(\mathrm{Q}(\varphi)))))$$

Let s be the end-sequent of φ. We define the sequent

$$\mathrm{s}_\mathrm{p}(\varphi) := \mathrm{P}(\mathrm{U}(s))$$

Proposition 4.3. Let φ be a cut-free prenex $\mathbf{LK^j}$-proof and let φ^* be any $\mathcal{M}$-NF of φ. Then

$$\mathcal{H}(\varphi^*) = \mathrm{set}(\mathrm{s}_\mathrm{p}(\varphi) \circ \mathcal{Q}_\mathrm{p}(\varphi))$$

Proof. We proceed by induction on the length n of the $\mathcal{M}$-reduction sequence of φ to φ^*.

1. For $n = 0$ we have $\varphi = \varphi^*$ in $\mathcal{M}$-NF and we show
$$\mathcal{H}(\varphi) = \mathrm{set}(\mathrm{s_p}(\varphi) \circ \mathcal{Q}_\mathrm{p}(\varphi))$$
by induction on the size of the quantifier part. Let ρ be the lowest propositional rule and let s be its conclusion sequent. Then $\mathcal{H}(\varphi) = \mathrm{set}(\mathrm{U}(s))$. We can partition φ as $\begin{matrix}\varphi_p \\ \varphi_q\end{matrix}$ where φ_p ends with ρ and φ_q consists only of quantifier rules, weakenings and contractions (which are all unary). We proceed by induction on m, the number of rules in φ_q: If $m = 0$ then $\mathcal{Q}_\mathrm{p}(\varphi) = \emptyset$ and $\mathcal{H}(\varphi) = \mathrm{set}(\mathrm{U}(s))$. If $m > 0$, let $\varphi_q = \begin{matrix}\varphi'_q \\ \rho'\end{matrix}$. By the induction hypothesis we know for $\varphi' = \begin{matrix}\varphi_p \\ \varphi'_q\end{matrix}$ that $\mathcal{H}(\varphi') = \mathrm{set}(\mathrm{s_p}(\varphi') \circ \mathcal{Q}_\mathrm{p}(\varphi'))$. But $\mathcal{H}(\varphi) = \mathcal{H}(\varphi_p) = \mathcal{H}(\varphi')$ and we also have $\mathrm{set}(\mathrm{s_p}(\varphi') \circ \mathcal{Q}_\mathrm{p}(\varphi')) = \mathrm{set}(\mathrm{s_p}(\varphi) \circ \mathcal{Q}_\mathrm{p}(\varphi))$ because if ρ' is a quantifier rule with an unused auxiliary occurrence or a contraction or a weakening then $\mathrm{set}(\mathrm{s_p}(\varphi)) = \mathrm{set}(\mathrm{s_p}(\varphi'))$ and $\mathcal{Q}_\mathrm{p}(\varphi) = \mathcal{Q}_\mathrm{p}(\varphi')$ and if ρ' is a quantifier rule with a used auxiliary formula occurrence μ then μ moves from $\mathrm{s_p}(\varphi')$ into $\mathcal{Q}_\mathrm{p}(\varphi)$.

2. For the induction step ($n > 0$) we show that if $\varphi \to_\mathcal{M} \varphi'$ then (a) $\mathcal{Q}_\mathrm{p}(\varphi) = \mathcal{Q}_\mathrm{p}(\varphi')$ and (b) $\mathrm{s_p}(\varphi) = \mathrm{s_p}(\varphi')$. (b) is obvious as $\mathcal{M}$-reduction does not modify the end-sequent and preserves usedness. For (a) observe that no quantifier rules are added, nor removed, so $\mathrm{S}(\mathrm{A}(\mathrm{Q}(\varphi))) = \mathrm{S}(\mathrm{A}(\mathrm{Q}(\varphi')))$. But $\mathcal{M}$-reduction also does not add nor remove weakenings and the ancestor relation in the modified parts is not modified, so $\mathrm{S}(\mathrm{U}(\mathrm{A}(\mathrm{Q}(\varphi)))) = \mathrm{S}(\mathrm{U}(\mathrm{A}(\mathrm{Q}(\varphi'))))$ and thus $\mathcal{Q}_\mathrm{p}(\varphi) = \mathcal{Q}_\mathrm{p}(\varphi')$.

□

The above proposition allows to define *the* mid-sequent of a cut-free prenex $\mathbf{LK^j}$-proof φ which is *not in $\mathcal{M}$-NF* as $\mathcal{H}(\varphi) := \mathrm{set}(\mathrm{s_p}(\varphi) \circ \mathcal{Q}_\mathrm{p}(\varphi))$. This shows that it is possible to calculate the Herbrand-sequent without explicitly executing $\mathcal{M}$-reduction steps by instead collecting all used propositional auxiliary formulas of quantifier inferences. Note that $\mathcal{H}(\varphi)$ is a propositional tautology and consists only of instance of formulas of the end-sequent of φ. For two sequents s and t we write $s \leq^\mathrm{q} t$ if there is an $\mathbf{LK}$-proof $\psi = \begin{matrix}s \\ \vdots \\ t\end{matrix}$ consisting only of quantifier rules, weakenings and contractions. So if φ is a cut-free prenex proof with end-sequent s then $\mathcal{H}(\varphi) \leq^\mathrm{q} s$.

4.2.2 Partial Proofs and Partial Herbrand Sequents

In order to carry out a more fine-grained analysis we will use partial Herbrand-sequents which are not tautological. We will define partial Herbrand-sequents

as Herbrand-sequents of partial proofs.

Definition 4.13 (partial proof)**.** Let φ be an $\mathbf{LK^j}$-proof with end-sequent s and let M be a closed set of formula occurrences. We define the $\mathbf{LK^j}$-proof $\varphi \mid M$ as follows: If $M = \emptyset$ then $\varphi \mid M := \vdash$, else we can assume that s contains a formula occurrence from M or that φ ends with a binary rule and both immediate sub-proofs contain formula occurrences from M (If this is not the case, we define $\varphi \mid M := \chi \mid M$ where χ is the smallest sub-proof of φ where this is true).

1. If φ is an axiom sequent α we define

$$\varphi \mid M \;:=\; \mathrm{S}(\alpha, M)$$

2. If φ ends with a unary rule ρ, let s' be its premise sequent, let φ' be the immediate sub-proof of φ and let M' be the subset of M of occurrences in φ'.

   (a) If ρ operates on M we define

$$\varphi \mid M \;:=\; \dfrac{\begin{matrix}(\varphi' \mid M')\\ \mathrm{S}(s', M')\end{matrix}}{\mathrm{S}(s, M)}\ \rho$$

   (b) If ρ does not operate on M then $\mathrm{S}(s, M) = \mathrm{S}(s', M')$ and we define

$$\varphi \mid M \;:=\; \varphi' \mid M'$$

3. If φ ends with a binary rule ρ let s_1, s_2 be its premise sequents and let φ_1, φ_2 be the proofs of s_1 and s_2 respectively. Let M_1, M_2 be the subsets of M of occurrences in φ_1, φ_2 respectively.

   (a) If ρ operates on M we define

$$\varphi \mid M \;:=\; \dfrac{\begin{matrix}(\varphi_1 \mid M_1) & (\varphi_2 \mid M_2)\\ \mathrm{S}(s_1, M_1) & \mathrm{S}(s_2, M_2)\end{matrix}}{\mathrm{S}(s, M)}\ \rho$$

   (b) If ρ does not operate on M then $\mathrm{S}(s, M) = \mathrm{S}(s_1, M_1) \circ \mathrm{S}(s_2, M_2)$.

      i. If $M_1 \neq \emptyset$ and $M_2 \neq \emptyset$ then we define

$$\varphi \mid M \;:=\; \dfrac{\begin{matrix}(\varphi_1 \mid M_1) & (\varphi_2 \mid M_2)\\ \mathrm{S}(s_1, M_1) & \mathrm{S}(s_2, M_2)\end{matrix}}{\mathrm{S}(s, M)}\ \mathrm{j}(\mathcal{L}(\rho))$$

      ii. If $M_1 = \emptyset$ then we define

$$\varphi \mid M \;:=\; \varphi_2 \mid M_2$$

iii. If $M_2 = \emptyset$ then we define

$$\varphi \mid M \;:=\; \varphi_1 \mid M_1$$

Partial proofs as defined above are similar to the inner proofs of [14] in that they consist of a subset of rule applications of the original, however they are different in that they do not require the axioms to be complete. Thus partial proofs in general do not end with a tautology as conclusion sequent.

Definition 4.14 (partial Herbrand-sequent)**.** Let φ be an $\mathbf{LK^j}$-proof and let μ be a prenex formula occurrence in φ. Let χ be the sub-proof of φ that contains μ in its end-sequent. We define the *partial Herbrand-sequent*

$$\mathcal{H}(\mu) := \mathcal{H}(\chi \mid \langle\mu\rangle)$$

Partial Herbrand-sequents are no longer tautologies. They contain the information which instances of a given formula have been used in the proof.

Example 4.1. Let $F = (\forall x)(\forall y)(P(x,y) \to P(s(x),y))$,
$G = (\forall x)(\forall y)(P(x,y) \to P(x,s(y)))$ and φ be a proof of the sequent

$$F, G \vdash P(0,0) \to P(s(s(0)), s(s(s(0))))$$

and let μ_1 (μ_2) be the occurrence of F (G) in the antecedens of the end-sequent of φ. The antecedens can be seen as axiomatizing a two-dimensional grid. There are different cut-free proofs of this sequent. Given a concrete such proof, it corresponds to a path in this grid. The partial Herbrand-sequent $\mathcal{H}(\mu_1)$ describes all the steps in the x-direction while $\mathcal{H}(\mu_2)$ describes the steps taken in the y-direction in this path.

4.2.3 Inductive Characterization of Partial Herbrand Sequents

Definition 4.15. Let μ be an occurrence of a formula F in an $\mathbf{LK^j}$-proof. We define the formula $[\mu]$ as

$$[\mu] := \begin{cases} F & \text{if } \mu \text{ occurs on the right side of the sequent} \\ \neg F & \text{if } \mu \text{ occurs on the left side of the sequent} \end{cases}$$

Definition 4.16 (Herbrand-Clauses)**.** Let φ be an $\mathbf{LK^j}$-proof and let μ be a formula occurrence in φ. We define the set of *Herbrand-clauses* $\mathcal{HC}(\mu)$ of μ inductively as follows:

1. μ occurs in an axiom:
$$\mathcal{HC}(\mu) = \{\{[\mu]\}\}$$
2. μ occurs in a rule:

(a) μ has no immediate ancestor (i.e. μ is introduced by weakening):

$$\mathcal{HC}(\mu) = \{\emptyset\}$$

(b) μ has exactly one immediate ancestor ν:

$$\mathcal{HC}(\mu) = \mathcal{HC}(\nu)$$

(c) μ has exactly two immediate ancestors ν_1 and ν_2:

i. ν_1 and ν_2 occur in the same sequent:

$$\mathcal{HC}(\mu) = \mathcal{HC}(\nu_1) \times \mathcal{HC}(\nu_2)$$

ii. ν_1 and ν_2 occur in different sequents:

$$\mathcal{HC}(\mu) = \mathcal{HC}(\nu_1) \cup \mathcal{HC}(\nu_2)$$

We will now show that the Herbrand-clauses as defined above provide an inductive characterization (up to propositional subsumption) of the conjunctive normal form of a partial Herbrand-sequent.

Lemma 4.3. Let φ be an **LK**-proof and let μ be a prenex formula occurrence in φ. Then

$$\mathcal{HC}(\mu) \trianglelefteq \mathrm{CNF}(\mathcal{H}(\mu))$$

Proof. We assume w.l.o.g. that μ occurs in the end-sequent of φ and proceed by induction on φ:

1. φ is an axiom sequent s. Then $\mathcal{HC}(\mu) = \{\{[\mu]\}\}$, $\mathcal{H}(\mu) = \mathcal{H}(s \mid \mu) = \mathrm{S}(s, \mu)$ and as s is atomic $\mathrm{CNF}(\mathrm{S}(s, \mu)) = \{\{[\mu]\}\}$.

2. φ ends with a rule ρ:
   If μ occurs in the context of ρ. Then μ has a unique immediate ancestor ν and $\mathcal{HC}(\mu) = \mathcal{HC}(\nu)$. But we also have $\mathrm{CNF}(\mathcal{H}(\mu)) = \mathrm{CNF}(\mathcal{H}(\nu))$ because $\mathcal{H}(\mu) = \mathcal{H}(\varphi \mid \langle\mu\rangle)$ and as $\varphi \mid \langle\mu\rangle$ is cut-free by Proposition 4.3 we can write $\mathcal{H}(\varphi \mid \langle\mu\rangle) = \mathrm{set}(\mathrm{s_p}(\varphi \mid \langle\mu\rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle\mu\rangle))$ and - by the same argument - $\mathcal{H}(\varphi \mid \langle\nu\rangle) = \mathrm{set}(\mathrm{s_p}(\varphi \mid \langle\nu\rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle\nu\rangle))$. But we have $\mathrm{s_p}(\varphi \mid \langle\mu\rangle) = \mathrm{s_p}(\varphi \mid \langle\nu\rangle)$ as well as $\mathcal{Q}_\mathrm{p}(\varphi \mid \langle\mu\rangle) = \mathcal{Q}_\mathrm{p}(\varphi \mid \langle\nu\rangle)$ because μ and ν occur in the context of ρ.

   So for the rest of this proof we assume that μ is the main occurrence of ρ and we make a case distinction on the type of ρ:

   (a) If $\rho = w : l$ then $\mathcal{HC}(\mu) = \{\emptyset\}$ and - writing s for the conclusion sequent of ρ - we have $\varphi \mid \langle\mu\rangle =$

   $$\dfrac{\vdash}{\mathrm{S}(s, \mu)}\ \mathrm{w : l}$$

   and thus $\mathcal{H}(\mu) = \vdash$ and $\mathrm{CNF}(\vdash) = \{\emptyset\}$. For $\rho = w : r$ we proceed analogously.

(b) If $\rho = c : l$ then μ has exactly two ancestors ν_1 and ν_2, $\mathcal{HC}(\mu) = \mathcal{HC}(\nu_1) \times \mathcal{HC}(\nu_2)$ and by the induction hypothesis: $\mathcal{HC}(\nu_1) \times \mathcal{HC}(\nu_2) \trianglelefteq \mathrm{CNF}(\mathcal{H}(\nu_1)) \times \mathrm{CNF}(\mathcal{H}(\nu_2))$. By Proposition 4.3 we have $\mathcal{H}(\nu_i) = \mathrm{set}(\mathrm{s_p}(\varphi \mid \langle \nu_i \rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_i \rangle))$ and $\mathcal{H}(\mu) = \mathrm{set}(\mathrm{s_p}(\varphi \mid \langle \mu \rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \mu \rangle))$.

i. If μ is quantifier-free then $\mathcal{H}(\nu_i) = \mathrm{s_p}(\varphi \mid \langle \nu_i \rangle)$ and $\mathcal{H}(\mu) = \mathrm{s_p}(\varphi \mid \langle \mu \rangle)$. As $[\mu] = [\nu_1] = [\nu_2]$ there are two possible values for $\mathrm{CNF}(\mathcal{H}(\mu)), \mathrm{CNF}(\mathcal{H}(\nu_1))$ and $\mathrm{CNF}(\mathcal{H}(\nu_2))$: Either $C := \mathrm{CNF}([\mu])$ if the respective formula occurrence is used or $\{\emptyset\}$ if it is not used. Now if μ is used, at least one of ν_1, ν_2 is used and both $C \times \{\emptyset\} \trianglelefteq C$ and $C \times C \trianglelefteq C$. If μ is not used then both ν_1, ν_2 must not be used and $\{\emptyset\} \times \{\emptyset\} \trianglelefteq \{\emptyset\}$ again holds.

ii. If μ contains a quantifier, then $\mathcal{H}(\mu) = \mathrm{set}(\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \mu \rangle))$ and $\mathcal{H}(\nu_i) = \mathrm{set}(\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_i \rangle))$. Note that - due to ν_1 and ν_2 being exactly the immediate ancestors of μ in φ - we have $\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \mu \rangle) = \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_1 \rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_2 \rangle)$.

$$\begin{aligned} & \mathrm{CNF}(\mathcal{H}(\nu_1)) \times \mathrm{CNF}(\mathcal{H}(\nu_2)) \\ = \; & \mathrm{CNF}(\mathrm{set}(\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_1 \rangle))) \times \mathrm{CNF}(\mathrm{set}(\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_2 \rangle))) \\ = \; & \mathrm{CNF}(\mathrm{set}(\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_1 \rangle)) \circ \mathrm{set}(\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_2 \rangle))) \\ \trianglelefteq \; & \mathrm{CNF}(\mathrm{set}(\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_1 \rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu_2 \rangle))) \\ = \; & \mathrm{CNF}(\mathcal{H}(\mu)) \end{aligned}$$

For $\rho = c : r$ we proceed analogously.

(c) If $\rho = \forall : l$ then μ has exactly one ancestor ν, $\mathcal{HC}(\mu) = \mathcal{HC}(\nu)$ and $\mathcal{HC}(\nu) \trianglelefteq \mathrm{CNF}(\mathcal{H}(\nu))$ by the induction hypothesis. Again by Proposition 4.3 we write $\mathcal{H}(\mu) = \mathrm{set}(\mathrm{s_p}(\varphi \mid \langle \mu \rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \mu \rangle))$ and $\mathcal{H}(\nu) = \mathrm{set}(\mathrm{s_p}(\varphi \mid \langle \nu \rangle) \circ \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu \rangle))$. But we have $\mathcal{H}(\mu) = \mathcal{H}(\nu)$ because $\mathrm{s_p}(\varphi \mid \langle \mu \rangle) = \vdash$ and if ν contains a quantifier then also $\mathrm{s_p}(\varphi \mid \langle \nu \rangle) = \vdash$ and $\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \mu \rangle) = \mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu \rangle)$. On the other hand, if ν is quantifier-free, then $\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \mu \rangle) = \mathrm{s_p}(\varphi \mid \langle \nu \rangle)$ and $\mathcal{Q}_\mathrm{p}(\varphi \mid \langle \nu \rangle) = \vdash$. For the other quantifier rules $\forall : r, \exists : l, \exists : r$ an analogous argument applies.

(d) If $\rho = \neg : l$ then μ has exactly one ancestor ν. The result follows from the induction hypothesis and $\mathrm{CNF}(\neg F \vdash) = \mathrm{CNF}(\vdash F)$ (analogous for $\rho = \neg : r$).

(e) If $\rho = \wedge : l$ then μ has exactly two ancestors ν_1, ν_2 which are in the same sequent. The result follows from the induction hypothesis and $\mathrm{CNF}(A \wedge B \vdash) = \mathrm{CNF}(A \vdash) \times \mathrm{CNF}(B \vdash)$ (analogous for $\rho = \vee : r, \rightarrow : r$).

(f) If $\rho = \wedge : r$ then μ has exactly two ancestors ν_1, ν_2 which are in different sequents. The result follows from the induction hypothesis and $\mathrm{CNF}(\vdash A \wedge B) = \mathrm{CNF}(A) \cup \mathrm{CNF}(B)$ (analogous for $\rho = \vee : l, \rightarrow : l$).

□

4.2.4 Ω-Subsumption

The following Lemma is the technical key to Theorem 4.2. It establishes the connection between CL and $\mathcal{HC}$ and therefore the connection between P^Ω and $\mathcal{HC}$.

Lemma 4.4. Let φ be an **LK**-proof, let M be a set of terminal occurrences and N be a set of end occurrences s.t. $M \cap N = \emptyset$. Then

$$\mathrm{CL}_{\langle M \uplus N \rangle}(\varphi) \trianglelefteq \mathrm{CL}_{\langle M \rangle}(\varphi) \between_{\nu \in N} \mathcal{HC}(\nu)$$

Proof. By induction on φ: If φ is an axiom α, then $\mathrm{CL}_{\langle M \uplus N \rangle}(\varphi) = \{\mathrm{S}(\alpha, M) \circ \mathrm{S}(\alpha, N)\}$ and $\mathrm{CL}_{\langle M \rangle}(\varphi) = \{\mathrm{S}(\alpha, M)\}$ and $\between_{\nu \in N} \mathcal{HC}(\nu) = \{\mathrm{S}(\alpha, N)\}$. So for the rest of this proof we assume that φ ends with a rule ρ. If ρ is a unary rule, we denote with φ' the immediate sub-proof of φ and with $M'(N')$ the set of immediate ancestors of $M(N)$. If ρ is a binary rule, we denote with φ_1, φ_2 the two immediate sub-proofs of φ and with $M_1, M_2(N_1, N_2)$ the immediate ancestors of $M(N)$ in φ_1, φ_2.

1. If all $\nu \in N$ occur in the context of ρ then each $\nu \in N$ has exactly one immediate ancestor ν' and thus $\mathcal{HC}(\nu) = \mathcal{HC}(\nu')$.

   (a) If ρ is a unary rule, then by the induction hypothesis

   $$\mathrm{CL}_{\langle M' \uplus N' \rangle}(\varphi') \trianglelefteq \mathrm{CL}_{\langle M' \rangle}(\varphi') \between_{\nu \in N'} \mathcal{HC}(\nu)$$

   and $\mathrm{CL}_{\langle M' \uplus N' \rangle}(\varphi') = \mathrm{CL}_{\langle M \uplus N \rangle}(\varphi)$, $\mathrm{CL}_{\langle M' \rangle}(\varphi') = \mathrm{CL}_{\langle M \rangle}(\varphi)$ immediately by definition and $\between_{\nu \in N} \mathcal{HC}(\nu) = \between_{\nu \in N'} \mathcal{HC}(\nu)$ by the above observation that $\mathcal{HC}(\nu) = \mathcal{HC}(\nu')$ for each $\nu \in N$ and its unique ancestor ν'.

   (b) If ρ is a binary rule, let $\diamond = \cup$ if ρ operates on $\langle M \rangle$ and $\diamond = \times$ otherwise. By the induction hypothesis

   $$\begin{aligned} \mathrm{CL}_{\langle M_1 \uplus N_1 \rangle}(\varphi_1) \diamond \mathrm{CL}_{\langle M_2 \uplus N_2 \rangle}(\varphi_2) \quad \trianglelefteq \quad & (\mathrm{CL}_{\langle M_1 \rangle}(\varphi_1) \between_{\nu \in N_1} \mathcal{HC}(\nu)) \diamond \\ & (\mathrm{CL}_{\langle M_2 \rangle}(\varphi_2) \between_{\nu \in N_2} \mathcal{HC}(\nu)) \end{aligned}$$

   But $\mathrm{CL}_{\langle M_1 \uplus N_1 \rangle}(\varphi_1) \diamond \mathrm{CL}_{\langle M_2 \uplus N_2 \rangle}(\varphi_2) = \mathrm{CL}_{\langle M \uplus N \rangle}(\varphi)$ and $(A \times B) \cup (C \times D) \trianglelefteq (A \cup C) \times B \times D$ and thus

   $$\mathrm{CL}_{\langle M \uplus N \rangle}(\varphi) \trianglelefteq (\mathrm{CL}_{\langle M_1 \rangle}(\varphi_1) \diamond \mathrm{CL}_{\langle M_2 \rangle}(\varphi_2)) \between_{\nu \in N_1} \mathcal{HC}(\nu) \between_{\nu \in N_2} \mathcal{HC}(\nu)$$

But as all $\nu \in N$ have exactly one ancestor we obtain

$$\mathrm{CL}_{\langle M \uplus N\rangle}(\varphi) \trianglelefteq \mathrm{CL}_{\langle M\rangle}(\varphi) \mathbin{⨯}_{\nu\in N} \mathcal{HC}(\nu)$$

2. The rule ρ has a main occurrence ν_0 and $\nu_0 \in N$. Note that all $\nu \in N \setminus \{\nu_0\}$ have a unique ancestor ν' and thus $\mathcal{HC}(\nu) = \mathcal{HC}(\nu')$.

   (a) If ν_0 does not have an ancestor (ρ must be weakening) then by the induction hypothesis

   $$\mathrm{CL}_{\langle M' \uplus N'\rangle}(\varphi') \trianglelefteq \mathrm{CL}_{\langle M'\rangle}(\varphi') \mathbin{⨯}_{\nu\in N'} \mathcal{HC}(\nu)$$

   The result follows from the observation that – due to $\mathcal{HC}(\nu_0) = \{\emptyset\}$ – $\mathbin{⨯}_{\nu\in N'}\mathcal{HC}(\nu) = \mathbin{⨯}_{\nu\in N}\mathcal{HC}(\nu)$.

   (b) If ν_0 has exactly one immediate ancestor then ρ must be unary, all $\nu \in N$ have exactly one ancestor and the argument of case (1a) applies.

   (c) If ν_0 has exactly two immediate ancestors ν_0^1, ν_0^2 and these occur in the same sequent, then ρ is unary and by the induction hypothesis

   $$\mathrm{CL}_{\langle M' \uplus N'\rangle}(\varphi') \trianglelefteq \mathrm{CL}_{\langle M'\rangle}(\varphi') \mathbin{⨯}_{\nu\in N'} \mathcal{HC}(\nu)$$

   The result then follows from the observation that – due to $\mathcal{HC}(\nu_0) = \mathcal{HC}(\nu_0^1) \times \mathcal{HC}(\nu_0^2)$ – we have $\mathbin{⨯}_{\nu\in N'}\mathcal{HC}(\nu) = \mathbin{⨯}_{\nu\in N}\mathcal{HC}(\nu)$.

   (d) If ν_0 has exactly two immediate ancestors ν_0^1, ν_0^2 and these occur in different sequents, then ρ is binary and operates on $\langle M \uplus N\rangle$ but not on $\langle M\rangle$. Let w.l.o.g. $\nu_0^1 \in N_1, \nu_0^2 \in N_2$. By induction hypothesis

   $$\begin{array}{lll} \mathrm{CL}_{\langle M_1 \uplus N_1\rangle}(\varphi_1) \cup \mathrm{CL}_{\langle M_2 \uplus N_2\rangle}(\varphi_2) & \trianglelefteq & (\mathrm{CL}_{\langle M_1\rangle}(\varphi_1) \mathbin{⨯}_{\nu\in N_1} \mathcal{HC}(\nu)) \\ & & \cup(\mathrm{CL}_{\langle M_2\rangle}(\varphi_2) \mathbin{⨯}_{\nu\in N_2} \mathcal{HC}(\nu)) \end{array}$$

   But as $\mathrm{CL}_{\langle M\uplus N\rangle}(\varphi) = \mathrm{CL}_{\langle M_1\uplus N_1\rangle}(\varphi_1) \cup \mathrm{CL}_{\langle M_2\uplus N_2\rangle}(\varphi_2)$ and $(A \times B) \cup (C \times D) \trianglelefteq (A \cup C) \times B \times D$ we have

   $$\begin{array}{lll} \mathrm{CL}_{\langle M\uplus N\rangle}(\varphi) & \trianglelefteq & ((\mathrm{CL}_{\langle M_1\rangle}(\varphi_1) \times \mathcal{HC}(\nu_0^1)) \\ & & \cup(\mathrm{CL}_{\langle M_2\rangle}(\varphi_2) \times \mathcal{HC}(\nu_0^2))) \\ & & \mathbin{⨯}_{\nu\in N_1\setminus\{\nu_0^1\}}\mathcal{HC}(\nu) \\ & & \mathbin{⨯}_{\nu\in N_2\setminus\{\nu_0^2\}}\mathcal{HC}(\nu) \end{array}$$

   As all $\nu \in N \setminus \{\nu_0\}$ have exactly one ancestor

   $$\mathbin{⨯}_{\nu\in N_1\setminus\{\nu_0^1\}}\mathcal{HC}(\nu) \mathbin{⨯}_{\nu\in N_2\setminus\{\nu_0^2\}} \mathcal{HC}(\nu) = \mathbin{⨯}_{\nu\in N\setminus\{\nu_0\}}\mathcal{HC}(\nu)$$

Again with $(A \times B) \cup (C \times D) \trianglelefteq A \times C \times (B \cup D)$ we have

$$(\mathrm{CL}_{\langle M_1 \rangle}(\varphi_1) \times \mathcal{HC}(\nu_0^1)) \cup (\mathrm{CL}_{\langle M_2 \rangle}(\varphi_2) \times \mathcal{HC}(\nu_0^2)) \trianglelefteq$$
$$\mathrm{CL}_{\langle M_1 \rangle}(\varphi_1) \times \mathrm{CL}_{\langle M_2 \rangle}(\varphi_2) \times (\mathcal{HC}(\nu_0^1) \cup \mathcal{HC}(\nu_0^2))$$

and as $\mathcal{HC}(\nu_0) = \mathcal{HC}(\nu_0^1) \cup \mathcal{HC}(\nu_0^2)$ and $\mathrm{CL}_{\langle M \rangle}(\varphi) = \mathrm{CL}_{\langle M_1 \rangle}(\varphi_1) \times \mathrm{CL}_{\langle M_2 \rangle}(\varphi_2)$ we finally obtain

$$\mathrm{CL}_{\langle M \uplus N \rangle}(\varphi) \trianglelefteq \mathrm{CL}_{\langle M \rangle}(\varphi) \bigtimes_{\nu \in N} \mathcal{HC}(\nu)$$

□

We are now ready to prove the first main theorem: $\mathrm{P}^{\Omega\mathrm{T}}(\varphi)$ propositionally subsumes the natural composition of the conjunctive normal forms of the partial Herbrand-sequents of the cut occurrences. This means that on the first-order level these two clause sets are the same: The Ω-profile characterizes exactly the used instances of the cut-formulas.

Theorem 4.2. Let φ be an **LK**-proof and let $\{\omega_1^+, \omega_1^-, \ldots, \omega_n^+, \omega_n^-\}$ be the cut occurrences ordered s.t. ω_i^+ and ω_i^- are auxiliary occurrences of the same cut. Then

$$\mathrm{P}^{\Omega\mathrm{T}}(\varphi) \trianglelefteq \bigtimes_{i=1}^{n} (\mathrm{CNF}(\mathcal{H}(\omega_i^-)) \cup \mathrm{CNF}(\mathcal{H}(\omega_i^+)))$$

Proof. By Lemma 4.3 and the relation between $\mathrm{P}^{\Omega\mathrm{T}}$ and CL it suffices to show

$$\mathrm{CL}(\varphi) \trianglelefteq \bigtimes_{i=1}^{n} (\mathcal{HC}(\omega_i^-) \cup \mathcal{HC}(\omega_i^+))$$

We proceed by induction on n. If $n = 0$ then φ does not contain cuts, $\mathrm{CL}(\varphi) = \{\emptyset\}$ and the empty product is also $\{\emptyset\}$. If $n > 0$ then we can assume that φ ends with a binary rule ρ that either (1) is a cut or (2) contains a cut in each of its immediate sub-proofs. For if φ does not end with such a rule, observe that $\mathrm{CL}(\varphi) = \mathrm{CL}(\psi[\varphi])$ for each cut-free context $\psi[]$.

1. If ρ is a cut, let φ_1, φ_2 be the immediate sub-proofs of φ, let $\Omega_1 = \{\omega_1^+, \omega_1^-, \ldots, \omega_k^+, \omega_k^-\}$ and $\Omega_2 = \{\omega_{k+1}^+, \omega_{k+1}^-, \ldots, \omega_{n-1}^+, \omega_{n-1}^-\}$ be the occurrences of cut formulas of cuts in φ_1 and φ_2 and let ω_n^+ (ω_n^-) be the occurrence of the cut formula of ρ in φ_1 (φ_2). Then by definition

$$\mathrm{CL}(\varphi) = \mathrm{CL}_{\langle \Omega_1 \cup \{\omega_n^+\} \rangle}(\varphi_1) \cup \mathrm{CL}_{\langle \Omega_2 \cup \{\omega_n^-\} \rangle}(\varphi_2)$$

Applying Lemma 4.4 and the induction hypothesis we obtain

$$\begin{aligned} \mathrm{CL}(\varphi) \quad \trianglelefteq \quad & ((\bigtimes_{i=1}^{k} (\mathcal{HC}(\omega_i^+) \cup \mathcal{HC}(\omega_i^-))) \times \mathcal{HC}(\omega_n^+)) \cup \\ & ((\bigtimes_{i=k+1}^{n-1} (\mathcal{HC}(\omega_i^+) \cup \mathcal{HC}(\omega_i^-))) \times \mathcal{HC}(\omega_n^-)) \end{aligned}$$

The result then follows from $(A \times B) \cup (C \times D) \trianglelefteq A \times C \times (B \cup D)$.

2. If ρ is not a cut, then by definition

$$\mathrm{CL}(\varphi) = \mathrm{CL}(\varphi_1) \times \mathrm{CL}(\varphi_2)$$

and as both φ_1 and φ_2 contain at least one cut, the result follows immediately from the induction hypothesis.

□

4.2.5 Σ-Subsumption

In this section we investigate the Σ-profiles and we will show that $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi)$ is propositionally subsumed by the disjunctive normal form of the partial Herbrand sequent of the Σ-part. This partial Herbrand-sequent is the Herbrand-sequent of the partial proof arising from φ by dropping all Ω-rules. Note that the proof projections of the CERES-method (see [8]) can be generated from this partial proof by replacing juxtapositions by weakenings (and completing the axioms). First some simple technical lemmas:

Lemma 4.5. Let φ, φ' be $\mathbf{LK^j}$-proofs with $\varphi \rightarrow^*_{\mathcal{M}} \varphi'$. Then

1. $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi')$ and
2. $\mathcal{H}(\varphi) = \mathcal{H}(\varphi')$

Proof Sketch. 1 Follows from the fact that $\rightarrow_{\mathcal{M}}$ moves only unary rules and 2 follows from Proposition 4.3. □

Lemma 4.6. Let φ be a cut-free $\mathbf{LK^j}$-proof with quantifier-free end-sequent s. Then there is a cut-free $\mathbf{LK^j}$-proof φ' with quantifier-free end-sequent $\mathrm{U}(s)$ s.t.

1. $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi')$ and
2. $\mathcal{H}(\varphi) = \mathcal{H}(\varphi')$

Proof Sketch. By shifting weakening rules towards the end-sequent. □

Lemma 4.7. Let φ be a cut-free $\mathbf{LK^j}$-proof with quantifier-free end-sequent s. Then there is a cut-free $\mathbf{LK^j}$-proof φ' with quantifier-free end-sequent $\mathrm{set}(s)$ s.t.

1. $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi')$ and
2. $\mathcal{H}(\varphi) = \mathcal{H}(\varphi')$

Proof Sketch. By adding contractions at the end of the proof. □

Now we will show that the Σ-profile of a part of the end-sequent depends only on the partial proof of this part.

Lemma 4.8. Let φ be an **LK**-proof and let N be a set of end occurrences of φ. Then

$$\mathrm{P}^{\Sigma\mathrm{T}}_{\langle N\rangle}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi \mid \langle N\rangle)$$

Proof. We will proceed by induction on φ.

1. If φ is an axiom sequent α, then $\mathrm{P}^{\Sigma\mathrm{T}}_{\langle N\rangle}(\varphi) = \mathrm{S}(\alpha, N) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi \mid \langle N\rangle)$.

2. If φ ends with a unary rule ρ, let s' be its premise sequent, let φ' be the immediate sub-proof of φ and let N' be the immediate ancestors of N. As ρ is unary we immediately have $\mathrm{P}^{\Sigma\mathrm{T}}_{\langle N\rangle}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}_{\langle N'\rangle}(\varphi')$ but also $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi \mid \langle N\rangle) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi' \mid \langle N'\rangle)$ because either $\varphi \mid \langle N\rangle$ and $\varphi' \mid \langle N'\rangle$ are equal or they differ by just a unary rule.

3. If φ ends with a binary rule ρ, let s_1, s_2 be its premise sequents and let φ_1, φ_2 be the proofs of s_1, s_2 respectively. Let N_1, N_2 be the immediate ancestors of N in φ_1 and φ_2.

   (a) If the main occurrence of ρ is in N, then $\mathrm{P}^{\Sigma\mathrm{T}}_{\langle N\rangle}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}_{\langle N_1\rangle}(\varphi_1) \times_{\mathcal{L}(\rho)} \mathrm{P}^{\Sigma\mathrm{T}}_{\langle N_2\rangle}(\varphi_2)$. By the induction hypothesis $\mathrm{P}^{\Sigma\mathrm{T}}_{\langle N\rangle}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1 \mid \langle N_1\rangle) \times_{\mathcal{L}(\rho)} \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2 \mid \langle N_2\rangle)$, but as $\varphi \mid \langle N\rangle$ is ρ applied to $\varphi_1 \mid \langle N_1\rangle$ and $\varphi_2 \mid \langle N_2\rangle$ and as the label set of the copy of ρ at the end of $\varphi \mid \langle N\rangle$ is still $\mathcal{L}(\rho)$ we obtain $\mathrm{P}^{\Sigma\mathrm{T}}_{\langle N\rangle}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi \mid \langle N\rangle)$.

   (b) If ρ has no main occurrence (i.e. is a cut) or the main occurrence is not in N then ρ does not operate on $\langle N\rangle$ and so $\mathrm{P}^{\Sigma\mathrm{T}}_{\langle N\rangle}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}_{\langle N_1\rangle}(\varphi_1) \cup \mathrm{P}^{\Sigma\mathrm{T}}_{\langle N_2\rangle}(\varphi_2)$.
   If both $N_1 \neq \emptyset$ and $N_2 \neq \emptyset$ then $\varphi \mid \langle N\rangle$ ends with a juxtaposition rule which does not operate on $\Sigma(\varphi \mid \langle N\rangle)$ and so $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi \mid \langle N\rangle) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1 \mid \langle N_1\rangle) \cup \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2 \mid \langle N_2\rangle)$. The result then follows from the induction hypothesis.
   If $N_1 = \emptyset$ then $\varphi \mid \langle N\rangle = \varphi_2 \mid \langle N_2\rangle$ and thus $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi \mid \langle N\rangle) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2 \mid \langle N_2\rangle)$ and the result follows from the induction hypothesis. If $N_2 = \emptyset$ the same argument applies.

□

Now considering only the upper (propositional) part of a cut-free proof in $\mathcal{M}$-NF we show that the disjunctive normal form of the end-sequent of the upper part propositionally subsumes the Σ-profile.

Lemma 4.9. Let φ be a cut-free $\mathbf{LK^j}$-proof with quantifier-free end-sequent s. Then

$$\mathrm{DNF}(s) \trianglelefteq \mathrm{P}^{\Sigma\mathrm{T}}(\varphi)$$

Proof. Define the relation $\trianglelefteq^{\mathrm{L}}$ between sets of labelled clauses as follows: $C \trianglelefteq^{\mathrm{L}} D$ if $\forall d \in D \exists c \in C$ with $\mathrm{set}(c) \subseteq \mathrm{set}(d)$ and $\mathcal{L}(c) \cap \mathcal{L}(d) \neq \emptyset$. Clearly $C \trianglelefteq^{\mathrm{L}} D$ implies $C \trianglelefteq D$. We will show $\mathrm{DNF}(s) \trianglelefteq^{\mathrm{L}} \mathrm{P}^{\Sigma\mathrm{T}}(\varphi)$ by induction on φ.

If φ is an axiom sequent then $\mathrm{DNF}(s) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi)$. If φ ends with a unary rule ρ, let φ' be the immediate sub-proof of φ and let s' be the end-sequent of φ'. As ρ is unary $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi')$ and by using the induction hypothesis it remains to show that $\mathrm{DNF}(s) \trianglelefteq^{\mathrm{L}} \mathrm{DNF}(s')$. For the propositional rules $\neg : l, \neg : r, \wedge : l, \vee : r$ and $\rightarrow : r$ it can be easily checked that $\mathrm{DNF}(s) = \mathrm{DNF}(s')$ by DNF-rewriting steps. If ρ is weakening then $\mathrm{DNF}(s) = D \cup C$ and $\mathrm{DNF}(s') = D$ for some sets of labelled clauses C, D and $D \cup C \trianglelefteq^{\mathrm{L}} D$. If ρ is a contraction, then $\mathrm{DNF}(s) = D \cup C$ and $\mathrm{DNF}(s') = D \cup C' \cup C''$ where C, C' and C'' have exactly the same clauses modulo labels. Thus, let $f'(f'')$ be the bijection mapping an atom occurrence in C to the same atom occurrence in $C'(C'')$. Then for the labels we have $\mathcal{L}(a) = \mathcal{L}(f'(a)) \cup \mathcal{L}(f''(a))$ and thus $D \cup C \trianglelefteq^{\mathrm{L}} D \cup C' \cup C''$.

If φ ends with a binary rule ρ, let φ_1, φ_2 be the two immediate sub-proofs of φ and let s_1, s_2 be their respective end-sequents.

If ρ is a juxtaposition, then $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1) \cup \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2)$ and as $s = s_1 \circ s_2$ also $\mathrm{DNF}(s) = \mathrm{DNF}(s_1) \cup \mathrm{DNF}(s_2)$ and the result follows from the induction hypothesis.

If ρ is an $\wedge : r$-rule then it has the following form:

$$\frac{\overset{(\varphi_1)}{\Gamma \vdash \Delta, A} \quad \overset{(\varphi_2)}{\Pi \vdash \Lambda, B}}{\Gamma, \Pi \vdash \Delta, \Lambda, A \wedge B} \wedge\text{: r}[\rho]$$

Abbreviating $\mathcal{L}(\rho)$ as L we have

$$\begin{aligned} \mathrm{P}^{\Sigma\mathrm{T}}(\varphi) &= \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1) \times_L \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2) \\ &= (\mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1)^L \times \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2)^L) \cup \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1)^{\neg L} \cup \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2)^{\neg L} \end{aligned}$$

Furthermore

$$\mathrm{DNF}(s) = \mathrm{DNF}(\Gamma \vdash \Delta) \cup \mathrm{DNF}(\Pi \vdash \Lambda) \cup \mathrm{DNF}(\vdash A \wedge B)$$

and

$$\mathrm{DNF}(s_1) = \mathrm{DNF}(\Gamma \vdash \Delta) \cup \mathrm{DNF}(\vdash A)$$

and

$$\mathrm{DNF}(s_2) = \mathrm{DNF}(\Pi \vdash \Lambda) \cup \mathrm{DNF}(\vdash B)$$

We will now show that $\forall d \in \mathrm{P}^{\Sigma\mathrm{T}}(\varphi) \exists c \in \mathrm{DNF}(s)$ s.t. $\mathrm{set}(c) \subseteq \mathrm{set}(d)$ and $\mathcal{L}(c) \cap \mathcal{L}(d) \neq \emptyset$ by a case distinction:

1. $d \in \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1)^{\neg L}$: Then $d \in \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1)$ and by induction hypothesis there is a $c \in \mathrm{DNF}(s_1)$ with $\mathrm{set}(c) \subseteq \mathrm{set}(d)$ and $\mathcal{L}(c) \cap \mathcal{L}(d) \neq \emptyset$. But $s_1 = \Gamma \vdash \Delta, A$ and $c \in \mathrm{DNF}(\Gamma \vdash \Delta)$ because if $c \in \mathrm{DNF}(\vdash A)$ then $\mathcal{L}(c) \cap \mathcal{L}(d) = \emptyset$ because $\mathcal{L}(c) \subseteq L$ and $d \in \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1)^{\neg L}$, so $c \in \mathrm{DNF}(s)$.

2. If $d \in \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2)^{\neg L}$ we proceed analogously to the previous case.

3. If $d = d_1 \circ d_2$ with $d_1 \in \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_1)^{L}$ and $d_2 \in \mathrm{P}^{\Sigma\mathrm{T}}(\varphi_2)^{L}$ then by the induction hypothesis there are $c_1 \in \mathrm{DNF}(\Gamma \vdash \Delta, A)$ and $c_2 \in \mathrm{DNF}(\Pi \vdash \Lambda, B)$ with $\mathrm{set}(c_i) \subseteq \mathrm{set}(d_i)$ and $\mathcal{L}(c_i) \cap \mathcal{L}(d_i) \neq \emptyset$ for both $i = 1, 2$. Now for both c_i we have $\mathrm{set}(c_i) \subseteq \mathrm{set}(d)$ and $\mathcal{L}(c_i) \cap \mathcal{L}(d) \neq \emptyset$. If $c_1 \in \mathrm{DNF}(\Gamma \vdash \Delta)$, then $c_1 \in \mathrm{DNF}(s)$ and if $c_2 \in \mathrm{DNF}(\Pi \vdash \Lambda)$ then $c_2 \in \mathrm{DNF}(s)$. So, assuming both $c_1 \notin \mathrm{DNF}(\Gamma \vdash \Delta)$ and $c_2 \notin \mathrm{DNF}(\Pi \vdash \Lambda)$ we have $c_1 \in \mathrm{DNF}(\vdash A)$ and $c_2 \in \mathrm{DNF}(\vdash B)$. But then $c_1 \circ c_2 \in \mathrm{DNF}(\vdash A \wedge B) \subseteq \mathrm{DNF}(s)$ and also $\mathrm{set}(c_1 \circ c_2) \subseteq \mathrm{set}(d)$ and $\mathcal{L}(c_1 \circ c_2) \cap \mathcal{L}(d) \neq \emptyset$.

   For the other binary rules we proceed analogously.

□

We can now establish a subsumption relation between the Σ-profile and the instances of the end-sequent in a way that is analogous to the relation in the Ω-part shown in Theorem 4.2.

Theorem 4.3. Let φ be an **LK**-proof with a prenex end-sequent and let σ be the set of end occurrences. Then

$$\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) \trianglerighteq \mathrm{DNF}(\mathcal{H}(\varphi \mid \langle\sigma\rangle))$$

Proof. Let φ' be the $\mathbf{LK}^{\mathbf{j}}$-proof $\varphi \mid \langle\sigma\rangle$, then by Lemma 4.8 using $N = \sigma$ we have $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi) = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi')$. Let φ'' be a mid-sequent normal form of φ', then by Lemma 4.5 $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi'') = \mathrm{P}^{\Sigma\mathrm{T}}(\varphi')$ and $\mathcal{H}(\varphi'') = \mathcal{H}(\varphi')$. As φ'' is a mid-sequent normal form, there is a propositional or juxtaposition rule ρ s.t. all other propositional or juxtaposition rules are above ρ and all quantifier rules are below ρ. Let χ be the sub-proof of φ'' ending with ρ. As all rules below ρ are unary, we have $\mathrm{P}^{\Sigma\mathrm{T}}(\varphi'') = \mathrm{P}^{\Sigma\mathrm{T}}(\chi)$ and $\mathcal{H}(\varphi'') = \mathcal{H}(\chi)$.

By Lemma 4.6 there is an $\mathbf{LK}^{\mathbf{j}}$-proof χ' whose end-sequent is $\mathrm{U}(s)$ where s is the end-sequent of χ. Applying Lemma 4.7 to χ' gives an $\mathbf{LK}^{\mathbf{j}}$-proof χ'' with end-sequent $s'' = \mathrm{set}(\mathrm{U}(s))$ and $\mathrm{P}^{\Sigma\mathrm{T}}(\chi'') = \mathrm{P}^{\Sigma\mathrm{T}}(\chi)$. Applying now Lemma 4.9 to χ'' gives $\mathrm{P}^{\Sigma\mathrm{T}}(\chi'') \trianglerighteq \mathrm{DNF}(s'')$ but by definition $s'' = \mathcal{H}(\chi)$ which concludes the proof.

□

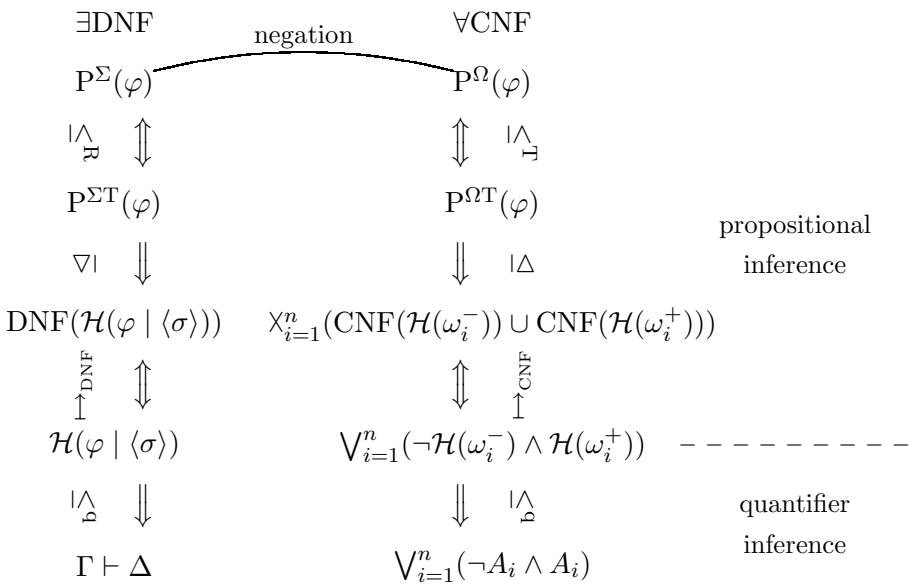


Figure 4.1: The Global Picture

4.2.6 Discussion

Summing up we have shown the relations as depicted in Figure 4.1 (for a proof φ with end-sequent $\Gamma \vdash \Delta$, set of end occurrences σ, cut-formulas $A_1, \ldots, A_n$ and respective cut occurrences $\omega_1^-, \omega_1^+, \ldots, \omega_n^-, \omega_n^+$). We have shown the syntactic relations (noted on the outside), the semantic relations, i.e. implication or equivalence (noted on the inside) hold as corollaries. The left side of the figure contains the information of the end-sequent part (clause sets here are interpreted as existentially quantified disjunctive normal forms), the right side contains the information of the cut-formulas part where clause sets are interpreted as universally quantifier conjunctive normal form. The separation between quantifier inferences and propositional inferences (on both sides) is clearly visible. The composition of the cut-formulas: $\bigvee_{i=1}^{n}(\neg A_i \wedge A_i)$ is obviously unsatisfiable and from this unsatisfiability it follows (going counterclockwise) that each element on the right side is unsatisfiable and each element on the left side is valid. This gives an alternative proof of the unsatisfiability of the characteristic clause set.

Corollary 4.2. Let φ be an **LK**-proof. Then $\mathrm{CL}(\varphi)$ is unsatisfiable.

Proof. By unsatisfiability of $\mathrm{P}^{\Omega}(\varphi)$ which follows from the relations depicted in Figure 4.1. □

The profiles $\mathrm{P}^{\Omega}(\varphi)$ and $\mathrm{P}^{\Sigma}(\varphi)$ being exactly dual to each other constitute *the two sides of the boundary* between the part of a proof that concerns the end-sequent and the part that concerns the cut-formulas.

The cut-elimination method CERES uses a resolution refutation of $\mathrm{P}^{\Omega}(\varphi)$ as a skeleton of a cut-free proof in which parts of $\varphi \mid \langle\sigma\rangle$ are plugged in to obtain the final cut-free proof (see [8] for details). The duality between $\mathrm{P}^{\Sigma}(\varphi)$ and $\mathrm{P}^{\Omega}(\varphi)$ allows to generate $\mathrm{P}^{\Omega}(\varphi)$ *from the end-sequent part* by generating $\mathrm{P}^{\Sigma}(\varphi)$ and negating it. Cut-elimination with CERES can thus be seen as a method that works on ancestors of the end-sequent only, i.e. a method transforming partial cut-free proofs into non-partial cut-free proofs. But not all partial cut-free proofs can be transformed into non-partial cut-free proofs because the end-sequent is not necessarily a tautology. The partial proofs generated by dropping exactly the cut ancestors have - among all partial proofs - the property that the dropped part is unsatisfiable (cf. the formula $\bigvee_{i=1}^{n}(\neg A_i \wedge A_i)$) and thus the end-sequent part is valid having a tautology as end-sequent.

By the duality of resolution the resolution refutation of $\mathrm{P}^{\Omega}(\varphi)$ can be seen as a *positive proof* of $\mathrm{P}^{\Sigma}(\varphi)$, so a normal form under cut-elimination is not only a (cut-free) proof of $\Gamma \vdash \Delta$, but also a cut-free proof of $\mathcal{H}(\varphi \mid \langle\sigma\rangle)$ via the Σ-profile. The converse holds for CERES, but not for reductive cut-elimination procedures (à la Gentzen). This allows to discriminate normal forms of a proof from other cut-free proofs of the same end-sequent.

Note that the assumption of prenex formulas is only relevant for the $\mathcal{H}$-operator, not for the profiles. As future work we plan to extend these results to the case of non-prenex formulas with a Herbrand-sequent extraction as in [6].

4.3 The Relation to Logical Flow Graphs

Logical flow graphs have been introduced in [12] in order to show that it is undecidable wether a given formula has a proof of length less than a given natural number k. Logical flow graphs, in particular those on the atom occurrences in a proof (the *atomic flow graphs*), are a simple representation of the abstract structure of a proof. They have interesting relations to cut-elimination which have been extensively studied in [14, 15, 16, 17, 18], see also [19]. In this chapter we will give a rather informal analysis of the relation between the profile and a variant of logical flow graphs on a sequence of proofs with exponential cut-elimination (taken from [7]).

Definition 4.17. Let P be a binary predicate symbol and f a unary function symbol. We define the abbreviations T for $(\forall x)(\forall y)(\forall z)((P(x,y) \wedge P(y,z)) \rightarrow P(x,z))$ and $A_k(m,n)$ for $P(f^m(\alpha_k), f^n(\alpha_k))$. We define a se-

quence of proofs $(\psi_k)_{k\geq 1}$ as follows: $\psi_k :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{A_k(2^k,2^{k-1}) \vdash^{1_k} A_k(2^k,2^{k-1}) \quad A_k(2^{k-1},0) \vdash^{2_k} A_k(2^{k-1},0)}{A_k(2^k,2^{k-1}), A_k(2^{k-1},0) \vdash A_k(2^k,2^{k-1}) \wedge A_k(2^{k-1},0)} \wedge\text{: r} \quad A_k(2^k,0) \vdash^{3_k} A_k(2^k,0)}{(A_k(2^k,2^{k-1}) \wedge A_k(2^{k-1},0)) \to A_k(2^k,0), A_k(2^k,2^{k-1}), A_k(2^{k-1},0) \vdash A_k(2^k,0)} \to : \text{l}}{T, A_k(2^k,2^{k-1}), A_k(2^{k-1},0) \vdash A_k(2^k,0)} \forall\text{: l(3x)}}{T, A_k(2^k,2^{k-1}), (\forall x)P(f^{2^{k-1}}(x),x) \vdash A_k(2^k,0)} \forall\text{: l}}{T, (\forall x)P(f^{2^{k-1}}(x),x), (\forall x)P(f^{2^{k-1}}(x),x) \vdash A_k(2^k,0)} \forall\text{: l}}{T, (\forall x)P(f^{2^{k-1}}(x),x) \vdash A_k(2^k,0)} \text{c} : \text{l}}{T, (\forall x)P(f^{2^{k-1}}(x),x) \vdash (\forall x)P(f^{2^k}(x),x)} \forall\text{: r}$$

where $1_k, 2_k$ and 3_k are the labels of the axioms (depending on k). Based on $(\psi_k)_{k\geq 1}$ we define another sequence $(\tau_k)_{k\geq 0}$ as follows: $\tau_0 :=$

$$\dfrac{\dfrac{\dfrac{P(f(\alpha_0),\alpha_0) \vdash^{3_0} P(f(\alpha_0),\alpha_0))}{(\forall x)P(f(x),x) \vdash P(f(\alpha_0),\alpha_0)} \forall\text{: l}}{(\forall x)P(f(x),x) \vdash (\forall x)P(f(x),x)} \forall\text{: r}}{T, (\forall x)P(f(x),x) \vdash (\forall x)P(f(x),x)} \text{w} : \text{l}$$

and $\tau_{k+1} :=$

$$\dfrac{\dfrac{(\tau_k) \qquad\qquad (\psi_{k+1})}{T, (\forall x)P(f(x),x) \vdash (\forall x)P(f^{2^k}(x),x) \quad (\forall x)P(f^{2^k}(x),x), T \vdash (\forall x)P(f^{2^{k+1}}(x),x)} \text{cut}}{T, T, (\forall x)P(f(x),x) \vdash (\forall x)P(f^{2^{k+1}}(x),x)} \text{c} : \text{l}}{T, (\forall x)P(f(x),x) \vdash (\forall x)P(f^{2^{k+1}}(x),x)}$$

By analysis of these proofs one can calculate that:

$$\mathrm{P}^{\Omega\mathrm{T}}(\tau_0) = \{\vdash^{3_0}\}$$

and

$$\mathrm{P}^{\Omega\mathrm{T}}(\tau_{k+1}) = \{\vdash^{3_0} A_0(1,0)\} \bigcup_{l=1}^{k} X_k \cup X'_{k+1}$$

where the unions arise from the cut rules and

$$\begin{aligned} X_k &= (\{A_k(2^k,2^{k-1}) \vdash^{1_k}\} \times_{1_k,2_k} \{A_k(2^{k-1},0) \vdash^{2_k}\}) \times_{1_k,2_k,3_k} \{\vdash^{3_k} A_k(2^k,0)\} \\ &= \{A_k(2^k,2^{k-1}), A_k(2^{k-1},0) \vdash^{1_k,2_k,3_k} A_k(2^k,0)\} \end{aligned}$$

and

$$\begin{aligned} X'_k &= (\{A_k(2^k,2^{k-1}) \vdash^{1_k}\} \times_{1_k,2_k} \{A_k(2^{k-1},0) \vdash^{2_k}\}) \times_{1_k,2_k,3_k} \{\vdash^{3_k}\} \\ &= \{A_k(2^k,2^{k-1}), A_k(2^{k-1},0) \vdash^{1_k,2_k,3_k}\} \end{aligned}$$

with the products arising from the $\wedge$: r- and $\rightarrow$: l-rules in the ψ_k. The difference between X_k and X'_k lies only in the status of the positive atom of the 3_k-axiom: In X_k it is cut-ancestor, in X'_k it is ancestor of the end-sequent. Furthermore

$$\mathrm{P}^{\Sigma\mathrm{T}}(\tau_0) = \{A_0(1,0) \vdash^{3_0} A_0(1,0)\}$$

and

$$\mathrm{P}^{\Sigma\mathrm{T}}(\tau_{k+1}) = (\cdots(\{A_0(1,0) \vdash^{3_0}\} \times_{3_0,1_1,2_1} Y_1) \ldots \times_{3_{k-1},1_k,2_k} Y_k) \times_{3_k,1_{k+1},2_{k+1}} Y'_{k+1}$$

where the product arise from the cut rules and

$$\begin{aligned} Y_k &= \{\vdash^{1_k} A_k(2^k, 2^{k-1})\} \cup \{\vdash^{2_k} A_k(2^{k-1}, 0)\} \cup \{A_k(2^k, 0) \vdash^{3_k}\} \\ &= \{\vdash^{1_k} A_k(2^k, 2^{k-1}) \,;\, \vdash^{2_k} A_k(2^{k-1}, 0) \,;\, A_k(2^k, 0) \vdash^{3_k}\} \end{aligned}$$

with the unions – as the products in X_k – coming from the binary rules in ψ_k.

$$\begin{aligned} Y'_k &= \{\vdash^{1_k} A_k(2^k, 2^{k-1})\} \cup \{\vdash^{2_k} A_k(2^{k-1}, 0)\} \cup \{A_k(2^k, 0) \vdash^{3_k} A_k(2^k, 0)\} \\ &= \{\vdash^{1_k} A_k(2^k, 2^{k-1}) \,;\, \vdash^{2_k} A_k(2^{k-1}, 0) \,;\, A_k(2^k, 0) \vdash^{3_k} A_k(2^k, 0)\} \end{aligned}$$

Calculating the value of the product of the Y_k we obtain

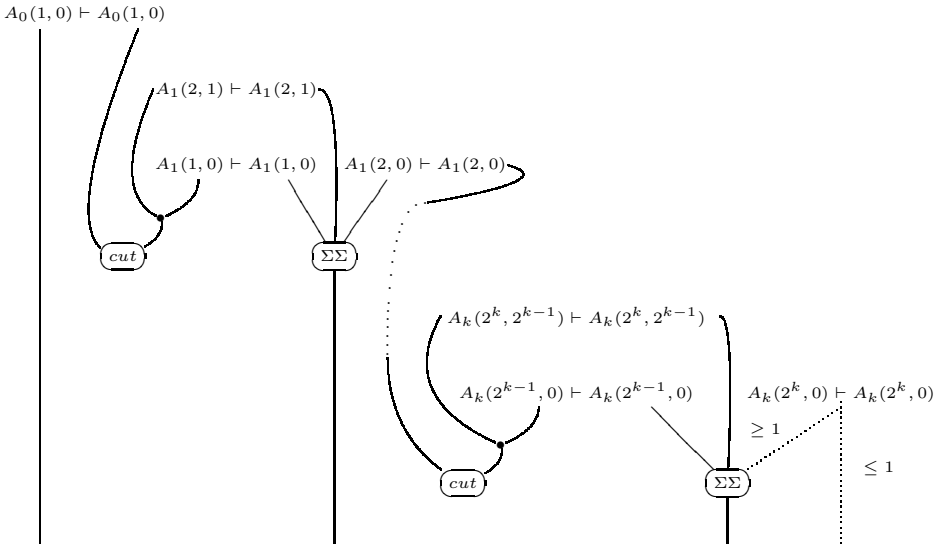
$$\mathrm{P}^{\Sigma\mathrm{T}}(\tau_{k+1}) = \bigcup_{l=0}^{k} Z_k \cup \{A_{k+1}(2^{k+1}, 0) \vdash^{3_{k+1}} A_{k+1}(2^{k+1}, 0)\}$$

where

$$Z_k = \{A_k(2^k, 0) \vdash^{3_k,1_{k+1}} A_{k+1}(2^{k+1}, 2^k) \,;\, A_k(2^k, 0) \vdash^{3_k,2_{k+1}} A_{k+1}(2^k, 0)\}$$

We will now show on this example sequence that the information present in the profile determines the structure of a proof to a surprisingly large extent.

Theorem 4.4. Let χ be an **LK**-proof with $\mathrm{P}^{\Omega\mathrm{T}}(\chi) = \mathrm{P}^{\Omega\mathrm{T}}(\tau_k)$ and $\mathrm{P}^{\Sigma\mathrm{T}}(\chi) = \mathrm{P}^{\Sigma\mathrm{T}}(\tau_k)$ for a $k \geq 1$, then χ has the following structure



where this picture is to be interpreted as follows: All axioms occurring in χ are shown, lines denote the ancestor relation, unary logical rules are not shown, dots denote contractions, *cut* denotes a cut rule with the two entering lines being the auxiliary formulas, $\Sigma\Sigma$ denotes two binary rules working on ancestors of the endsequent s.t. the main formula of the upper rule is ancestor of an auxiliary formula of the lower rule and the three entering lines are the two auxiliary formulas of the upper and the remaining auxiliary formula of the lower rule, i.e. $\Sigma\Sigma$ denotes a "ternary" rule. The dotted line with ≥ 1 represents at least one ancestor path of the atom occurrences of the rightmost axiom and the dotted line with ≤ 1 is at most one ancestor path of the atom occurrences of the rightmost atom, i.e. the only freedom in this graph concerns the question wether both atoms of the rightmost axiom go into the rightmost $\Sigma\Sigma$-complex or just one.

Proof Sketch. As we are dealing with the profiles containing the tautologies we know from counting the labels in the profile that χ must have $3 \cdot k + 1$ axioms. The number of binary rules of a proof with m axioms must be $m - 1$, so χ has $3 \cdot k$ binary rules. In $\mathrm{P}^{\Omega\mathrm{T}}(\chi)$ there are k product clauses with 3 labels each where the label sets are disjoint. Therefore for each of these clauses there must be a distinct ternary rule (in the above sense). Partitioning the product clauses of $\mathrm{P}^{\Sigma\mathrm{T}}(\chi)$ into label-disjoint sets we obtain k pairs to each of which must correspond a cut (because of the disjointness of the labels). By analyzing the labels of these pairs of products one sees that 3_j must be on one side of the cut and 1_{j+1} and 2_{j+1} must be on the other side of the cut, but as the cut-formula on both sides must be the same

there must be a contraction applied to descendents of the atoms from 1_{j+1} and 2_{j+1}.

Hence we have k independent pairs of rules working on ancestors of the end-sequent and k independent cuts, the connection to the axioms are derived from the labels with the only uncertainty of wether $\vdash^{3_k} A_k(2^k, 0)$ goes directly into the end-sequent or via an (already existing) rule because it does not occur in the last Ω-product in X'_k. □

Note that the above proof shows that these profiles uniquely determine the atomic flow graph of the occurrences that are ancestors of cut formulas. The atomic flow graph of the ancestors of the end-sequent however is not completely determined: Nothing can be said about contractions applied on ancestors of the end-sequent. Indeed, in τ_k the main formulas of the $\Sigma\Sigma$-rules (which is always the transitivity) are contracted into the end-sequent. But there exist proofs χ s.t. these contractions do not take place or where even different forms of writing transitivity are allowed (e.g. the negation normal form of T) at each instance of a $\Sigma\Sigma$-pair of rules.

Chapter 5

The Dynamics of the Profile

In this chapter we will investigate the effect of various proof transformations on the profile.

5.1 Cut-Elimination

In [10] an analysis of the behavior of the original characteristic clause sets under Gentzen's cut-elimination procedure has been given. It has been shown that, if φ is reduced to φ' by cut-elimination steps, the characteristic clause set of φ subsumes that of φ'. The subsumption relation consists of the three basic parts of 1) duplication of clauses (including variable renaming), 2) instantiation of clauses and 3) deletion of clauses. However, due to the nature of this cut-elimination procedure and the characteristic clause sets these three parts occur in a mixed fashion at different cut-elimination steps.

In this section we carry out an analogous analysis but with the important difference that we move from Gentzen's original calculus (which is a mixture of multiplicative and additive rules) to the purely multiplicative calculus **LKps** and from the original characteristic clause sets to the proof profiles defined in this paper. This allows to carry out the analysis of [10] in a much "cleaner" fashion which will make it possible to use the lemmas in the analysis of the effect of transformations defined by cut-elimination (as done in Section 5.2.1). We will now show that

1. duplication of clauses arises iff a contraction rule is eliminated, that
2. instantiation of clauses arises iff a quantifier rule is eliminated and that
3. deletion of clauses arises iff a weakening rule is eliminated.

In all other cases the profile remains unchanged.

Lemma 5.1 (rank-reduction)**.**

$$\chi \to_{\mathrm{G_r}} \chi' \quad \Longrightarrow \quad \mathrm{P}(\chi') = \mathrm{P}(\chi)$$

Proof. As rank-reduction $\to_{\mathrm{G_r}}$ is contained in the permutation of adjacent independent rules $\approx_\pi$, we can apply Proposition 4.1. □

Lemma 5.2 (propositional reduction)**.**

$$\chi \to_{\mathrm{G_p}} \chi' \quad \Longrightarrow \quad \mathrm{P}(\chi') = \mathrm{P}(\chi)$$

Proof. By duality it is enough to show $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi)$. Let μ be the position where the reduction is applied, so $\chi = \chi[\varphi]_\mu$ and $\chi' = \chi[\varphi']_\mu$. We first show $\mathrm{P}^\Omega(\chi').\mu = \mathrm{P}^\Omega(\chi).\mu$ by case distinction on the main connective of the cut at μ:

1. Conjunction: Then φ has the form:

$$\dfrac{\dfrac{\dfrac{(\varphi_1, C)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_2, D)}{\Pi \vdash \Lambda, B}}{\Gamma, \Pi \vdash \Delta, \Lambda, A \wedge B}\ \wedge\!: \mathrm{r} \quad \dfrac{\dfrac{(\varphi_3, E)}{A, B, \Theta \vdash \Sigma}}{A \wedge B, \Theta \vdash \Sigma}\ \wedge\!: \mathrm{l}}{\Gamma, \Pi, \Theta \vdash \Delta, \Lambda, \Sigma}\ \mathrm{cut}$$

   and φ' has the form:

$$\dfrac{\dfrac{(\varphi_2, D)}{\Pi \vdash \Lambda, B} \quad \dfrac{\dfrac{(\varphi_1, C)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\varphi_3, E)}{A, B, \Theta \vdash \Sigma}}{B, \Gamma, \Theta \vdash \Delta, \Sigma}\ \mathrm{cut}}{\Gamma, \Pi, \Theta \vdash \Delta, \Lambda, \Sigma}\ \mathrm{cut}$$

   So we have

$$\mathrm{P}^\Omega(\chi).\mu = (C \cup D) \cup E$$

   and

$$\mathrm{P}^\Omega(\chi').\mu = D \cup (C \cup E)$$

   which are equal by commutativity and associativity of $\cup$.

2. Disjunction: analogous: by commutativity and associativity of $\cup$

3. Implication: analogous: by commutativity and associativity of $\cup$

4. Negation: analogous: by commutativity and associativity of $\cup$

Also condition 2 of Lemma 4.1 is fulfilled because $\to_{\mathrm{G_p}}$ does not change the ancestor axioms of the formula occurrences in the end-sequent of the rewritten part. So we can use Lemma 4.1 to conclude $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi)$. □

Lemma 5.3 (quantifier reduction)**.** Let χ be a regular **LKps**-proof and let

$$\chi \to_{\mathrm{G_q}} \chi'$$

where the substitution $\{\alpha \leftarrow t\}$ is applied to the reduced sub-proof of χ. Then

$$\mathrm{P}(\chi') = \mathrm{P}(\chi)\{\alpha \leftarrow t\}$$

Proof. By duality, it is enough to show $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi)$. Let μ be the position where the reduction is applied, so $\chi = \chi[\varphi]_\mu$ and $\chi' = \chi[\varphi']_\mu$. We will show this only for the universal quantifier, for the existential quantifier the proof is analogous:

Then φ has the form

$$\dfrac{\dfrac{\overset{(\varphi_1, C)}{\Gamma \vdash \Delta, B\{x \leftarrow \alpha\}}}{\Gamma \vdash \Delta, (\forall x)B}\,\wedge\!:\mathrm{l} \qquad \dfrac{\overset{(\varphi_2, D)}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{(\forall x)B, \Pi \vdash \Lambda}\,\wedge\!:\mathrm{l}}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}$$

and φ' has the form

$$\dfrac{\overset{(\varphi_1\{\alpha \leftarrow t\}, C\{\alpha \leftarrow t\})}{\Gamma \vdash \Delta, B\{x \leftarrow t\}} \qquad \overset{(\varphi_2, D)}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}$$

So we have

$$\mathrm{P}^\Omega(\chi).\mu = C \cup D$$

and

$$\mathrm{P}^\Omega(\chi').\mu = C\{\alpha \leftarrow t\} \cup D$$

but α does not occur in D so

$$\mathrm{P}^\Omega(\chi').\mu = (\mathrm{P}^\Omega(\chi).\mu)\{\alpha \leftarrow t\}$$

And as the label sets of the formula occurrences in the sequent at μ do not change we can apply Lemma 4.1. □

The reduction of a weakening rule deletes a sub-proof and - by introducing new weakening rules - makes some formula occurrences further down in the proof weak that have not been weak before. This may have the result that an auxiliary formula of a binary rule, that goes into the end-sequent, becomes weak and thus this binary rule becomes superfluous (because it could be replaced by a weakening). The effect of this transformation on the profile is that of deletion of certain clauses: All clauses from the deleted sub-proof as well as all clauses that share a label with a superfluous binary rule are deleted.

Lemma 5.4 (weakening reduction)**.** Let χ be an **LKps**-proof and μ a position in χ of a cut that can be reduced by $\to_{\mathrm{G_w}}$. Then

$$\chi[\varphi]_\mu \to_{\mathrm{G_w}} \chi[\varphi']_\mu$$

We write χ' for $\chi[\varphi']_\mu$. Let D be the set of axiom labels of the sub-proof deleted by this $\to_{\mathrm{G_w}}$-step. Let furthermore $\sigma_1, \ldots, \sigma_n$ be those binary Σ-rules on the path between μ and the end-sequent of χ that each have an auxiliary occurrence $\alpha_1, \ldots, \alpha_n$ with $\mathcal{L}(\alpha_i) \subseteq D$. Let $\beta_1, \ldots, \beta_n$ be the other auxiliary formula occurrences of these rules and abbreviate $L_i := \mathcal{L}(\beta_i)$. Then

$$\mathrm{P}(\chi') = \mathrm{P}(\chi)^{\neg D \wedge \neg L_1 \wedge \ldots \wedge \neg L_n}$$

Proof. Again by duality it suffices to show $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi)^{\neg D \wedge \neg L_1 \wedge \ldots \wedge \neg L_n}$. Let ν be a formula occurrence in χ but not in φ and let ν' be the corresponding formula occurrence in χ'. Then one can easily show by induction on the length l of the path between μ and the end-sequent of χ that:

$$(\star) \quad \mathcal{L}(\nu') = L(\nu) \setminus D$$

We abbreviate $D^* := \neg D \wedge \neg L_1 \wedge \ldots \wedge \neg L_n$ and show $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi)^{D^*}$ again by induction on the length l of the path between μ and the end-sequent.

If $l = 0$ then $n = 0$. Furthermore, $\mathrm{P}^\Omega(\chi) = X \cup Y$ for sets of labelled clauses X and Y and $\mathrm{P}^\Omega(\chi') = X$. But X contains no labels from D while Y contains only labels from D, so $\mathrm{P}^\Omega(\chi') = X = (X \cup Y)^{\neg D} = \mathrm{P}^\Omega(\chi)^{\neg D}$.

If $l > 0$ we make a case distinction according to the type of the last rule ρ in χ: If ρ is unary then the result follows immediately from the induction hypothesis. If ρ is a binary Ω-rule then $\mathrm{P}^\Omega(\chi) = X \cup Y$ and $\mathrm{P}^\Omega(\chi') = X^{D^*} \cup Y$, but Y contains no labels from D nor any from $L_1, \ldots, L_n$, so $Y = Y^{D^*}$ and thus $\mathrm{P}^\Omega(\chi') = X^{D^*} \cup Y = X^{D^*} \cup Y^{D^*} = (X \cup Y)^{D^*} = \mathrm{P}^\Omega(\chi)^{D^*}$. If ρ is a binary Σ-rule, let α be the auxiliary occurrence on the path between μ and the root. We distinguish two cases:

1. $\mathcal{L}(\alpha) \subseteq D$, i.e. α becomes weak after the reduction, so $\alpha = \alpha_{n+1}$, the other auxiliary occurrence is β_{n+1} and its labels $\mathcal{L}(\beta_{n+1}) = L_{n+1}$. We have $\mathrm{P}^\Omega(\chi) = X \times_{\mathcal{L}(\alpha) \cup L_{n+1}} Y$ and by $(\star)$ and the induction hypothesis that $\mathrm{P}^\Omega(\chi') = X^{D^*} \times_{L_{n+1}} Y$. By algebraic manipulations one shows that $\mathrm{P}^\Omega(\chi') = (X \cup Y)^{D^* \wedge \neg L_{n+1}}$ and $\mathrm{P}^\Omega(\chi)^{D^* \wedge \neg L_{n+1}} = X^{\neg \mathcal{L}(\alpha) \wedge D^* \wedge \neg L_{n+1}} \cup Y^{D^* \wedge \neg L_{n+1}}$. By our case assumption $\mathcal{L}(\alpha) \subseteq D$, so $\neg \mathcal{L}(\alpha) \wedge D^*$ can be simplified to D^* because $\neg D$ is contained in D^* and thus $\mathrm{P}^\Omega(\chi)^{D^* \wedge \neg L_{n+1}} = X^{D^* \wedge \neg L_{n+1}} \cup Y^{D^* \wedge \neg L_{n+1}} = (X \cup Y)^{D^* \wedge \neg L_{n+1}}$.

2. $\mathcal{L}(\alpha) \not\subseteq D$: In this case we have $\mathrm{P}^\Omega(\chi) = X \times_L Y$ for a set of labels L, and by $(\star)$ and the induction hypothesis that $\mathrm{P}^\Omega(\chi') = X^{D^*} \times_{L \setminus D} Y$.

Writing $L \setminus D$ as $L \wedge \neg D$, using algebraic manipulations and simplifying $D^* \wedge L \wedge \neg D$ to $D^* \wedge L$ gives $\mathrm{P}^\Omega(\chi') = (X^L \times Y^L)^{D^*} \cup X^{D^* \wedge \neg(L \wedge \neg D)} \cup Y^{\neg(L \wedge \neg D)}$. By further simplifications one shows that $\mathrm{P}^\Omega(\chi') = (X^L \times Y^L)^{D^*} \cup (X^{\neg L})^{D^*} \cup (Y^{\neg L})^{D^*} = \mathrm{P}^\Omega(\chi)^{D^*}$

□

Corollary 5.1. Let χ be an **LKps**-proof and μ a position in χ of a cut that can be reduced by $\to_{\mathrm{G_w}}$. Let D be the set of axiom labels of the sub-proof deleted by this $\to_{\mathrm{G_w}}$-step. If all formula occurrences in the deleted sub-proof are ancestors of cut formulas then

$$\mathrm{P}(\chi') = \mathrm{P}(\chi)$$

Proof. By applying Lemma 5.4 and observing that in this case there can be no binary Σ-rule with an auxiliary formula α s.t. $\mathcal{L}(\alpha) \subseteq D$, thus $n = 0$ and $\mathrm{P}(\chi') = \mathrm{P}(\chi)^{\neg D}$. But $\mathrm{P}(\chi)^D = \emptyset$ because all axioms with labels from D contain only Ω-formulas, hence the respective clause sets are $\emptyset$. □

Lemma 5.5 (contraction reduction)**.** Let χ be an **LKps**-proof and μ a position in χ of a cut that can be reduced by $\to_{\mathrm{G_c}}$. Then

$$\chi[\varphi]_\mu \to_{\mathrm{G_c}} \chi[\varphi']_\mu$$

Let D be the set of axiom labels of the sub-proof duplicated by this $\to_{\mathrm{G_c}}$-step and let π be the permutation on labels and variables applied to the new copy of the duplicated sub-proof. We write χ' for $\chi[\varphi']_\mu$. Then

$$\mathrm{P}(\chi') = \mathrm{P}(\chi) \cup \mathrm{P}(\chi)^D\pi$$

Proof. By duality it is enough to show $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi) \cup \mathrm{P}^\Omega(\chi)^D\pi$. Let ν be a formula occurrence in χ but not in φ and let ν' be the corresponding formula occurrence in χ'. Then one can show by induction on the length l of the path between μ and the end-sequent of χ that:

$$(\star) \quad \mathcal{L}(\nu') = \mathcal{L}(\nu) \cup (\mathcal{L}(\nu) \cap D)\pi$$

We show $\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi) \cup \mathrm{P}^\Omega(\chi)^D\pi$ again by induction on the length l of the path between μ and the end-sequent. If $l = 0$ then $\mathrm{P}^\Omega(\chi) = X \cup Y$ and $\mathrm{P}^\Omega(\chi') = X \cup X\pi \cup Y$ but as $(X \cup Y)^D = X$ we obtain $\mathrm{P}^\Omega(\chi)^D\pi = X\pi$. If $l > 0$ we make a case distinction according to the type of the last rule ρ: If ρ is a unary rule then the result holds immediately by the induction hypothesis. If ρ is a binary Ω-rule then $\mathrm{P}^\Omega(\chi) = X \cup Y$ and by the induction hypothesis: $\mathrm{P}^\Omega(\chi') = X \cup X^D\pi \cup Y$ but as Y contains no labels from D we have $\mathrm{P}^\Omega(\chi)^D\pi = X^D\pi$.

If ρ is a binary Σ-rule then $\mathrm{P}^\Omega(\chi) = X \times_L Y$ and by the induction hypothesis and $(\star)$: $\mathrm{P}^\Omega(\chi') = (X \cup X^D\pi) \times_{L\cup(L\cap D)\pi} Y$. By observing that neither X nor Y contain any labels from the image of π and that thus for $Z \in \{X, Y\}$ and any label sets M, N: $Z^{M\vee N\pi} = Z^M$ and $Z^{\neg(M\vee N\pi)} = Z^{\neg M}$ one shows that

$$\mathrm{P}^\Omega(\chi') = \mathrm{P}^\Omega(\chi) \cup ((X^D\pi)^{L\vee(L\wedge D)\pi} \times Y^L) \cup (X^D\pi)^{\neg(L\vee(L\wedge D)\pi)}$$

So it remains to show

$$\mathrm{P}^\Omega(\chi)^D\pi = ((X^D\pi)^{L\vee(L\wedge D)\pi} \times Y^L) \cup (X^D\pi)^{\neg(L\vee(L\wedge D)\pi)}$$

As Y cannot contain any labels from D, we have

$$\mathrm{P}^\Omega(\chi)^D\pi = ((X^L \times Y^L)^D \cup X^{\neg L\wedge D})\pi = (X^{L\wedge D}\pi \times Y^L) \cup X^{\neg L\wedge D}\pi$$

By algebraic manipulations concerning the variable and label permutation π one shows the remaining equations:

$$X^{L\wedge D}\pi = (X^D\pi)^{L\vee(L\wedge D)\pi} \text{ and } X^{\neg L\wedge D}\pi = (X^D\pi)^{\neg(L\vee(L\wedge D)\pi)}$$

□

5.2 Simple Transformations

Definition 5.1. Let A and B be formulas. Then any cut-free proof of $A \vdash B$ is called a *transformation* of A to B (generally denoted by $\tau_{A,B}$).

We define the effect of transformations on proofs via cut-elimination. To this aim we define a refinement of $\to_{\mathrm{G}}$ and corresponding normal forms:

Definition 5.2. Let $\tau_{A,B}$ be a transformation, φ be a proof of a sequent $\Gamma \vdash \Delta, A$ and ψ be a proof of a sequent $B, \Pi \vdash \Lambda$. We consider the proofs $T(\varphi, \tau_{A,B})$:

$$\dfrac{\overset{(\varphi)}{\Gamma \vdash \Delta, A} \quad \overset{\tau_{A,B}}{A \vdash B}}{\Gamma \vdash \Delta, B}\ \mathrm{cut}$$

and $T(\tau_{A,B}, \psi)$:

$$\dfrac{\overset{\tau_{A,B}}{A \vdash B} \quad \overset{\psi}{B, \Pi \vdash \Lambda}}{A, \Pi \vdash \Lambda}\ \mathrm{cut}$$

We mark in $T(\varphi, \tau_{A,B})(T(\tau_{A,B}, \psi))$ all ancestors of the final cut and refine $\to_{\mathrm{G}}$ to $\to_{\mathrm{G_t}}$ by the following restrictions:

(1) apply the reduction rules only cuts whose auxiliary formulas are marked.

(2) apply the elimination rules for axioms only if all other $\rightarrow_{\mathrm{G}}$-reduction rules on marked formulas fail.

(3) Eliminate a cut between two (atomic) axioms by eliminating the axiom coming from $\tau_{A,B}$ (i.e. the axiom with the labels coming from $\tau_{A,B}$). In more detail: replace the subproof

$$\frac{B^{\{i\}} \vdash B^{\{i\}} \quad B^{\{j\}} \vdash B^{\{j\}}}{B^{\{i\}} \vdash B^{\{j\}}} \text{ cut}$$

(where i is a label in the φ-part (in the ψ-part) and j is a label in the $\tau_{A,B}$-part) by

$$B^{\{i\}} \vdash B^{\{i\}}.$$

Then by $\tau_{A,B}(\psi)((\varphi)\tau_{A,B})$ we denote the set of all $\rightarrow_{\mathrm{G_t}}$-normal forms of $T(\tau_{A,B}, \psi)$ $(T(\varphi, \tau_{A,B}))$.

Note that Gentzen normal forms of proofs are not unique in general. Therefore the elimination of the cut with the transformation $\tau_{A,B}$ may yield different proofs. So any element from the set $(\varphi)\tau_{A,B}$ can be considered as the transformed proof.

Below we investigate a class of transformations $\tau_{A,B}$ where A is logically equivalent to B:

Definition 5.3. Two formulas A, B are called *V-equivalent* if they contain the same variables.

Definition 5.4. Let τ be a transformation $\tau_{A,B}$ and let A, B be V-equivalent. Moreover let $x_1, \ldots, x_n$ be the bound variables in A (respectively in B). Then τ is called *Q-simple* if

(a) For every variable x_i there are exactly two quantifier introductions in τ.

(b) If $\{x_i \leftarrow \alpha_i\}$ is a substitution corresponding to a strong quantifier introduction on an ancestor of A then $\{x_i \leftarrow \alpha_i\}$ is also a substitution corresponding to a weak quantifier introduction on an ancestor of B.

(c) If $\{x_i \leftarrow \alpha_i\}$ is a substitution corresponding to a strong quantifier introduction on an ancestor of B then $\{x_i \leftarrow \alpha_i\}$ is also a substitution corresponding to a weak quantifier introduction on an ancestor of A.

In a Q-simple transformation the strong substitutions for A are the weak ones for B and vice versa. In particular, all quantifier introductions have variable substitutions.

Example 5.1. The following transformation τ is Q-simple:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(\alpha_1,\alpha_2)\vdash P(\alpha_1,\alpha_2)}{\vdash \neg P(\alpha_1,\alpha_2), P(\alpha_1,\alpha_2)}\,\neg\text{: r}}{\vdash \neg P(\alpha_1,\alpha_2), (\exists y)P(\alpha_1,y)}\,\exists\text{: r}}{\vdash (\forall y)\neg P(\alpha_1,y), (\exists y)P(\alpha_1,y)}\,\wedge\text{: r}}{\vdash (\exists x)(\forall y)\neg P(x,y), (\exists y)P(\alpha_1,y)}\,\exists\text{: r}}{\vdash (\exists x)(\forall y)\neg P(x,y), (\forall x)(\exists y)P(x,y)}\,\wedge\text{: r}}{\neg(\forall x)(\exists y)P(x,y)\vdash (\exists x)(\forall y)\neg P(x,y)}\,\neg\text{: l}$$

No transformation with end-sequent $(\forall x)Q(x)\vdash(\exists x)Q(x)$ is Q-simple.

Definition 5.5. A transformation $\tau_{A,B}$ is called *simple* if it is Q-simple and does not contain structural rules.

Example 5.2. The transformation τ defined in Example 5.1 is simple. Moreover the identical transformation I is simple. I can be defined in the following way:

If A is an atom then $I(A) = A\vdash A$. If A contains logical operators, then $I(A)$ can be defined inductively. We consider the cases $A\equiv B\to C$ and $A\equiv(\forall x)B$, the others are straightforward.

$$I(B\to C) = \dfrac{\dfrac{\dfrac{I(B)}{B\vdash B}\quad\dfrac{I(C)}{C\vdash C}}{B, B\to C\vdash C}\to\text{: l}}{B\to C\vdash B\to C}\to\text{: r}$$

$$I((\forall x)B) = \dfrac{\dfrac{\dfrac{I(B\{x\leftarrow\alpha\})}{B\{x\leftarrow\alpha\}\vdash B\{x\leftarrow\alpha\}}}{(\forall x)B\vdash B\{x\leftarrow\alpha\}}\wedge\text{: l}}{(\forall x)B\vdash(\forall x)B}\wedge\text{: r}$$

Definition 5.6. Two formulas A, B are called strongly equivalent (notation $A\sim_s B$) if there exist simple transformations $\tau_{A,B}$ and $\tau_{B,A}$.

Note that, in contrast to full logical equivalence, it is decidable whether two formulas are strongly equivalent. This is clear as the number of inferences in a simple transformation $\tau_{A,B}$ is bounded by the logical complexity of $A\vdash B$.

Example 5.3. Note that the existence of a simple transformation from A to B does not imply the existence of a simple transformation from B to A. Let $P(x)$ and Q be atom formulas. Then there is a simple transformation from $(\forall x)P(x)\wedge Q$ to $(\forall x)(P(x)\wedge Q)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(\alpha)\vdash P(\alpha)\quad Q\vdash Q}{P(\alpha), Q\vdash P(\alpha)\wedge Q}\,\wedge\text{: r}}{(\forall x)P(x), Q\vdash P(\alpha)\wedge Q}\,\wedge\text{: l}}{(\forall x)P(x)\wedge Q\vdash P(\alpha)\wedge Q}\,\wedge\text{: l}}{(\forall x)P(x)\wedge Q\vdash(\forall x)(P(x)\wedge Q)}\,\wedge\text{: r}$$

But there is no simple transformation from $(\forall x)(P(x)\wedge Q)$ to $(\forall x)P(x)\wedge Q$.

Definition 5.7. A binary relation ∇ on formulas is called *compatible* if, for all formulas A and B, $A \nabla B$ implies $C[A]_\lambda \nabla C[B]_\lambda$ for any formula context $C[\ ]_\lambda$.

Proposition 5.1. $\sim_s$ is a compatible equivalence relation on formulas.

Proof. reflexivity: Define $\tau_{A,A}$ as $I(A)$; $I(A)$ is simple for all A.

symmetry: immediate by definition.

transitivity:
Assume $A \sim_s B$ and $B \sim_s C$. Then there exist simple transformations $\tau_{A,B}$ and $\tau_{B,C}$; we may assume w.l.o.g. that $\tau_{A,B}$ and $\tau_{B,C}$ do not share eigenvariables. By $V(X)$ we denote the set of variables in X.

By definition of $\sim_s$ we have $V(A) = V(B)$, $V(B) = V(C)$ and thus $V(A) = V(C)$. We consider the proof η_{AC}:

$$\dfrac{\overset{\tau_{A,B}}{A \vdash B} \quad \overset{\tau_{B,C}}{B \vdash C}}{A \vdash C}\ \text{cut}$$

As $\tau_{A,B}$ and $\tau_{B,C}$ do not contain weakening and contractions, the same holds for η_{AC} as well. Clearly η_{AC} is not a transformation; but it is enough to show that any cut-elimination sequence Ψ on η_{AC} yields a transformation which is also simple.

Let $\eta_{AC} \to_{\mathrm{G}}^* \xi$. Then, by definition of the reduction rules for $\to_{\mathrm{G}}$, ξ does not contain weakenings and/or contractions (indeed no additional weakenings and contractions are introduced by the cut-reduction rules). So let Ψ be a cut-elimination sequence on η_{AC}; then its result is a transformation $\tau_{A,C}$ which is weakening- and contraction-free. It remains to show that $\tau_{A,C}$ is also Q-simple.

Let us assume that $X\colon\ \{x_1, \ldots, x_n\}$ are the bound variables in A, B, C. As $\tau_{A,B}$ is simple, X can be partitioned into two sets

$$\{y_1, \ldots, y_m\} \quad \{z_1, \ldots, z_k\}$$

s.t. the y_i are the strong variables of quantifier introductions on ancestors of A, and the z_j are the weak variables of quantifier introductions on ancestors of A. Moreover, as $\tau_{A,B}$ is Q-simple, the y_i are the weak variables of quantifier introductions on ancestors of B, and the z_j are the strong variables of quantifier introductions on ancestors of B. Now let us list the vectors of variables in the following order:

(1) strong, ancestor of A, (2) weak, ancestor of A,
(3) strong, ancestor of B, (4) weak, ancestor of B.

This way we obtain a tuple

$$X_{AB}\colon\quad < (y_1, \ldots, y_m), (z_1, \ldots, z_k), (z_1, \ldots, z_k), (y_1, \ldots, y_m) > .$$

Now consider the tuple X_{AB} under substitution of the bound variables by the quantifier substitutions. Then we obtain the *quantifier-introduction vector* for $\tau_{A,B}$:

$$Y_{AB}: \quad <(\alpha_1,\ldots,\alpha_m),(\beta_1,\ldots,\beta_k),(\beta_1,\ldots,\beta_k),(\alpha_1,\ldots,\alpha_m)> .$$

For $\tau_{B,C}$ we obtain (replacing A by B, B by C in the tuple notation)

$$X_{BC}: \quad <(y_1,\ldots,y_m),(z_1,\ldots,z_k),(z_1,\ldots,z_k),(y_1,\ldots,y_m)> .$$

and the quantifier introduction vector

$$Y_{BC}: \quad <(\beta'_1,\ldots,\beta'_m),(\gamma_1,\ldots,\gamma_k),(\gamma_1,\ldots,\gamma_k),(\beta'_1,\ldots,\beta'_m)> .$$

Note that η_{AC} is regular and so the β'_i are different from the β_j.

Now let Ψ be a cut-elimination sequence on η_{AC}. According to the cut-reduction rules for quantifiers, strong variables are replaced by weak terms. As the proofs in Ψ do not contain weakenings and contractions, Ψ contains *exactly* $m+k$ $(=n)$ quantifier-elimination steps. Therefore these steps can be characterized by the single substitution

$$\{\beta'_1 \leftarrow \alpha_1,\ldots,\beta'_m \leftarrow \alpha_m,\ \beta_1 \leftarrow \gamma_1,\ldots,\beta_k \leftarrow \gamma_k\}.$$

Hence the quantifier introduction vector for the result $\tau_{A,C}$ of Ψ is

$$Y_{AC}: \quad <(\alpha_1,\ldots,\alpha_m),(\gamma_1,\ldots,\gamma_k),(\gamma_1,\ldots,\gamma_k),(\alpha_1,\ldots,\alpha_m)> .$$

But this quantifier introduction vector is that of a Q-simple transformation. Therefore $\tau_{A,C}$ is simple.

It remains to show that $\sim_s$ is compatible.

We proceed by induction on the logical complexity of the context. The case of the empty context is trivial.

The induction hypothesis is $C[A]_\lambda \sim_s C[B]_\lambda$ whenever $A \sim_s B$, for any C of complexity $\leq n$ and any position λ in C.

Now let C be of complexity $n+1$. Then C is of one of the following forms

$$(a)\ C \equiv C_1 \wedge C_2, \quad (b)\ C \equiv C_1 \vee C_2, \quad (c)\ C \equiv C_1 \to C_2,$$
$$(d)\ C \equiv \neg C', \qquad (e)\ C \equiv (\forall x)C', \quad (f)\ C \equiv (\exists x)C'.$$

We only show the cases c,d,e, the others are analogous.

(c) We consider the formulas $(C_1 \to C_2)[A]_\mu$ and $(C_1 \to C_2)[B]_\mu$. There are two possibilities:

(c1) μ is an occurrence in C_1, and
(c2) μ is an occurrence in C_2.

(c1) There exists a position λ in C_1 (corresponding to μ in C) s.t.

$$C[A]_\mu = C_1[A]_\lambda \to C_2,\ C[B]_\mu = C_1[B]_\lambda \to C_2.$$

We define a transformation τ transforming $C_1[A]_\lambda \to C_2$ into $C_1[B]_\lambda \to C_2$ (the other direction can be obtained by exchanging A and B).

$$\dfrac{\dfrac{\overset{\tau'}{C_1[B]_\lambda \vdash C_1[A]_\lambda} \quad \overset{I(C_2)}{C_2 \vdash C_2}}{C_1[B]_\lambda, C_1[A]_\lambda \to C_2 \vdash C_2} \to : \mathrm{l}}{C_1[A]_\lambda \to C_2 \vdash C_1[B]_\lambda \to C_2} \to : \mathrm{r}$$

By the induction hypothesis a simple τ' exists, and $I(C_2)$ is simple; obviously τ itself is simple.

(c2) symmetric to (c1).

(d) We have to show $(\neg C')[A]_\mu \sim_s (\neg C')[B]_\mu$. Again there exists a position λ in C' with $\neg C'[A]_\lambda = (\neg C')[A]_\mu$ (the same for B). The desired transformation τ is

$$\dfrac{\dfrac{\overset{\tau'}{C'[B]_\lambda \vdash C'[A]_\lambda}}{\neg C'[A]_\lambda, C'[B]_\lambda \vdash} \neg : \mathrm{l}}{\neg C'[A]_\lambda \vdash \neg C'[B]_\lambda} \neg : \mathrm{r}$$

By the induction hypothesis such a simple transformation τ' exists. Clearly τ is also simple. The transformation from $\neg C'[B]_\lambda$ into $\neg C'[A]_\lambda$ can be obtained by exchanging A and B.

(e) We have to prove $((\forall x)C')[A]_\mu \sim_s ((\forall x)C')[B]_\mu$. Again there must be a position λ s.t. $((\forall x)C')[A]_\mu = (\forall x)C'[A]_\lambda$ (the same for B). We define τ as

$$\dfrac{\dfrac{\overset{\tau'}{C'[A]_\lambda\{x \leftarrow \alpha\} \vdash C'[B]_\lambda\{x \leftarrow \alpha\}}}{(\forall x)C'[A]_\lambda \vdash C'[B]_\lambda\{x \leftarrow \alpha\}} \wedge : \mathrm{l}}{(\forall x)C'[A]_\lambda \vdash (\forall x)C'[B]_\lambda} \wedge : \mathrm{r}$$

A simple transformation τ' exists by induction hypothesis.
Let $A' = A\{x \leftarrow \alpha\},\ B' = B\{x \leftarrow \alpha\}$. Then

$$C'\{x \leftarrow \alpha\}[A']_\lambda = C'[A]_\lambda\{x \leftarrow \alpha\},\ C'\{x \leftarrow \alpha\}[B']_\lambda = C'[B]_\lambda\{x \leftarrow \alpha\}.$$

Clearly the complexity of $C'\{x \leftarrow \alpha\}$ is that of C' itself. It remains to show that $A' \sim_s B'$: consider a simple transformation $\tau_{A,B}$. Either x is a free variable in A and B or it does not occur in both of them. As α is a variable not occurring in A and B, the transformation $\tau_{A,B}\{x \leftarrow \alpha\}$ is also simple. Therefore the transformation τ above is simple as well.

□

Example 5.4. $\neg(\forall x)(\exists y)P(x,y) \sim_s (\exists x)(\forall y)\neg P(x,y)$:

we have shown in Example 5.1 that there exists a simple transformation of $\neg(\forall x)(\exists y)P(x,y)$ to $(\exists x)(\forall y)\neg P(x,y)$. It is easy to construct a simple transformation of $(\exists x)(\forall y)\neg P(x,y)$ to $\neg(\forall x)(\exists y)P(x,y)$.

We give an example of logically equivalent formulas which are not strongly equivalent:

$$(\forall x)P(x) \to Q(a) \not\sim_s (\exists x)(P(x) \to Q(a)).$$

Indeed, all transformations of $(\forall x)P(x) \to Q(a)$ to $(\exists x)(P(x) \to Q(a))$ require the use of contractions and thus are not simple. In fact, the quantifier $(\forall x)$ in

$$S\colon\ (\forall x)P(x) \to Q(a) \vdash (\exists x)(P(x) \to Q(a)).$$

is strong in S and thus (going from the end-sequent to the axioms) must be eliminated prior to $(\exists x)$ (which is weak in S). We see that, in general, the quantifier shifting principles go beyond strong equivalence.

Definition 5.8. A formula A is in *negation normal form* (NNF) if it does not contain $\to$ and $\neg$ occurs only immediately above atoms (i.e. for any subformula $\neg C$ of A, C is an atom).

Lemma 5.6. A formula is in negation normal from iff it is a normal form under the rewrite rules $\mathcal{R}$ (applied to arbitrary occurrences of subformulas):

(1) $\neg\neg A \Rightarrow A$, (2) $\neg(A \wedge B) \Rightarrow \neg A \vee \neg B$, (3) $\neg(A \vee B) \Rightarrow \neg A \wedge \neg B$,

(4) $A \to B \Rightarrow \neg A \vee B$, (5) $\neg(\forall x)A \Rightarrow (\exists x)\neg A$, (6) $\neg(\exists x)A \Rightarrow (\forall x)\neg A$.

Moreover all formulas A can be transformed to a NNF B via $\mathcal{R}$ (we say that B is the NNF of A).

Proof. In [2], proposition 4.6. □

Proposition 5.2. A formula A is strongly equivalent to its negation normal form.

Proof. It is enough to show that, for the rewrite rules defined in Lemma 5.6, the left and right sides are strongly equivalent. Then the result follows from Lemma 5.6 and the fact that $\sim_s$ is compatible and transitive (Proposition 5.1).

We give the simple transformations corresponding to the rules in $\mathcal{R}$:

(1) $\neg\neg A \sim_s A$:

$$\dfrac{\dfrac{\dfrac{I(A)}{A \vdash A}}{\vdash A, \neg A}\ \neg\colon \mathrm{r}}{\neg\neg A \vdash A}\ \neg\colon \mathrm{l} \qquad \dfrac{\dfrac{\dfrac{I(A)}{A \vdash A}}{\neg A, A \vdash}\ \neg\colon \mathrm{l}}{A \vdash \neg\neg A}\ \neg\colon \mathrm{r}$$

(2) $\neg(A \wedge B) \sim_s \neg A \vee \neg B$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{I(A) \quad I(B)}{A \vdash A \quad B \vdash B}}{A, B \vdash A \wedge B}\wedge\text{: r}}{A, B, \neg(A \wedge B) \vdash}\neg\text{: l}}{A, \neg(A \wedge B) \vdash \neg B}\neg\text{: r}}{\neg(A \wedge B) \vdash \neg A, \neg B}\neg\text{: r}}{\neg(A \wedge B) \vdash \neg A \vee \neg B}\vee\text{: r}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{I(A)}{A \vdash A}}{A, \neg A \vdash}\neg\text{: l} \quad \dfrac{I(B)}{B \vdash B}}{A, B, \neg A \vee \neg B \vdash}\neg\text{: l}}{A \wedge B, \neg A \vee \neg B \vdash}\vee\text{: l}}{\neg A \vee \neg B \vdash \neg(A \wedge B)}\wedge\text{: l}}{}\neg\text{: r}$$

(3) $\neg(A \vee B) \sim_s \neg A \wedge \neg B$: symmetric to (2).

(4) $A \to B \sim_s \neg A \vee B$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{I(A) \quad I(B)}{A \vdash A \quad B \vdash B}}{A, A \to B \vdash B}\to\text{: l}}{A \to B \vdash \neg A, B}\neg\text{: r}}{A \to B \vdash \neg A \vee B}\vee\text{: r}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{I(A)}{A \vdash A}}{A, \neg A \vdash}\neg\text{: l} \quad I(B)}{A, \neg A \vee B \vdash B}\vee\text{: l}}{\neg A \vee B \vdash A \to B}\to\text{: r}$$

(5) $\neg(\forall x)A \sim_s (\exists x)\neg A$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{I(A\{x \leftarrow \alpha\})}{A\{x \leftarrow \alpha\} \vdash A\{x \leftarrow \alpha\}}}{\vdash \neg A\{x \leftarrow \alpha\}, A\{x \leftarrow \alpha\}}\neg\text{: r}}{\vdash (\exists x)\neg A, A\{x \leftarrow \alpha\}}\exists\text{: r}}{\vdash (\exists x)\neg A, (\forall x)A}\wedge\text{: r}}{\neg(\forall x)A \vdash (\exists x)\neg A}\neg\text{: l}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{I(A\{x \leftarrow \alpha\})}{A\{x \leftarrow \alpha\} \vdash A\{x \leftarrow \alpha\}}}{A\{x \leftarrow \alpha\}, \neg A\{x \leftarrow \alpha\} \vdash}\neg\text{: l}}{(\forall x)A, \neg A\{x \leftarrow \alpha\} \vdash}\wedge\text{: l}}{(\forall x)A, (\exists x)\neg A \vdash}\exists\text{: l}}{(\exists x)\neg A \vdash \neg(\forall x)A}\neg\text{: r}$$

(6) $\neg(\exists x)A \sim_s (\forall x)\neg A$: symmetric to (5).

□

5.2.1 Invariance under Simple Transformations

In this section we will show that the application of simple transformations to ancestors of cut-formulas does not modify the profile. The following lemma is the technical key to the main result. It shows that simple transformations applied to ancestors of cuts do not change the proof profile modulo variable renaming. In particular, this holds for the transformation to negation normal form.

Lemma 5.7. Let φ' be a subproof of an **LKps**-proof φ s.t. φ' is an **LK**-proof of a sequent $\Gamma \vdash \Delta, A$ at node ν, and A is an ancestor of a pseudo-cut. Let $\tau_{A,B}$ be a simple transformation. Then, for any proof ψ in $(\varphi')\tau_{A,B}$, $\mathrm{P}(\varphi[\psi]_\nu) = \mathrm{P}(\varphi)\pi$, where π is a permutation of eigenvariables.

Remark 5.1. Note that, in general, $\varphi[\psi]_\nu$ is a pseudo-proof, even if φ is a proof, as the substitution of ψ for φ' may violate cut- and contraction rules. But note that φ' must be an **LK**-proof!

Proof. We will treat only P^Ω, the result for P^Σ follows from duality. We proceed by cut-elimination on the proof $T(\varphi', \tau_{A,B})$:

$$\dfrac{\begin{matrix}(\varphi') & (\tau_{A,B})\\ \Gamma \vdash \Delta, A & A \vdash B\end{matrix}}{\Gamma \vdash \Delta, B}\ \mathrm{cut}$$

As in $\tau_{A,B}$ each axiom contains only ancestors of cuts in φ, $\mathrm{P}^\Omega(\varphi).\nu_r = \emptyset$ where ν_r is the position of the last rule of $\tau_{A,B}$ and thus $\mathrm{P}^\Omega(\varphi).\nu = \mathrm{P}^\Omega(\varphi).\nu_l$ where ν_l is the position of the last rule of φ'. Let $L := \mathcal{L}(\tau_{A,B})$. Then $\mathrm{P}^\Omega(\varphi)^L = \emptyset$ because all axioms of $\tau_{A,B}$ contain only cut-ancestors.

We apply cut-elimination based on $\to_{\mathrm{G_t}}$ in two phases (as defined in Definition 5.2): in the first step we eliminate all marked cuts without applying the elimination rule for axioms. In a second step we eliminate the atomic cuts between axioms.

In every phase of cut-elimination by $\to_{\mathrm{G_t}}$ we distinguish a φ'-part (i.e. the part labelled by the original label set of φ) and a $\tau_{A,B}$-part. Indeed, every cut appearing in a proof χ obtained by cut-elimination is of the form ξ:

$$\dfrac{\begin{matrix}(\rho) & (\sigma)\\ \Pi \vdash \Lambda, C & C, \Pi' \vdash \Lambda'\end{matrix}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{cut}$$

where ρ is an (possibly instantiated) subproof of φ', and σ one of $\tau_{A,B}$. For simplicity we assume that the φ'-part is to the left and the $\tau_{A,B}$-part to the right (in fact the sides may change by elimination on negated formulas).

We prove that for all χ with $T(\varphi', \tau_{A,B}) \to^*_{\mathrm{G_t}} \chi$,we have

$$(\star) \quad \mathrm{P}^\Omega(\varphi[\chi]_\nu).\nu = \mathrm{P}^\Omega(\varphi)\pi,$$

where π is a permutation of eigenvariables.

We know by Lemmas 5.1 and 5.2 that $\to_{\mathrm{G_r}}$ and $\to_{\mathrm{G_p}}$ do not change the profile, so we may assume that the cut in ξ is introduced (1) by weakening, or (2) by contraction, or (3) by quantifier introductions on both sides. Let us furthermore assume inductively that $(\star)$ holds for χ, we show that it also holds for χ', the reduct of χ.

(1) ξ is of the form

$$\dfrac{\dfrac{(\rho')}{\Pi \vdash \Lambda}}{\Pi \vdash \Lambda, C}\ \mathrm{w:r} \qquad \dfrac{\begin{matrix}(\sigma)\\ C, \Pi' \vdash \Lambda'\end{matrix}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{cut}$$

Indeed, weakening can only appear in the φ'-part, not in the $\tau_{A,B}$-part (as $\tau_{A,B}$ is simple). According to the rules of $\rightarrow_{\mathrm{G_t}}$, ξ reduces to ξ' for $\xi' =$

$$\dfrac{\dfrac{(\rho')}{\Pi \vdash \Lambda}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{w}:*$$

From now on (for the remaining part of the proof) let us assume that the root node of ξ is μ and $\chi' = \chi[\xi']_\mu$. Then, as Π' and Λ' contain only ancestors of cuts, we may apply Corollary 5.1 and obtain

$$\mathrm{P}^\Omega(\varphi[\chi']_\nu) = \mathrm{P}^\Omega(\varphi[\chi]_\nu)$$

(2) contraction: as in (1) contractions can only occur in the φ'-part, not in the $\tau_{A,B}$-part. So ξ is of the form

$$\dfrac{\dfrac{\dfrac{(\rho')}{\Pi \vdash \Lambda, C, C}}{\Pi \vdash \Lambda, C}\ \mathrm{c}:\mathrm{r} \qquad \dfrac{(\sigma)}{C, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{cut}$$

Then $\xi \rightarrow_{\mathrm{G_t}} \xi'$ for $\xi' =$

$$\dfrac{\dfrac{\dfrac{(\rho')}{\Pi \vdash \Lambda, C, C} \quad \dfrac{(\sigma)}{C, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda', C}\ \mathrm{cut} \qquad \dfrac{(\sigma')}{C, \Pi' \vdash \Lambda'}}{\dfrac{\Pi, \Pi', \Pi' \vdash \Lambda, \Lambda', \Lambda'}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{c}:*}\ \mathrm{cut}$$

where σ' is σ after renaming of eigenvariables and labels. Again, let $\chi' = \chi[\xi']_\mu$. Then, by Lemma 5.5,

$$\mathrm{P}^\Omega(\varphi[\chi']_\nu) = \mathrm{P}^\Omega(\varphi[\chi]_\nu) \cup \mathrm{P}^\Omega(\varphi[\chi]_\nu)^D\pi$$

but $D \subseteq L$ and – as $\mathrm{P}^\Omega(\varphi)^L = \emptyset$ – we have

$$\mathrm{P}^\Omega(\varphi[\chi']_\nu) = \mathrm{P}^\Omega(\varphi[\chi]_\nu)$$

(3) Elimination of a quantifier:

(3a) $\xi =$

$$\dfrac{\dfrac{\dfrac{(\rho')}{\Pi \vdash \Lambda, A\{x \leftarrow t\}}}{\Pi \vdash \Lambda, (\exists x)A}\ \exists\mathrm{:}\,\mathrm{r} \qquad \dfrac{\dfrac{(\sigma')}{A\{x \leftarrow \alpha\}, \Pi' \vdash \Lambda'}}{(\exists x)A, \Pi' \vdash \Lambda'}\ \exists\mathrm{:}\,\mathrm{l}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{cut}$$

Then $\xi \to_{\mathrm{G_t}} \xi'$ for $\xi' =$

$$\dfrac{\begin{array}{cc}(\rho') & (\sigma'\{\alpha \leftarrow t\}) \\ \Pi \vdash \Lambda, A\{x \leftarrow t\} & A\{x \leftarrow t\}, \Pi' \vdash \Lambda'\end{array}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{cut}$$

Then, by Lemma 5.3,

$$\mathrm{P}^{\Omega}(\varphi[\chi']_{\nu}) = \mathrm{P}^{\Omega}(\varphi[\chi]_{\nu})\pi\{\alpha \leftarrow t\}.$$

but α does not occur in $\mathrm{P}^{\Omega}(\varphi[\chi]_{\nu})\pi$ so

$$\mathrm{P}^{\Omega}(\varphi[\chi']_{\nu}) = \mathrm{P}^{\Omega}(\varphi[\chi]_{\nu})\pi$$

(3b) $\xi =$

$$\dfrac{\dfrac{\begin{array}{c}(\rho') \\ \Pi \vdash \Lambda, A\{x \leftarrow \alpha\}\end{array}}{\Pi \vdash \Lambda, (\forall x)A}\ \forall\colon \mathrm{r} \quad \dfrac{\begin{array}{c}(\sigma') \\ A\{x \leftarrow \beta\}, \Pi' \vdash \Lambda'\end{array}}{(\forall x)A, \Pi' \vdash \Lambda'}\ \forall\colon \mathrm{l}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{cut}$$

As σ' is a $\tau_{A,B}$-part, the quantifier substitution for $\forall : l$ is of the form $\{x \leftarrow \beta\}$ where β is an eigenvariable in the proof $\varphi[\xi]_{\nu}$. Note that no substitution of an eigenvariable in the $\tau_{A,B}$-part (see case (3a)) can change the weak quantifier substitutions in this part, because $\tau_{A,B}$ is simple. Now $\xi \to_{\mathrm{G_t}} \xi'$ for $\xi' =$

$$\dfrac{\begin{array}{cc}(\rho'\{\alpha \leftarrow \beta\}) & (\sigma') \\ \Pi \vdash \Lambda, A\{x \leftarrow \beta\} & A\{x \leftarrow \beta\}, \Pi' \vdash \Lambda'\end{array}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ \mathrm{cut}$$

Again, by Lemma 5.3, we obtain

$$\mathrm{P}^{\Omega}(\varphi[\chi']_{\nu}) = \mathrm{P}^{\Omega}(\varphi[\chi]_{\nu})\pi\{\alpha \leftarrow \beta\}.$$

We know that β is a variable. But β cannot occur in $\mathrm{P}^{\Omega}(\varphi[\chi]_{\nu})\pi$ (i.e. in the φ'-part of the proof) as β is an eigenvariable in the $\tau_{A,B}$-part and the proof χ is regular. So we obtain $\pi\{\alpha \leftarrow \beta\}$ as new permutation of eigenvariables.

We have seen that in all cases (1), (2), (3) the property $(\star)$ is preserved. Thus it holds after the first phase of cut-elimination, before the axioms are eliminated. It remains to investigate the elimination of the axioms. Let χ^* be the normal form of $T(\varphi', \tau_{A,B})$ under the first phase of cut-elimination. Then

$$\mathrm{P}^{\Omega}(\varphi[\chi^*]_{\nu}) = \mathrm{P}^{\Omega}(\varphi)\pi$$

where π is a permutation. Now the only cuts left in χ^* are of the form $\xi =$

$$\frac{B^{\{i\}} \vdash B^{\{i\}} \quad B^{\{j\}} \vdash B^{\{j\}}}{B^{\{i\}} \vdash B^{\{j\}}} \text{ cut}$$

Where i is a label in the φ'-part and j is a label in the $\tau_{A,B}$-part. Let μ, μ_l, μ_r be the positions of the cut and of the axioms above it on the left and right side. Then $\mathrm{P}^{\Omega}(\varphi).\mu_r = \emptyset$ because both atoms in $B^{\{j\}} \vdash B^{\{j\}}$ are cut-ancestors and $\mathrm{P}^{\Omega}(\varphi[\chi^*]_\nu).\mu = \mathrm{P}^{\Omega}(\varphi[\chi^*]_\nu).\mu_l$ According to the definition of $\rightarrow_{\mathrm{G_t}}$ (Definition 5.2), ξ is replaced by $\xi' =$

$$B^{\{i\}} \vdash B^{\{i\}}.$$

Let $\chi' = \chi^*[\xi']_\mu$. Then

$$\mathrm{P}^{\Omega}(\varphi[\chi']_\nu).\mu = \mathrm{P}^{\Omega}(\varphi[\chi^*]_\nu).\mu$$

and all labels occurring in this clause set are the same for the formula occurrences in the sequent at μ so by Lemma 4.1 we have

$$\mathrm{P}^{\Omega}(\varphi[\chi']_\nu) = \mathrm{P}^{\Omega}(\varphi)\pi$$

This procedure is repeated until all marked cuts are eliminated. Let us call the resulting proof ψ, which does not contain any marked cuts. Then

$$\mathrm{P}(\varphi[\psi]_\nu) = \mathrm{P}^{\Omega}(\varphi)\pi.$$

. □

Corollary 5.2. Let φ' be a subproof of an **LKps**-proof φ s.t. φ' is a proof of a sequent $B, \Gamma \vdash \Delta$ at node ν, and B is an ancestor of a pseudo-cut. Let $\tau_{A,B}$ be a simple transformation. Then, for any proof ψ in $\tau_{A,B}(\varphi')$, $\mathrm{P}(\varphi[\psi]_\nu) = \mathrm{P}(\varphi)\pi$, where π is a permutation of eigenvariables.

Proof. completely symmetric to the proof of Lemma 5.7. □

Lemma 5.8. Let φ be an **LK**-proof and σ be a subproof of φ (at node ν) of the form

$$\frac{\begin{matrix}(\sigma_1) \\ \Gamma \vdash \Delta, A\end{matrix} \quad \begin{matrix}(\sigma_2) \\ A, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda} \text{ cut}$$

and let A be strongly equivalent to B. Then there exists an **LK**-proof ψ of the form

$$\frac{\begin{matrix}(\psi_1) \\ \Gamma \vdash \Delta, B\end{matrix} \quad \begin{matrix}(\psi_2) \\ B, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda} \text{ cut}$$

and a permutation of eigenvariables π s.t. $\varphi[\psi]_\nu$ is an **LK**-proof and $\mathrm{P}(\varphi[\psi]_\nu) = \mathrm{P}(\varphi)\pi$.

Proof. Apply Lemma 5.7 to the subproof σ_1 with the transformation $\tau_{A,B}$. The result is a pseudo-proof $\varphi_1 = \varphi[\rho]_\nu$ with $\mathrm{P}(\varphi_1) = \mathrm{P}(\varphi)\pi_1$ for a permutation π_1 and for $\rho =$

$$\dfrac{\begin{array}{cc}(\psi_1) & (\sigma_2)\\ \Gamma \vdash \Delta, B & A, \Pi \vdash \Lambda\end{array}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{pscut}$$

Then apply Corollary 5.2 to σ_2 (within φ_1) and obtain a pseudo-proof φ_2, for $\varphi_2 = \varphi_1[\psi]_\nu$, with $\mathrm{P}(\varphi_2) = \mathrm{P}(\varphi_1)\pi_2$ for a permutation π_2 and for $\psi =$

$$\dfrac{\begin{array}{cc}(\psi_1) & (\psi_2)\\ \Gamma \vdash \Delta, B & B, \Pi \vdash \Lambda\end{array}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

Then

$$\mathrm{P}(\varphi_2) = \mathrm{P}(\varphi[\psi]_\nu) = \mathrm{P}(\varphi)\pi_1\pi_2.$$

Clearly $\pi_1\pi_2$ is a variable permutation. Moreover φ_2 is not only a pseudo-proof but also a proof (note that ψ is a proof and has the same end-sequent as σ). □

The following theorem shows that we can transform the cuts in an **LK**-proof into arbitrary strongly equivalent form without changing the proof profile (indeed, variants that differ only by variable permutations can be considered as equal). All these forms can thus be considered as equivalent w.r.t. cut-elimination.

Theorem 5.1. Let φ be an **LK**-proof with cut formulas $A_1, \ldots, A_n$ and $B_1 \sim_s A_1, \ldots, B_n \sim_s A_n$. Then there exists a proof ψ with cut formulas $B_1, \ldots, B_n$ and $\mathrm{P}(\psi) = \mathrm{P}(\varphi)\pi$ for a variable permutation π.

Proof. We iterate the construction defined in Lemma 5.8, by transforming the cuts with $A_1, \ldots, A_n$ successively into cuts with $B_1, \ldots, B_n$. This way we obtain a proof ψ and permutations $\pi_1, \ldots, \pi_n$ with

$$\mathrm{P}(\psi) = \mathrm{P}(\varphi)\pi_1 \ldots \pi_n.$$

But $\pi_1 \ldots \pi_n$ is also a permutation. □

Corollary 5.3. Let φ be a proof with cut formulas $A_1, \ldots, A_n$. Then there exists a proof ψ with cut formulas $B_1, \ldots, B_n$, where the B_i are the negation normal forms of the A_i and $\mathrm{P}(\psi) = \mathrm{P}(\varphi)\pi$ for a permutation π.

Proof. By Proposition 5.2 and Theorem 5.1. □

Corollary 5.3 does not hold for prenex normal from in place of NNF. This is based on the fact, that quantifier shifting does not preserve strong equivalence in general (see Example 5.4); so Theorem 5.1 is not applicable in case of prenex normal forms. Moreover, a proof transformation to prenex form, under preservation of cut-homomorphism, is impossible in principle (see [7]).

In Section 4.1 we have shown that profiles define equivalence classes of proofs at least as large as proof nets. Theorem 5.1 proves that the equivalence classes defined by profiles are in fact larger, due to the strong abstraction from the syntax of cuts.

Note that the invariance results from this section even hold for $\mathrm{P}^{\Omega\mathrm{T}}$, see [31] for details.

5.2.2 Discussion

We have shown that proofs with strongly equivalent cut-formulas (obtained via simple transformations) have the same profile (under variable renaming) and thus can be considered as equal w.r.t. cut-elimination. We defined profiles as sets of *labelled* clauses, i.e. two clauses that differ only in their labels are treated as two different clauses. If profiles are defined as sets of clauses (dropping the labels after generation of the profile), the class of equivalent proofs becomes even larger while still having the same set of normal forms of the CERES method. Then, however, cut-elimination on propositional proofs would not increase the profile (it can only shrink by weakening), and thus would not express the duplication of subproofs.

In [20] Danos, Joinet and Schellinx give an elegant formulation of a class of confluent and strongly terminating cut-elimination procedures for classical logic. In [21] they build on this work to show that the normal forms are not changed after application of transformations called computational isomorphisms. The work in this chapter is similar to [21] in its conceptual aims: to isolate a class of transformations that have no effect on the cut-elimination of a proof. However, the frameworks in which these analyses are carried out are very different: [21] builds on the confluence (and termination) result established in [20] to show that *the normal form* is preserved. In this paper, we isolate a *structural invariant*, the proof profile whose preservation induces the equality of the *set of normal forms* of the cut-elimination method CERES. The former can be considered a restriction, the latter an extension of Gentzen's original cut-elimination procedure. In contrast to [21] however, we have to restrict the application of our transformations to the parts of a proof that go into cuts. We conjecture that our result also holds without this restriction (it is easy to show that it holds for transformations to negation normal form), but it is much harder to prove: indeed, if we apply a transformation to a formula which goes to the end-sequent, the original formula

changes its status (as it now goes to the cut with the transformation), and the whole profile changes in a more complicated way.

Chapter 6

Analysis of Proofs

In this chapter we will show how the system CERES[1] can be used for the comparison and analysis of mathematical proofs. We will investigate different proofs of a single proposition. We start with two different proofs, each of them containing mathematically meaningful cuts. We will show that the characteristic clause sets of these proofs already contain the key steps of the mathematical argument. By applying the CERES-method to these two proofs we will obtain cut-free proofs which contain different combinatorial arguments. We will not use the characteristic clause sets directly but instead apply the pruning operations of tautology-deletion and subsumption before. This makes the clause sets easier to read but does not change their logical meaning. In the cases under investigation, the pruned profile would be the same as the pruned characteristic clause sets.

In addition to the rules of the calculus **LK** the following rules for the handling of equality will appear in the examples in this chapter.

$$\frac{\Gamma_1 \vdash \Delta_1, s = t \quad A[s]_\Lambda, \Gamma_2 \vdash \Delta_2}{A[t]_\Lambda, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} = : \mathrm{l1} \qquad \frac{\Gamma_1 \vdash \Delta_1, t = s \quad A[s]_\Lambda, \Gamma_2 \vdash \Delta_2}{A[t]_\Lambda, \Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2} =: l2$$

$$\frac{\Gamma_1 \vdash \Delta_1, s = t \quad \Gamma_2 \vdash \Delta_2, A[s]_\Lambda}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A[t]_\Lambda} = : \mathrm{r1} \qquad \frac{\Gamma_1 \vdash \Delta_1, t = s \quad \Gamma_2 \vdash \Delta_2, A[s]_\Lambda}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, A[t]_\Lambda} = : \mathrm{r2}$$

where Λ is a set of positions and $A[s]_\Lambda$ denotes the formula A with the term s at all positions in Λ. The CERES-method can be extended to this calculus in a very straightforward way, see [4].

The statement we will analyze is the following proposition:

Definition 6.1. An *infinite tape* is a function $f : \mathbb{N} \to \mathbb{N}$

Proposition 6.1. Let f be an infinite tape where every cell is labelled by either 0 or 1. Then on f there exist two different cells with the same value.

[1] http://www.logic.at/ceres/

Clearly this theorem is true and altough it is mathematically simple it is substantial enough to allow different proofs, thus making it a good candidate for this kind of analysis.

6.1 The Infinity Argument

The proof below is taken from [50]; it was formalized in **LK** and analyzed by a former version of the system `CERES` in [3] and modified to a formalization in **LKDe**, a sequent calculus extended by definitions and equality in [4].

Proof. **First Proof of Proposition 6.1 (Infinity Argument):** If f is an infinite tape where every cell is labelled by either 0 or 1 then clearly there must be infinitely many 0s or infinitely many 1s.

1. If there are infinitely many 0s choose two of them to obtain two different cells with the same value.
2. If there are infinitely many 1s – again – choose two of them to obtain two different cells with the same value.

□

The formalization φ_1 of this proof has the following shape:

$$\dfrac{\dfrac{\dfrac{(\tau)}{T \vdash I_0, I_1} \quad \dfrac{(\epsilon_0)}{I_0 \vdash P}}{T \vdash P, I_1}\,\text{cut} \quad \dfrac{(\epsilon_1)}{I_1 \vdash P}}{T \vdash P}\,\text{cut}$$

where

$$\begin{aligned} T &\equiv (\forall x)(f(x) = 0 \vee f(x) = 1), \\ P &\equiv (\exists p)(\exists q)(p \neq q \wedge f(p) = f(q)), \\ I_0 &\equiv (\forall x)(\exists y) f(x + y) = 0, \\ I_1 &\equiv (\forall x)(\exists y) f(x + y) = 1. \end{aligned}$$

The axioms used for the proof are the standard axioms of type $A \vdash A$ and instances of $\vdash x = x$, of commutativity $\vdash x + y = y + x$, of associativity $\vdash (x + y) + z = x + (y + z)$, and of the axiom

$$x = x + (1 + y) \vdash,$$

expressing that $x + (1 + y) \neq x$ for all natural numbers x, y.

The characteristic clause set of φ_1 is (after variable renaming)

$$\begin{array}{lll} \mathrm{CL}(\varphi_1) = \{ & (C_1) & \vdash f(x+y)=0, f(y+x)=1; \\ & (C_2) & f(x+y)=0, f(((x+y)+1)+z)=0 \vdash; \\ & (C_3) & f(x+y)=1, f(((x+y)+1)+z)=1 \vdash \}. \end{array}$$

Applying `CERES` to this proof results in the following resolution refutation (generated by otter[2]) of $\mathrm{CL}(\varphi_1)$: $\psi_1 :=$

$$\dfrac{\begin{array}{cc}(C_1) & (C_2)\\ \vdash f(y'+x')=1, f(x'+y')=0 & f(x+y)=0, f(((x+y)+1)+z)=0 \vdash\end{array}}{D_1 : f(((x+y)+1+z)=0 \vdash f(y+x)=1}\ \mathrm{res}_{\sigma_1}$$

where $\sigma_1 = \{x' \leftarrow x, y' \leftarrow y\}$.

$\psi_2 :=$

$$\dfrac{\begin{array}{cc}(C_1) & (D_1)\\ \vdash f(y'+x')=1, f(x'+y')=0 & f(((x+y)+1)+z)=0 \vdash f(y+x)=1\end{array}}{C_4 :\vdash f(y+x)=1, f(z+((x+y)+1))=1}\ \mathrm{res}_{\sigma_2}$$

where $\sigma_2 = \{x' \leftarrow (x+y)+1, y' \leftarrow z\}$.

$\psi_3 :=$

$$\dfrac{\begin{array}{cc}(C_4) & (C_3)\\ \vdash f(y'+x')=1, f(z'+((x'+y')+1))=1 & f(((x+y)+1)+z)=1, f(x+y)=1 \vdash\end{array}}{D_2 : f(x+y)=1 \vdash f(y'+x')=1}\ \mathrm{res}_{\sigma_3}$$

where $\sigma_3 = \{z \leftarrow (x'+y')+1, z' \leftarrow (x+y)+1\}$.

$\psi_4 :=$

$$\dfrac{\dfrac{\begin{array}{cc}(C_4) & (D_2)\\ \vdash f(y''+x'')=1, f(z''+((x''+y'')+1))=1 & f(x+y)=1 \vdash f(y'+x')=1\end{array}}{\vdash f(y''+x'')=1, f(y'+x')=1}\ \mathrm{res}_{\sigma_4}}{C_5 :\vdash f(v+u)=1}\ \mathrm{factor}$$

where $\sigma_4 = \{x \leftarrow z'', y \leftarrow (x''+y'')+1\}$.

$\psi_5 :=$

$$\dfrac{\begin{array}{cc}(C_5) & \dfrac{\begin{array}{cc}(C_5) & (C_3)\\ \vdash f(v+u)=1 & f(x+y)=1, f(((x+y)+1)+z)=1 \vdash\end{array}}{f(((x+y)+1)+z))=1 \vdash}\ \mathrm{res}_{\sigma_6}\\ \vdash f(v+u)=1 & \end{array}}{\vdash}\ \mathrm{res}_{\sigma_5}$$

where $\sigma_5 = \{v \leftarrow (x+y)+1, u \leftarrow z\}$ and $\sigma_6 = \{v \leftarrow x, u \leftarrow y\}$.

[2] `http://www.mcs.anl.gov/AR/otter/`

The projections are: $\varphi_1[C_1] =$

$$\dfrac{\dfrac{f(s)=0 \vdash f(s)=0 \qquad \dfrac{\vdash t=s \quad f(t)=1 \vdash f(t)=1}{f(s)=1 \vdash f(t)=1} =:\mathrm{l}}{f(s)=0 \vee f(s)=1 \vdash f(s)=0, f(t)=1} \vee:\mathrm{l}}{\dfrac{(\forall x)(f(x)=0 \vee f(x)=1) \vdash f(s)=0, f(t)=1}{T \vdash \exists p \exists q(p \neq q \wedge f(p)=f(q)), f(s)=0, f(t)=1} \mathrm{w}:\mathrm{r}} \wedge:\mathrm{l}$$

where $s = n_0 + n_1$ and $t = n_1 + n_0$.

For $i = 2, 3$ the projection $\varphi_1[C_i] =$

$$\dfrac{\dfrac{\dfrac{\psi \quad \eta_i}{f(s)=i, f(t)=i \vdash s \neq t \wedge f(s)=f(t)} \wedge:\mathrm{r}}{f(s)=i, f(t)=i \vdash \exists q(s \neq q \wedge f(s)=f(q))} \exists:\mathrm{r}}{f(s)=i, f(t)=i, T \vdash \exists p \exists q(p \neq q \wedge f(p)=f(q))} \exists:\mathrm{r}$$

for $s = n_0 + k_0$, $t = ((n_0 + k_0) + 1) + k_1$ and

$\psi =$

$$\dfrac{\vdash (n_0+k_0)+(1+k_1)=((n_0+k_0)+1)+k_1 \quad n_0+k_0=(n_0+k_0)+(1+k_1) \vdash}{\dfrac{\dfrac{n_0+k_0=((n_0+k_0)+1)+k_1 \vdash}{\vdash \neg n_0+k_0=((n_0+k_0)+1)+k_1}\neg:\mathrm{r}}{\vdash n_0+k_0 \neq ((n_0+k_0)+1)+k_1}} =:\mathrm{l}$$

and $\eta_i =$

$$\dfrac{f(s)=i \vdash f(s)=i \qquad \dfrac{f(t)=i \vdash f(t)=i \quad \vdash i=i}{f(t)=i \vdash i=f(t)} =:\mathrm{r}}{f(s)=i, f(t)=i \vdash f(s)=f(t)} =:\mathrm{r}$$

Putting together the resolution refutation with the projections we obtain the atomic cut normal form φ_1'. From the point of view of the analysis of mathematical proofs it is useful to transform this formal proof into a mathematical argument in the usual textbook format. In this process – which is carried out by hand – it is necessary to be more liberal than a formal calculus: In particular we regard clauses modulo the negation-left and negation-right rules (from sequent calculus), we read them – as it fits – as disjunctions or implications, and we regard terms modulo simple arithmetical transformations like associativity and commutativity. The proof φ_1' in a usual textbook style is as follows:

Proof. **First Combinatorial Proof of Proposition 6.1:** Assume that Proposition 6.1 does not hold, then for all cells x we would have ($\varphi_1[C_2]$) that $f(x) = 0$ implies that all cells behind x are different from 0 (C_2) and the same for 1 ($\varphi_1[C_3]$).

But as the only values are 0 and 1 (C_1) this would mean that $f(x) = 1$ or all cells behind x are equal to 1 (C_4). Now, in particular this means that there is a cell with value 1 with index, say x'. But then all cells behind it are different from 1, in particular all cells of the form $u+(x'+1)+1$ (resolve C_3, C_4) so there is a cell behind u that is different from 1. So $f(u)$ must be 1 but u was arbitrary so all cells would have value 1 (C_5). But we know (C_3) that there is a cell different from 1. Contradiction! □

Note that in this proof φ'_1 the argument making the connection between the value of a cell and the values behind it is absolutely essential. This argument is contained in the clauses C_2 (for the value 0) and C_3 (for the value 1). It is derived from the assumption that the proposition is false by the projections $\varphi[C_2]$ and $\varphi[C_3]$. Every cut-free proof originating from φ_1 *must* make use of this kind of argument because only by using both C_2 and C_3 we can arrive at a contradiction. This connection between a cell x and all cells behind it is the trace – in the cut-free proofs – of the form of the lemmas that are eliminated: $(\forall n)(\exists k)f(n+k) = v$. So although the lemma on the existence of a value occurring an infinite number of times on the tape does no longer occur in the cut-free proof, its traces are still present and can be described by a detailed analysis of the cut-elimination process.

6.2 The Alternating Tape Argument

We will now analyze a second proof of the same proposition resulting both in a different characteristic clause set and in different cut-free proofs.

Definition 6.2. An infinite tape f is called *changing* if each two adjacent cells have different values ($C := (\forall x)f(x) \neq f(x+1)$).

Definition 6.3. An infinite tape f is called *alternating* if it is changing and for all positions x we have $f(x) = f(x+2)$ ($A := C \wedge (\forall x)f(x) = f(x+2)$).

Proof. **Second Proof of Proposition 6.1 (Alternating Tape Argument):** We make a case distinction on wether f is changing.

1. If f is changing then, as there are only two values, the tape is also alternating. Now, as the tape is alternating, the cells at positions 0 and 2 have the same value.

2. If f is not changing then by definition there is a position x with $f(x) = f(x+1)$ but as x and $x+1$ are different, the proposition follows.

□

The formalization φ_2 of this proof is as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{(\chi_1)}{T, C \vdash A} \quad \dfrac{(\chi_2)}{A \vdash P}}{T, C \vdash P}\,\text{cut}}{T \vdash P, \neg C}\,\neg\text{: r} \qquad \dfrac{\dfrac{(\chi_3)}{\neg C \vdash E} \quad \dfrac{(\chi_4)}{E \vdash P}}{\neg C \vdash P}\,\text{cut}}{T \vdash P}\,\text{cut}$$

where

$$\begin{aligned} T &\equiv (\forall x)(f(x) = 0 \vee f(x) = 1), \\ P &\equiv (\exists p)(\exists q)(p \neq q \wedge f(p) = f(q)), \\ C &\equiv (\forall x) f(x) \neq f(x+1), \\ A &\equiv C \wedge (\forall x) f(x) = f(x+2), \\ E &\equiv (\exists x) f(x) = f(x+1). \end{aligned}$$

and the case distinction on wether C or $\neg C$ is formalized as a cut on $\neg C$. The proof χ_1 shows that every changing tape is alternating by case distinctions on cell values, χ_2 shows that an alternating tape fulfills the proposition *by choosing the two cells* 0 *and* 2, χ_3 shows that on a tape that is not changing there must be two *adjacent* cells with the same value and χ_4 shows that in this case the proposition is fulfilled.

The characteristic clause set of φ_2 consists of 127 clauses. However after application of a tautology-deletion and a subsumption operator (which can easily be done fully automatically) the set collapses to the following three non-redundant clauses:

$$\begin{aligned} \mathcal{C} = \{ \quad & (C_1) \quad \vdash f(x) = 0, f(x) = 1; \\ & (C_2) \quad f(0) = f(2) \vdash; \\ & (C_3) \quad f(y) = f(y+1) \vdash \}. \end{aligned}$$

This clause set shares the clause C_1 with the clause set of the previous proof $CL(\varphi_1)$. This clause contains the *positive information* axiomatizing the tape situation: It is logically equivalent to T. The other two clauses, however, are different: The clause C_2 is generated from the proof χ_2 (and would contain other numerals if other cells would have been compared in χ_2), C_3 is generated from χ_3 and its structure clearly reflects the formula C.

The resolution prover otter found the following refutation of $\mathcal{C}$:

$\psi_1 :=$

$$\dfrac{\dfrac{(C_1)}{\vdash f(x)=0, f(x)=1} \quad \dfrac{\dfrac{(C_1)}{\vdash f(x)=0, f(x)=1} \quad \dfrac{\dfrac{(C_3)}{\vdash 0+1=1 \quad f(y)=f(y+1)\vdash}\ \text{para}_{\{y\leftarrow 0\}}}{f(1)=f(0)\vdash}\ \text{para}_{\{x\leftarrow 1\}}}{f(0)=1\vdash f(1)=0}\ \text{res}_{\{x\leftarrow 0\}}}{C_4 :\vdash f(0)=0, f(1)=0}$$

$\psi_2 :=$

$$\dfrac{\dfrac{(C_1)}{\vdash f(x)=1, f(x)=0} \quad \dfrac{\dfrac{(C_1)}{\vdash f(x)=1, f(x)=0} \quad \dfrac{\dfrac{(C_3)}{\vdash 0+1=1 \quad f(y)=f(y+1)\vdash}\ \text{para}_{\{y\leftarrow 0\}}}{f(1)=f(0)\vdash}\ \text{para}_{\{x\leftarrow 1\}}}{f(0)=0\vdash f(1)=1}\ \text{res}_{\{x\leftarrow 0\}}}{C_5 :\vdash f(0)=1, f(1)=1}$$

$\psi_3 :=$

$$\dfrac{\dfrac{(C_1)}{\vdash f(x)=1, f(x)=0} \quad \dfrac{(C_3)}{f(y)=f(y+1)\vdash}\ \text{para}_{\{x\leftarrow y+1\}} \quad \dfrac{(C_2)}{f(2)=f(0)\vdash}\ \text{para}_{\{y\leftarrow 1\}}}{C_6 : f(1)=0, f(0)=1\vdash}$$

$\psi_4 :=$

$$\dfrac{\dfrac{(C_1)}{\vdash f(x)=0, f(x)=1} \quad \dfrac{\dfrac{(C_4)}{\vdash f(0)=0, f(1)=0} \quad \dfrac{(C_6)}{f(1)=0, f(0)=1\vdash}\ \text{res}}{f(0)=1\vdash f(0)=0}\ \text{res}_{\{x\leftarrow 0\}}}{C_7 :\vdash f(0)=0}$$

$\psi_5 :=$

$$\dfrac{\dfrac{(C_1)}{\vdash f(x)=1, f(x)=0} \quad \dfrac{\dfrac{(C_5)}{\vdash f(1)=1, f(0)=1} \quad \dfrac{(C_6)}{f(0)=1, f(1)=0\vdash}\ \text{res}}{f(1)=0\vdash f(1)=1}\ \text{res}_{\{x\leftarrow 1\}}}{C_8 :\vdash f(1)=1}$$

$\psi_6 :=$

$$\dfrac{\dfrac{(C_7)}{\vdash f(0)=0} \quad \dfrac{\dfrac{(C_1)}{\vdash f(x)=1, f(x)=0} \quad \dfrac{(C_2)}{f(0)=f(2)\vdash}\ \text{para}_{\{x\leftarrow 2\}}}{f(0)=0\vdash f(2)=1}\ \text{res}}{C_9 :\vdash f(2)=1}$$

$\psi_7 :=$

$$\dfrac{\dfrac{(C_9)}{\vdash f(2)=1} \quad \dfrac{\dfrac{(C_8)}{\vdash f(1)=1} \quad \dfrac{(C_3)}{f(y)=f(y+1)\vdash}\ \text{para}_{\{y\leftarrow 1\}}}{f(2)=1\vdash}\ \text{res}}{\vdash}$$

The projections are:

$\varphi_2[C_1] :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{f(\alpha)=0 \vdash f(\alpha)=0}{f(\alpha)=0, T \vdash f(\alpha)=0}\, w:l \quad \dfrac{f(\alpha)=1 \vdash f(\alpha)=1}{f(\alpha)=1, T \vdash f(\alpha)=1}\, w:l}{f(\alpha)=0 \vee f(\alpha)=1, T, T \vdash f(\alpha)=0, f(\alpha)=1}\, \vee:l}{f(\alpha)=0 \vee f(\alpha)=1, T \vdash f(\alpha)=0, f(\alpha)=1}\, c:l}{(\forall x)(f(x)=0 \vee f(x)=1), T \vdash f(\alpha)=0, f(\alpha)=1}\, \forall:l}{T \vdash P, f(\alpha)=0, f(\alpha)=1}\, \mathrm{w:r, c:r}$$

$\varphi_2[C_2] :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{0=1+1 \vdash}{\vdash \neg 0=1+1}\, \neg:r}{\vdash 0 \neq 1+1} \qquad f(0)=f(1+1) \vdash f(0)=f(1+1)}{f(0)=f(1+1) \vdash 0 \neq 1+1 \wedge f(0)=f(1+1)}\, \wedge:r}{f(0)=f(1+1) \vdash (\exists y)(0 \neq y \wedge f(0)=f(y))}\, \exists:r}{f(0)=f(1+1) \vdash (\exists x)(\exists y)(x \neq y \wedge f(x)=f(y))}\, \exists:r}{f(0)=f(1+1), T \vdash P}\, \mathrm{w:l}$$

$\varphi_2[C_3] :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\gamma=\gamma+1 \vdash}{\vdash \neg\gamma=\gamma+1}\, \neg:r}{\vdash \gamma \neq \gamma+1} \qquad f(\gamma)=f(\gamma+1) \vdash f(\gamma)=f(\gamma+1)}{f(\gamma)=f(\gamma+1) \vdash \gamma \neq \gamma+1 \wedge f(\gamma)=f(\gamma+1)}\, \wedge:r}{f(\gamma)=f(\gamma+1) \vdash (\exists y)(\gamma \neq y \wedge f(\gamma)=f(y))}\, \exists:r}{f(\gamma)=f(\gamma+1) \vdash (\exists x)(\exists y)(x \neq y \wedge f(x)=f(y))}\, \exists:r}{f(\gamma)=f(\gamma+1), T \vdash P}\, \mathrm{w:l}$$

The atomic cut normal form φ_2' produced by `CERES` is then again (manually) translated into a meaningful mathematical argument in textbook style:

Proof. **Second Combinatorial Proof of Proposition 6.1:** Assume Proposition 6.1 does not hold, then $f(0) \neq f(2)$ ($\varphi_2[C_2]$) and for all y we would have $f(y) \neq f(y+1)$ ($\varphi_2[C_3]$).

As $f(0) \neq f(1)$ (C_3) and there are only two values (C_1), one of these cells must have value 0 (C_4) and one of them must have value 1 (C_5).

As two neighboring cells must be different (C_3), we have that – in particular – $f(1) = 0$ implies $f(2) = 1$. But as $f(2) \neq f(0)$ (C_2) then also $f(0) \neq 1$,

i.e. $f(1) = 0$ implies $f(0) \neq 1$, so $f(1) \neq 0$ or $f(0) \neq 1$ (C_6). So there must be an $i \in \{1, 2\}$ with $f(i) = i$.

But as one of $f(0), f(1)$ must be 0 and one must be 1, the only possibility is $f(0) = 0$ (C_7) and $f(1) = 1$ (C_8). And as $f(0) = 0$ and $f(2) \neq f(0)$ (C_2), we must have $f(2) = 1$ (C_9). But as $f(1) = 1$ and $f(1) \neq f(2)$ (C_3) we must also have $f(2) \neq 1$. Contradiction! □

This proof differs considerably from the combinatorial proof obtained from the infinity-argument: Its building blocks are comparisons of concrete cell values: (1) the values $f(0)$ and $f(2)$ and (2) two adjacent values at various positions, the first kind of comparison arising from the clause C_2, the second from C_3.

6.3 Discussion

The usual situation for a mathematical proof is that we have some background theory Γ and that we want to show that in this theory, some proposition P holds[3]. Formally this means to construct a sequent calculus proof of the sequent $\Gamma \vdash P$ or equivalently: $\Gamma, \neg P \vdash$.

The characteristic clause set (as well as the profile) can be divided into two different classes of clauses: Those that follow from Γ alone and are thus true in the intended interpretation (of the theory) and those that follow only from $\Gamma \wedge \neg P$ and are thus false in the intended interpretation and so form the basic building blocks of a proof-by-contradiction of P. Which case applies to a specific clause can be read off from the projection to the clause.

The atomic cut normal forms produced by the CERES-method can thus be interpreted as indirect mathematical proofs divided into two parts: In the first part the clauses that are false in the intended interpretation are derived from the axioms Γ and the negation of the proposition P, and the true clauses are derived from the axioms alone; this corresponds to the projections in CERES. In the second part, it is shown that a contradiction can be derived from all these clauses and that thus P cannot be false (if the truth of the axioms is to be maintained). This part corresponds to the resolution refutation.

An analysis of the characteristic clause sets of different proofs of the same theorem (without actually going through the whole cut-elimination process) thus already reveals restrictions on the type of cut-free argument that can be obtained. Although different combinatorial arguments can be obtained from the same proof with cuts (see [3]) *all* the arguments obtained from a certain

[3] In our example Γ is T plus the simple arithmetical axioms that were used in the proofs as atomic initial sequents: associativity and commutativity of $+$, etc.

proof with cuts have in common that they have the same argumentative building blocks at their disposal: the clauses of the characteristic clause set.

In the infinity argument this building block was a relation between the value of a cell and the values of all cells behind it, in the alternating-tape argument these building blocks where comparisons of the value of the cells 0 and 2 as well as of two adjacent cells in general. This means that although the cuts are completely eliminated from the output proofs, the form of the argument with cuts leaves its traces in the cut-free proofs by a restriction on the form of cut-free proofs that can be obtained. This can be seen in the above-mentioned division of the mathematical interpretation of an atomic cut normal form as the fact that *all* combinatorial arguments obtained from the same proof with cuts will have the same first part (that is the derivation of the clauses from the axioms and the negated proposition) and will differ only in their second part: The way the contradiction is derived from the clauses.

This restriction on the form of cut-free proofs can be modelled with and read off the characteristic clause set. Furthermore, due to the subsumption result in [10] (and in Section 5.1 for the profile) this restriction is not specific to the CERES-method but applies to all reductive cut-elimination procedures, in particular Gentzen's original.

The extraction of the characteristic clause set can always be done fully automatically. In the examples given here the resolution refutations were also generated automatically but in general – and in particular for larger proofs – it seems necessary to generate the refutations in a semi-automatic, interactive way. But the above considerations show that the extraction of the characteristic clause set alone is already of a high mathematical value. Thus the subdivision of the cut-elimination process into two phases, the first being the extraction of the characteristic clause set and the second being its refutation is a *qualitative* advantage of the CERES-method over reductive cut-elimination methods because it provides information about the proof with cuts that reductive methods cannot.

Chapter 7

Conclusion and Future Work

We have presented an improved variant of the characteristic clause sets of the CERES-method: The *profile* of a proof. The profile is computationally superior to the characteristic clause set: Due to the subsumption of the characteristic clause set by the profile (Proposition 3.4) for any resolution refutation of the characteristic clause set of length l there exists one of the profile of length $l' \leq l$. This result justifies the replacement of the characteristic clause set by the profile in the implementation of the CERES-method. But the profile is even stronger in detecting certain kinds of redundancies One can show that there exist sequences of proofs where all resolution refutations of the characteristic clause set are of non-elementary length while there is a refutation of the profile of a constant length (Example 3.1).

We have shown that the profile is invariant under permutation of independent rules (Proposition 4.1) which shows that if two proofs have the same proof net, they also have the same profile. In this sense the profile is a generalization of the proof net: It abstracts from more details of the formal proof.

In Section 4.2 we first gave different characterizations of the Herbrand-disjunction (or -sequent) of a formal proof and of partial Herbrand-sequents. This served as technical preparation for showing the main result of Chapter 4: That there is an intimate relation between the two partial Herbrand-sequents of a proof – the instances of the end-sequent and the instances of the cut-formulas – to the two dual parts of the profile defined for the respective parts of the proof (see Figure 4.2.6). The most involved part of this result is showing that the two parts of the profile with tautologies indeed subsume (respectively are subsumed by) the conjunctive (respectively disjunctive) normal form of the partial Herbrand-sequent of the respective part of the proof. This demonstrates that the profile is a combination of two different techniques for abstracting from formal details of a proof or of a formula: of Herbrand-sequents on one hand for abstracting from details of the

proof structure and of the CNF and DNF normal form transformations on the other hand for abstracting from details of the representation of the formulas in the Herbrand-sequents. Moreover, removing the tautologies yields clause sets which contain the same logical information with considerably less redundancy. The most surprising aspect of this result is that there exists a simple duality between the partial Herbrand-sequent of the end-sequent and the partial Herbrand-sequent of the cut-formulas, the first representing the instances of formulas of the theorem shown in the proof and the second representing the instances of the lemmas used in the proof for showing the theorem.

In Section 5.1 we have given a detailed analysis of the effect of cut-elimination on the profile. It turned out that it is extremely well behaved: Clauses are removed if and only if a weakening rule is eliminated, clauses are duplicated if and only if a contraction rule is eliminated and clauses are instantiated if and only if a quantifier rules is eliminated. In all other cases the profile remains unchanged.

We have defined a large class of proof transformations that can be applied to cut-formulas and leave the profile invariant in Section 5.2. This not only gives as corollary the invariance of the profile under certain important specific transformations like e.g. the negation normal form transformation but also gives general conditions that guarantee the invariance of the profile. These simple transformations basically perform a rearrangement of the proof without changing its size. Indeed, the most important structural restrictions are the absence of deletion and duplication operations while the restriction on the term level amounts to allowing only variable permutations as substitutions. This class of transformations has been defined by defining a class of transformation proofs that are applied – by using cut-elimination as an interpreter – to the proof to be transformed, a way of using formal proofs not uncommon in the literature on the λ-calculus.

In Chapter 6 we have used the characteristic clause set for the analysis of two different proofs (with cuts) of the same proposition. We have run the CERES-method on both of these proofs to obtain – for each of them – a purely combinatorial argument. Interestingly we could observe not only that the two combinatorial arguments obtained this way are different, but it is already possible by examination of the characteristic clause sets alone to anticipate these differences. The clauses of the profile of a proof constitute the argumentative building blocks of *all* cut-free proofs that can be obtained from the original proof. This means that the profile provides qualitative information about a proof that cannot be obtained in a different way, in particular not by standard cut-elimination methods à la Gentzen. As the extraction of the profile can be easily automated, this kind of computer-aided proof analysis scales also to much larger proofs.

Apart from the application of these methods to concrete mathematical proofs, there exists also considerable potential for future theoretical work: In Section 5.2 we have shown that simple transformations when applied to cut-formulas do not change the profile. An obvious extension of this result is to investigate also the effect of these transformations when applied to the end-sequent. Altough this will be a more complicated situation – the status of the transformed formula occurrences changes from being ancestor of the end-sequent to being ancestor of a cut-formula – we still conjecture that the same result, i.e. the invariance of the profile can be shown. Another interesting extension of this result is to consider systems of second- and higher-order logic. Also for those systems rewrite relations performing cut-elimination exist and can be used as a basis for the definition of simple transformations. As the simple transformations do not use essential second-order features (like comprehension), defining the profile as for the first-order system will make it possible to carry out the invariance proofs in a similar way.

The nice behavior of the profile under cut-elimination (see Section 5.1) together with the invariance under simple transformation suggests to consider also other classes of transformations. For example allowing weakening to be applied to the formula that is transformed might result in the profile not staying completely invariant but instead losing certain (corresponding) clauses. Similarly, one might conjecture that allowing contractions will exactly duplicate certain clauses and allowing substitutions which are not only variable permutations will exactly instantiate certain clauses.

For studying the combinatorics of the profile, it seems most rewarding to perform a deeper analysis of the label sets that can be found in the clauses of the profile. Each of these label sets corresponds to a set of axioms of the original proof that is needed as a basis for a cut-free fragment of the original proof: a projection. In this sense the projections of the CERES-method are a decomposition of the original proof into its cut-free parts. Apart from forming a basis for all cut-free proofs what does this decomposition tell us about the structure of the original proof ? The analysis in Section 4.3 shows that there is a remarkable connection to the logical flow graph of the proof under consideration. It remains to be investigated how far this connection can be extended.

Bibliography

[1] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[2] Matthias Baaz, Uwe Egly, and Alexander Leitsch. Normal Form Transformations. In *Handbook of Automated Reasoning*, pages 273–333. 2001.

[3] Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter, and Hendrik Spohr. Cut-Elimination: Experiments with CERES. In Franz Baader and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning (LPAR) 2004*, volume 3452 of *Lecture Notes in Computer Science*, pages 481–495. Springer, 2005.

[4] Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter, and Hendrik Spohr. Proof Transformation by CERES. In Jonathan M. Borwein and William M. Farmer, editors, *Mathematical Knowledge Management (MKM) 2006*, volume 4108 of *Lecture Notes in Artificial Intelligence*, pages 82–93. Springer, 2006.

[5] Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter, and Hendrik Spohr. System Description: The Cut-Elimination System CERES. In G. Sutcliffe, R. Schmidt, and S. Schulz, editors, *Proceedings of the FLoC'06 Workshop on Empirically Sucessful Computerized Reasoning*, volume 192 of *CEUR Workshop Proceedings*, pages 159–167, 2006.

[6] Matthias Baaz and Alexander Leitsch. On skolemization and proof complexity. *Fundamenta Informaticae*, 20(4):353–379, 1994.

[7] Matthias Baaz and Alexander Leitsch. Cut Normal Forms and Proof Complexity. *Annals of Pure and Applied Logic*, 97:127–177, 1999.

[8] Matthias Baaz and Alexander Leitsch. Cut-elimination and Redundancy-elimination by Resolution. *Journal of Symbolic Computation*, 29(2):149–176, 2000.

[9] Matthias Baaz and Alexander Leitsch. Ceres in many-valued logics. In Franz Baader and Andrei Voronkov, editors, *Logic for Programming,*

Artificial Intelligence, and Reasoning, LPAR 2004, volume 3452 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2005.

[10] Matthias Baaz and Alexander Leitsch. Towards a clausal analysis of cut-elimination. *Journal of Symbolic Computation*, 41(3–4):381–410, 2006.

[11] Garrett Birkhoff. *Lattice Theory*, volume XXV of *American Mathematical Society Colloquium Publications*. American Mathematical Society, 3rd edition, 1967.

[12] Samuel R. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic*, 53:75–102, 1991.

[13] Samuel R. Buss. On Herbrand's Theorem. In *Logic and Computational Complexity*, volume 960 of *Lecture Notes in Computer Science*, pages 195–209. Springer, 1995.

[14] Alessandra Carbone. Interpolants, cut elimination and flow graphs for the propositional calculus. *Annals of Pure and Applied Logic*, 83:249–299, 1997.

[15] Alessandra Carbone. Duplication of directed graphs and exponential blow up of proofs. *Annals of Pure and Applied Logic*, 100:1–76, 1999.

[16] Alessandra Carbone. Turning cycles into spirals. *Annals of Pure and Applied Logic*, 96:57–73, 1999.

[17] Alessandra Carbone. Cycling in Proofs and Feasibility. *Transactions of the American Mathematical Society*, 352:2049–2075, 2000.

[18] Alessandra Carbone. The cost of a cycle is a square. *Journal of Symbolic Logic*, 67:35–60, 2002.

[19] Alessandra Carbone and Stephen Semmes. *A Graphic Apology for Symmetry and Implicitness*. Oxford Mathematical Monographs. Oxford University Press, 2000.

[20] Vincent Danos, Jean-Baptiste Joinet, and Harold Schellinx. A New Deconstructive Logic: Linear Logic. *Journal of Symbolic Logic*, 62(3):755–807, 1997.

[21] Vincent Danos, Jean-Baptiste Joinet, and Harold Schellinx. Computational isomorphisms in classical logic. *Theoretical Computer Science*, 294(3):353–378, 2003.

[22] Jean Gallier. Constructive Logics. Part I: A Tutorial on Proof Systems and Typed λ-Calculi. *Theoretical Computer Science*, 110(2):249–339, 1993.

[23] G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210,405–431, 1934–1935.

[24] Gerhard Gentzen. Die Widerspruchsfreiheit der reinen Zahlentheorie. *Mathematische Annalen*, 112:493–565, 1936.

[25] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50, 1987.

[26] Jean-Yves Girard. *Proof Theory and Logical Complexity*. Elsevier, 1987.

[27] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[28] Georges Gonthier. A computer-checked proof of the Four-Color Theorem. available from `http://research.microsoft.com/~gonthier/4colproof.pdf`.

[29] J. Herbrand. *Recherches sur la théorie de la démonstration*. PhD thesis, University of Paris, 1930.

[30] Stefan Hetzl. A Similiarity Criterion for Proofs (abstract). In Arnold Beckmann, Ulrich Berger, Benedikt Löwe, and John V. Tucker, editors, *Logical Approaches to Computational Barriers, Second Conference on Computability in Europe, CiE 2006*, number CSR 7-2006 in Report Series, page 296. University of Wales, Swansea, 2006.

[31] Stefan Hetzl and Alexander Leitsch. Proof Transformations and Structural Invariance. In Stefano Aguzzoli, Agata Ciabattoni, Brunella Gerla, Corrado Manara, and Vincenzo Marra, editors, *Algebraic and Proof-theoretic Aspects of Non-classical Logics*, Lecture Notes in Computer Science. Springer, 2007. to appear.

[32] Stefan Hetzl and Petra Mutzel. A Graph–Theoretic Approach to Steganography. In Jana Dittmann, Stefan Katzenbeisser, and Andreas Uhl, editors, *9th IFIP Conference on Communications and Multimedia Security (CMS 2005)*, volume 3677 of *Lecture Notes in Computer Science*, pages 119–128. Springer, 2005.

[33] S. C. Kleene. Permutability of Inferences in Gentzen's Calculi LK and LJ. *Memoirs of the American Mathematical Society*, (10):1–26, 1952.

[34] Ulrich Kohlenbach. Effective Uniform Bounds from Proofs in Abstract Functional Analysis. In B. Cooper, B. Loewe, and A. Sorbi, editors, *CiE 2005 New Computational: Changing Conceptions of What is Computable*. Springer. to appear.

[35] Georg Kreisel. On the Interpretation of Non-Finitist Proofs – Part I. *Journal of Symbolic Logic*, 16(4):241–267, 1951.

[36] Georg Kreisel. On the Interpretation of Non-Finitist Proofs – Part II. Interpretation of Number Theory. *Journal of Symbolic Logic*, 17(1):43–58, 1952.

[37] Georg Kreisel. Mathematical Significance Of Constistency Proofs. *Journal of Symbolic Logic*, 23(2):155–182, 1958.

[38] Alexander Leitsch. *The Resolution Calculus*. Texts in Theoretical Computer Science. Springer, 1997.

[39] Horst Luckhardt. Herbrand-Analysen zweier Beweise des Satzes von Roth: Polynomiale Anzahlschranken. *Journal of Symbolic Logic*, 54(1):234–263, 1989.

[40] Richard McKinley. *Categorical Models of First-Order Classical Proofs*. PhD thesis, University of Bath, 2006.

[41] P.V. Orevkov. Lower bounds for increasing complexity of derivations after cut elimination. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta*, 88:137–161, 1979.

[42] Dag Prawitz. *Natural Deduction: A Proof-Theoretical Study*. Almqvist and Wicksell, Stockholm, 1965.

[43] Pavel Pudlák. The Lengths of Proofs. In Sam Buss, editor, *Handbook of Proof Theory*, pages 547–637. Elsevier, 1998.

[44] Edmund Robinson. Proof nets for classical logic. *Journal of Logic and Computation*, 13(5):777–797, 2003.

[45] J. A. Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12(1):23–41, 1965.

[46] Thoralf Skolem. Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit und Beweisbarkeit mathematischer Sätze nebst einem Theoreme über dichte Mengen. In J. E. Fenstad, editor, *Selected works in logic by Th. Skolem*, pages 103–136. Universitetsforlaget Oslo-Bergen-Tromsö, 1970.

[47] R. Statman. Lower bounds on Herbrand's theorem. *Proceedings of the American Mathematical Society*, 75:104–107, 1979.

[48] W.W. Tait. Normal derivability in classical logic. In J. Barwise, editor, *The Syntax and Semantics of Infinitary Languages*, volume 72 of *Lecture Notes in Mathematics*, pages 204–236. Springer, 1968.

[49] Gaisi Takeuti. *Proof Theory*. North-Holland, Amsterdam, 2nd edition, March 1987.

[50] Christian Urban. *Classical Logic and Computation*. PhD thesis, University of Cambridge, October 2000.

[51] Christian Urban and Gavin Bierman. Strong Normalization of Cut-Elimination in Classical Logic. *Fundamenta Informaticae*, 44:1–34, 2000.

Index of Notation

Index