Describing Proofs by Short Tautologies ⋆

Stefan Hetzl *

Institute of Computer Languages (E185),
Vienna University of Technology, Favoritenstraße 9,
1040 Vienna, Austria

Abstract

Herbrand's theorem is one of the most fundamental results about first-order logic. In the context of proof analysis, Herbrand-disjunctions are used for describing the constructive content of cut-free proofs. However, given a proof with cuts, the computation of an Herbrand-disjunction is of significant computational complexity, as the cuts in the proof have to be eliminated first.

In this paper we prove a generalization of Herbrand's theorem: From a proof with cuts, one can read off a small (linear in the size of the proof) tautology composed of instances of the end-sequent and the cut formulas. This tautology describes the proof in the following way: Each cut induces a (propositional) formula stating that a disjunction of instances of the cut formula implies a conjunction of instances of the cut formula. All these cut-implications together then imply the already existing instances of the end-sequent. The proof that this formula is a tautology is carried out by transforming the instances in the proof to normal forms and using characteristic clause sets to relate them. These clause sets have first been studied in the context of cut-elimination.

This extended Herbrand theorem is then applied to cut-elimination sequences in order to show that, for the computation of an Herbrand-disjunction, the knowledge of only the term substitutions performed during cut-elimination is already sufficient.

Key words: Proof theory, Herbrand's theorem, Cut-elimination

AMS subject code classification: 03F05, 03F07, 03F20

⋆ supported by the Austrian Science Fund (projects no. P17995 and P19875)
* Phone +43-1-58801-18547, Fax +43-1-58801-18597
Email address: hetzl@logic.at (Stefan Hetzl).

1 Introduction

One of the most fundamental results about first-order logic is Herbrand's Theorem: In its simplest version it says that, if F is a quantifier-free formula and $(\exists \vec{x})F$ is valid, then there exists a finite disjunction of instances of F which is a propositional tautology. There are other variants and generalizations of this theorem, see [6]. Herbrand's theorem is the basis for completeness proofs of various calculi for first-order logic. Herbrand-disjunctions also play an important role for proof analysis: They provide a description of the constructive content of a cut-free proof, see e.g. [13] for an Herbrand-analysis. The computation of an Herbrand-disjunction from a proof however can be quite expensive: It is a well-known result that the size of the shortest Herbrand-disjunction of a formula cannot be bounded by an elementary function in the size of the shortest proof of the formula [14]. This is due to the complexity of cut-elimination: A cut-free proof has an Herbrand-disjunction of linear size.

In this paper we prove a generalization of Herbrand's theorem: From a prenex proof with cuts, one can read off a tautology composed of instances of the end-sequent *and the cut formulas*. This tautology is of a particularly natural form: Each cut induces an implication stating that the disjunction of the instances of the positive cut formula implies the conjunction of the instances of the negative cut formula. The conjunction of all these cut-implications then implies the instances of the end-sequent (composed as a sequent, i.e. a conjunction implying a disjunction). This tautology can easily be read off from a proof and its size is linearly bounded by the size of the proof. In the case of a cut-free proof, the formula coincides with the mid-sequent of the proof.

To show that this formula is a tautology, we will proceed as follows: The proof with cuts is divided into two parts: The *implicit* inferences (deriving the cut formulas) and the *explicit* inferences (deriving the end-sequent). For each of these parts we will transform the quantifier-free formula instances to clause normal forms and relate them via subsumption to *characteristic clause sets* (which were first studied in the context of cut-elimination [5]). Showing a simple duality between the characteristic clause sets associated to the implicit part and those associated to the explicit part allows to conclude that the formula is indeed a tautology.

Finally, this extended Herbrand-theorem is applied to cut-elimination. We show that a cut-elimination sequence can be partitioned into a propositional and a first-order part, the latter consisting of a composition of the substitutions and variable renamings performed during cut-elimination. We show that knowledge of this part of the cut-elimination sequence is sufficient for computing an Herbrand-disjunction from the original proof. This result paves the way for more streamlined cut-elimination procedures computing only this

first-order part.

2 Sequent Calculus

We use a standard sequent calculus for first-order logic. A sequent will be a pair of multisets of formulas.

Definition 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:

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

(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 usual conditions must hold:
(a) t must not contain a variable that occurs bound in A
(b) α is called eigenvariable *and must not occur in $\Gamma \cup \Delta \cup \{A\}$ (eigenvariable condition).*

(3) Structural Rules

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

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

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

The rules $\forall : r$ and $\exists : l$ are called *strong* quantifier rules. A proof φ is called *regular* if the eigenvariables of the strong quantifier rules are pairwise different. We will assume regularity throughout this paper. 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. If an occurrence is not active for a rule ρ, it is said to be in the *context* of ρ. An auxiliary occurrence of a cut is called *cut occurrence*. A formula occurrence is called *end occurrence* if it is in the end-sequent. A formula occurrence is called *terminal occurrence* if it is a cut occurrence or an end occurrence. For technical purposes we will also consider proofs in a calculus extended by a juxtaposition rule.

Definition 2 ($\mathbf{LK^j}$-proof) *An* $\mathbf{LK^j}$*-proof is an* $\mathbf{LK}$*-proof where in addition the following rule of* juxtaposition *is allowed:*

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

3 Herbrand Sequents

Gentzen's mid-sequent theorem [8] is a proof-theoretic version of Herbrand's theorem based on cut-elimination. It states that any cut-free prenex $\mathbf{LK}$-proof can be transformed into a proof of the same end-sequent s.t. no quantifier rule occurs above a propositional rule. A formula is called *prenex* if no quantifier appears behind 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. In this section we define a unique mid-sequent $\mathcal{H}(\varphi)$ of a cut-free prenex $\mathbf{LK^j}$-proof φ. In order to do this, we build on the notion of *ancestor* in the sequent calculus, defined 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.

Definition 3 (associated contraction) *Let φ be an* $\mathbf{LK}^{\mathrm{j}}$*-proof containing a quantifier rule ρ with main occurrence μ. If σ is a contraction rule below ρ having 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, then σ is said to be* associated to *ρ.*

Definition 4 (mid-sequent reduction) *Let φ be a cut-free prenex* $\mathbf{LK}^{\mathrm{j}}$*-proof and let ρ be a quantifier rule appearing above a propositional or juxtaposition rule. We define the transformation $\to_{\mathcal{M}}$ permuting ρ downwards.*

Assume 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). If τ is a unary propositional rule, then the subproof χ of φ at τ has the following form: $\chi =$

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

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'. Then $\chi \to_{\mathcal{M}} \chi'$ where $\chi' =$

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

Due to regularity, the eigenvariable condition of ρ in χ' is fulfilled. If τ is a juxtaposition or a binary propositional rule and ρ any other type of quantifier rule, we proceed analogously.

We say that a cut-free prenex proof φ is in mid-sequent normal form if there is no φ' s.t. $\varphi \to_{\mathcal{M}} \varphi'$. A proof in mid-sequent normal form 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. If the two parts are separated by a list of structural rules, there are several mid-sequents. We will apply a further normalization step to obtain a unique mid-sequent.

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. For a multiset M we write $\mathrm{set}(M)$ for the set that contains an element iff M contains it at least once.

Definition 5 (Herbrand-sequent) *Let φ be a cut-free prenex $\mathbf{LK^j}$-proof in mid-sequent normal form. Then φ has a lowest propositional or juxtaposition rule ρ. Let s be the conclusion sequent of ρ. We define the* Herbrand-sequent

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

Using $\mathrm{U}(\cdot)$ and $\mathrm{set}(\cdot)$ gives a unique definition of the Herbrand-sequent of a proof in *mid-sequent normal form*. But mid-sequent reduction is not confluent in the strict syntactic sense. We will show, however, that it is confluent w.r.t. the Herbrand-sequent defined above.

Definition 6 *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.

Let μ be a prenex formula occurrence in a proof φ. A formula F is called instance *of μ if there is an occurrence ν of F that is auxiliary formula of a quantifier rule and an ancestor of μ.*

Definition 7 *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

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

For two sequents $\Gamma \vdash \Delta$ and $\Pi \vdash \Lambda$ we define their *merge* as $(\Gamma \vdash \Delta) \circ (\Pi \vdash \Lambda) := \Gamma, \Pi \vdash \Delta, \Lambda$.

Lemma 1 *Let φ be a cut-free prenex $\mathbf{LK^j}$-proof and let φ^* be any mid-sequent normal form of φ. Then*

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

Proof Sketch. By induction on the length of the mid-sequent-reduction sequence of φ to φ^*. □

The above proposition allows to define *the* Herbrand-sequent of a cut-free prenex $\mathbf{LK^j}$-proof φ which is *not in mid-sequent normal form* 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 mid-sequent reduction by instead collecting all used instances of the formulas of the end-sequent.

3.1 Partial Proofs and Partial Herbrand Sequents

In order to carry out a more fine-grained analysis we need partial Herbrand-sequents which are not tautological. Partial Herbrand-sequents are Herbrand-sequents of partial proofs. A partial proof of a certain set of formula occurrences consists of only those rules that operate on these occurrences. The juxtaposition rule plays a crucial role here: It replaces deleted binary rules to keep the scattered proof parts together in a single proof.

If s is a sequent in a proof and M is a set of formula occurrences, then $\mathrm{S}(s, M)$ denotes the sub-sequent of s consisting of the formula occurrences from M. A set M of formula occurrences 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. 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. If M is a closed set of formula occurrences, 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.

Definition 8 (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* s*, define*

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

(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 *in* φ'*.*
(a) If ρ *operates on* M*, 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 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 *in* φ_1, φ_2 *respectively.*
(a) If ρ *operates on* M*, 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*

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

(ii) If $M_1 = \emptyset$ *then*

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

(iii) If $M_2 = \emptyset$ *then*

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

Partial proofs as defined above are similar to the inner proofs of [7] 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 valid conclusion sequent.

Definition 9 (partial Herbrand-sequent) *Let* φ *be an* $\mathbf{LK}^{\mathrm{j}}$*-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

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

Note that a partial proof of the form $\varphi \mid \langle\mu\rangle$ for a formula occurrence μ is cut-free, therefore the computation of the Herbrand-sequent is possible. Partial Herbrand-sequents are no longer tautologies, but they contain the information which instances of a given formula have been used in the proof.

Example 1 *Define the formulas $X = (\forall x)(\forall y)(P(x,y) \to P(s(x),y))$ and $Y = (\forall x)(\forall y)(P(x,y) \to P(x,s(y)))$ which axiomatizes a two-dimensional grid where it is possible to move along both directions step-by-step. Let φ be the following proof (abbreviating $s^n(0)$ by n):*

$$\dfrac{\dfrac{P(0,0)\vdash P(0,0) \qquad \dfrac{\dfrac{P(0,1)\vdash P(0,1) \qquad \dfrac{\dfrac{P(1,1)\vdash P(1,1) \quad P(1,2)\vdash P(1,2)}{P(1,1), P(1,1)\to P(1,2)\vdash P(1,2)}\to:\mathrm{l}}{\dfrac{P(1,1), P(1,1)\to P(1,2)\vdash P(1,2)}{P(0,1), P(0,1)\to P(1,1), Y\vdash P(1,2)}\forall:\mathrm{l},\forall:\mathrm{l}}\to:\mathrm{l}}{P(0,1), X, Y\vdash P(1,2)}\forall:\mathrm{l},\forall:\mathrm{l}}{P(0,0), P(0,0)\to P(0,1), X, Y\vdash P(1,2)}\to:\mathrm{l}}{P(0,0), X, Y\vdash P(1,2)}\mathrm{c}:\mathrm{l},\forall:\mathrm{l},\forall:\mathrm{l}}{X, Y\vdash P(0,0)\to P(1,2)}\to:\mathrm{r}$$

Let μ be the occurrence of Y in the end-sequent. Then $\varphi \mid \langle\mu\rangle =$

$$\dfrac{\dfrac{\vdash P(0,0) \qquad \dfrac{\dfrac{P(0,1)\vdash \qquad \dfrac{\dfrac{\vdash P(1,1) \quad P(1,2)\vdash}{P(1,1)\to P(1,2)\vdash}\to:\mathrm{l}}{Y\vdash}\forall:\mathrm{l},\forall:\mathrm{l}}{P(0,1), Y\vdash}\mathrm{j}}{P(0,0)\to P(0,1), Y\vdash}\to:\mathrm{l}}{Y\vdash}\mathrm{c}:\mathrm{l},\forall:\mathrm{l},\forall:\mathrm{l}$$

and the partial Herbrand-sequent

$$\mathcal{H}(\mu) = P(0,0)\to P(0,1), P(1,1)\to P(1,2)\vdash$$

describes exactly the steps taken in the y-direction of the grid.

4 Characteristic Clause Sets

In order to prove that a short tautology can be read off from a proof with cuts, we will transform the instances of the end-sequent on one hand and the instances of the cut formulas on the other hand into clause normal forms. This

will allow to relate these two collections of instances to each other via the characteristic clause sets of the proof. These kind of clause sets have originally been studied in the context of cut-elimination: They are the main proof-theoretic tool of the cut-elimination method CERES (cut-elimination by resolution), introduced in [5]. In [2] this method has been extended to a sequent calculus augmented by explicit definitions and equality reasoning designed for the formalization of realistic mathematical proofs. An implementation [1] of this method has been used for the analysis of Fürstenberg's topological proof of the infinity of primes [1]. Another version of these clause sets, the proof profile, has been developed in the author's PhD thesis [9,10] and shown to be an interesting structural invariant under simple proof transformations in [11].

4.1 Clause Logic

A literal is an atom or a negated atom. A clause is a multiset of literals. Let $c = \{L_1, \ldots, L_k\}$ and $d = \{M_1, \ldots, M_n\}$ be clauses. We define the *merge* of c and d as $c \circ d := \{L_1, \ldots, L_k, M_1, \ldots, M_n\}$. Let C, D be clause sets. We define the *product* of C and D as $C \times D := \{c \circ d \mid c \in C, d \in D\}$. In order to transform quantifier-free formulas to clause sets we define a set of rewrite rules.

Definition 10 *Let F, G, H be quantifier-free formulas. We define the following 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 $\{\text{(I)}, \text{(DN)}, \text{(M1)}, \text{(M2)}, \text{(D1)}, \text{(D2)}\}$. Both $\mapsto_{\text{CNF}}$ and $\mapsto_{\text{DNF}}$ are strongly normalizing and confluent up to commutativity of $\wedge$ and $\vee$. We will speak about the resulting formulas as *conjunctive* respectively *disjunctive normal form* of a formula and we define corresponding clause sets:

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

Definition 11 (CNF, DNF) *Let F be a quantifier-free formula. Furthermore, let $\bigwedge_{i=1}^{k}\bigvee_{j=1}^{l_i} L_{i,j}$ be a normal form of F under $\mapsto_{\mathrm{CNF}}$ and $\bigvee_{i=1}^{n}\bigwedge_{j=1}^{m_i} M_{i,j}$ be a normal form of F under $\mapsto_{\mathrm{DNF}}$. Define the clause sets*

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

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

Accordingly, there are two different interpretations of a clause set as a propositional formula: as conjunction of disjunctions or as disjunction of conjunctions.

Definition 12 (CD, DC) *Let $C = \{c_1,\ldots,c_n\}$ be a clause set where $c_i = \{L_{i,1},\ldots L_{i,m_i}\}$ for $i = 1,\ldots,n$. Define the formulas*

$$\mathrm{CD}(C) := \bigwedge_{i=1}^{n}\bigvee_{j=1}^{m_i} L_{i,j} \qquad \textit{and} \qquad \mathrm{DC}(C) := \bigvee_{i=1}^{n}\bigwedge_{j=1}^{m_i} L_{i,j}$$

The reader can easily convince himself that, under the CD-interpretation, the logical meaning of $\cup$ is conjunction and the logical meaning of $\times$ is disjunction. Under the DC-interpretation it is the other way round.

Definition 13 (propositional subsumption) *Let C and D be clause sets. 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 $\mathrm{CD}(C)$ implies $\mathrm{CD}(D)$ and $\mathrm{DC}(D)$ implies $\mathrm{DC}(C)$.

Definition 14 (dualization) *For a literal L, $\overline{L}$ denotes the dual of L: 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 $\overline{L} := P(t_1,\ldots,t_n)$. For a clause $c = \{L_1,\ldots,L_n\}$, define $\overline{c} := \{\overline{L_1},\ldots,\overline{L_n}\}$ and for a clause set $C = \{c_1,\ldots,c_m\}$, define $\overline{C} := \{\overline{c_1},\ldots,\overline{c_m}\}$.*

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. For any literal L, any clause c and any clause set C: $\overline{\overline{L}} = L$, $\overline{\overline{c}} = c$ and $\overline{\overline{C}} = C$. Furthermore, dualization distributes over $\cup$ and $\times$, i.e. $\overline{C \cup D} = \overline{C} \cup \overline{D}$ and $\overline{C \times D} = \overline{C} \times \overline{D}$. Note that dualization is related to negation in the sense that $\neg\mathrm{CD}(C)$ is logically equivalent to $\mathrm{DC}(\overline{C})$ and $\neg\mathrm{DC}(C)$ is logically equivalent to $\mathrm{CD}(\overline{C})$.

4.2 The implicit part of a proof

It is a well-known observation – see e.g. [15, p. 79] – that in a sequent calculus proof two types of rules can be distinguished: The *implicit* rules, working on

ancestors of cut formulas and the *explicit* rules, working on ancestors of the end-sequent. Our analysis in this paper is based on this distinction. In this section we treat the implicit part, in Section 4.3 we treat the explicit part. We start with defining the characteristic clause sets of the implicit part.

Definition 15 (implicit clause sets) *Let φ be an $\mathbf{LK}^{\mathsf{j}}$-proof, let M be a closed set of formula occurrences. We define the clause sets $\mathcal{C}^{\mathrm{I}}_M(\varphi)$ and $\mathcal{C}^{\mathrm{IT}}_M(\varphi)$ by induction on φ:*

(1) φ is an axiom s. Let $\mu_1, \ldots, \mu_m$ be the literals[2] in $S(s, M)$. Define

$$\mathcal{C}^{\mathrm{IT}}_M(\varphi) := \{\{\mu_1, \ldots, \mu_m\}\} \qquad \mathcal{C}^{\mathrm{I}}_M(\varphi) := \begin{cases} \emptyset \text{ if } S(s, M) = s \\ \mathcal{C}^{\mathrm{IT}}_M(\varphi) \text{ otherwise} \end{cases}$$

For the rest of this definition let $X \in \{\mathrm{I}, \mathrm{IT}\}$ 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

$$\mathcal{C}^X_M(\varphi) := \mathcal{C}^X_{M'}(\varphi')$$

(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

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

(b) ρ does not operate on M. Then

$$\mathcal{C}^X_M(\varphi) := \mathcal{C}^X_{M_1}(\varphi_1) \times \mathcal{C}^X_{M_2}(\varphi_2)$$

Note that these sets are indeed clause sets because the axioms consist only of atomic formulas. For a proof φ we denote with $\mathrm{I}(\varphi)$ the ancestor-closure of the set of cut occurrences and abbreviate $\mathcal{C}^{\mathrm{I}}(\varphi) := \mathcal{C}^{\mathrm{I}}_{\mathrm{I}(\varphi)}(\varphi)$ and $\mathcal{C}^{\mathrm{IT}}(\varphi) := \mathcal{C}^{\mathrm{IT}}_{\mathrm{I}(\varphi)}(\varphi)$, Note that $\mathcal{C}^{\mathrm{I}}(\varphi)$, if interpreted as universally quantified conjunctive normal form, has the important property of being unsatisfiable (a fact that is at the core of the cut-elimination method CERES [5]). However, interpreted as a propositional conjunction of disjunctions, it is, in general, not unsatisfiable. The size of its (first-order) refutations is asymptotically the same as the size of the cut-free proofs [5], so it can be non-elementary [14].

Definition 16 (tautology-elimination) *Let C and D be clause sets. We write $C \leq^{\mathrm{T}} D$ if*

[2] Note that $m \leq 2$.

(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 $\mathrm{CD}(C)$ and $\mathrm{CD}(D)$ as well as $\mathrm{DC}(C)$ and $\mathrm{DC}(D)$ are logically equivalent because $D \setminus C$ contains only tautological clauses. Note that $\leq^{\mathrm{T}}$ is compatible with union and product, i.e. if $C \leq^{\mathrm{T}} C'$ and $D \leq^{\mathrm{T}} D'$ then $C \cup D \leq^{\mathrm{T}} C' \cup D'$ and $C \times D \leq^{\mathrm{T}} C' \times D'$. By induction on the size of the proof it is easy to show the following lemma.

Lemma 2 *Let* φ *be an* $\mathbf{LK}^{\mathbf{j}}$*-proof and let* M *be a closed set of formula occurrences. Then*

$$\mathcal{C}^{\mathrm{I}}_M(\varphi) \leq^{\mathrm{T}} \mathcal{C}^{\mathrm{IT}}_M(\varphi)$$

4.2.1 Inductive Characterization of Partial Herbrand Sequents

In order to describe the relation between $\mathcal{C}^{\mathrm{IT}}(\varphi)$ and the instances of the cut formulas of φ we introduce a characterization of the conjunctive normal form of a partial Herbrand-sequent, that is defined inductively over the structure of the proof.

Definition 17 *Let* μ *be an occurrence of a formula* F *in an* $\mathbf{LK}^{\mathbf{j}}$*-proof. 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 18 (Herbrand-Clauses) *Let* φ *be an* $\mathbf{LK}^{\mathbf{j}}$*-proof and let* μ *be a formula occurrence in* φ*. 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:

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

Lemma 3 *Let φ be an $\mathbf{LK}^{\mathsf{j}}$-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. If φ is an axiom sequent s, then $\mathcal{HC}(\mu) = \{\{[\mu]\}\} = \mathrm{CNF}(\mathcal{H}(\mu))$ because axioms are atomic. If φ ends with a rule ρ, assume first that μ occurs in the context of ρ. Then μ has a unique immediate ancestor ν and $\mathcal{HC}(\mu) = \mathcal{HC}(\nu)$. But then also $\mathcal{H}(\mu) = \mathcal{H}(\nu)$ because the used instances in the partial proofs $\varphi \mid \langle\mu\rangle$ and $\varphi \mid \langle\nu\rangle$ are the same (apply Lemma 1).

So, for the rest of this proof, we assume that μ is the main occurrence of ρ and make a case distinction on the type of ρ: If $\rho = \mathrm{w} : \mathrm{l}$ then $\mathcal{HC}(\mu) = \{\emptyset\}$ and – writing s for the conclusion sequent of ρ – we have $\varphi \mid \langle\mu\rangle =$

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

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

If $\rho = \mathrm{c} : \mathrm{l}$, then μ has two ancestors ν_1 and ν_2. By induction hypothesis

$$\mathcal{HC}(\mu) \;=\; \mathcal{HC}(\nu_1) \times \mathcal{HC}(\nu_2) \;\trianglelefteq\; \mathrm{CNF}(\mathcal{H}(\nu_1)) \times \mathrm{CNF}(\mathcal{H}(\nu_2))$$

and it remains to show $\mathrm{CNF}(\mathcal{H}(\nu_1)) \times \mathrm{CNF}(\mathcal{H}(\nu_2)) \;\trianglelefteq\; \mathrm{CNF}(\mathcal{H}(\mu))$.

(1) Assume μ is quantifier-free. If μ is not used, then both ν_1, ν_2 are not used and $\mathrm{CNF}(\mathcal{H}(\nu_1)) \times \mathrm{CNF}(\mathcal{H}(\nu_2)) = \{\emptyset\} \times \{\emptyset\} = \{\emptyset\} = \mathrm{CNF}(\mathcal{H}(\mu))$. Now, abbreviate $C := \mathrm{CNF}([\mu]) = \mathrm{CNF}([\nu_i])$. If μ is used, then at least one of ν_1, ν_2 is used and both $C \times \{\emptyset\} \trianglelefteq C$ and $C \times C \trianglelefteq C$.

(2) If μ contains a quantifier, then $\mathcal{H}(\mu) = \mathrm{set}(\mathcal{Q}_{\mathrm{p}}(\varphi \mid \langle\mu\rangle))$ and $\mathcal{H}(\nu_i) = \mathrm{set}(\mathcal{Q}_{\mathrm{p}}(\varphi \mid \langle\nu_i\rangle))$, but $\mathcal{Q}_{\mathrm{p}}(\varphi \mid \langle\mu\rangle) = \mathcal{Q}_{\mathrm{p}}(\varphi \mid \langle\nu_1\rangle) \circ \mathcal{Q}_{\mathrm{p}}(\varphi \mid \langle\nu_2\rangle)$ and by set-contraction of possible common instances in $\mathcal{H}(\nu_1)$ and $\mathcal{H}(\nu_2)$ we obtain

$$\mathrm{CNF}(\mathcal{H}(\nu_1)) \times \mathrm{CNF}(\mathcal{H}(\nu_2)) \;\trianglelefteq\; \mathrm{CNF}(\mathcal{H}(\mu)).$$

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

If $\rho = \forall\mathrm{:l}$ then μ has a unique immediate ancestor ν and by induction hypothesis

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

In this case $\mathcal{H}(\mu) = \mathcal{H}(\nu)$ because $\mathcal{H}(\mu) = \mathrm{set}(\mathrm{s}_{\mathrm{p}}(\varphi \mid \langle\mu\rangle) \;\circ\; \mathcal{Q}_{\mathrm{p}}(\varphi \mid \langle\mu\rangle))$ and $\mathcal{H}(\nu) = \mathrm{set}(\mathrm{s}_{\mathrm{p}}(\varphi \mid \langle\nu\rangle) \;\circ\; \mathcal{Q}_{\mathrm{p}}(\varphi \mid \langle\nu\rangle))$ by Lemma 1. Furthermore, μ

contains a quantifier, so $\mathrm{s_p}(\varphi \mid \langle\mu\rangle) = \vdash$ and if ν also contains a quantifier then $\mathrm{s_p}(\varphi \mid \langle\nu\rangle) = \vdash$ 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 the same argument applies.

For a propositional rule ρ it is easily checked that the CNF of the active occurrences is preserved using – by definition of $\mathcal{HC}$ – the product $\times$ for two auxiliary occurrences in the same sequent and the union $\cup$ for two auxiliary occurrences in different sequents. $\square$

4.2.2 Subsumption

The following Lemma is the technical key in the treatment of the implicit part because it establishes the connection between the global $\mathcal{C}^{\mathrm{IT}}$ and the local and inductively defined $\mathcal{HC}$. We show that, modulo propositional subsumption, the $\mathcal{C}^{\mathrm{IT}}$-clause set can be constructed by successively multiplying with $\mathcal{HC}(\omega)$ for the cut occurrence ω immediately above its cut. This constitutes the encoding of the partial proofs of all cuts into the single global structure $\mathcal{C}^{\mathrm{IT}}$.

Lemma 4 *Let φ be an $\mathbf{LK}^{\mathsf{j}}$-proof and ν be an end occurrence. Then*

$$\mathcal{C}^{\mathrm{IT}}_{\mathrm{I}(\varphi)\cup\langle\nu\rangle}(\varphi) \;\trianglelefteq\; \mathcal{C}^{\mathrm{IT}}(\varphi) \times \mathcal{HC}(\nu)$$

Proof. By induction on φ we show the following more general statement: Let M be a set of terminal occurrences and N be a set of end occurrences s.t. $M \cap N = \emptyset$. Then

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

If φ is an axiom s, then $\mathcal{C}^{\mathrm{IT}}_{\langle M\uplus N\rangle}(\varphi) = \{\mathrm{S}(s,M)\circ\mathrm{S}(s,N)\}$, $\mathcal{C}^{\mathrm{IT}}_{\langle M\rangle}(\varphi) = \{\mathrm{S}(s,M)\}$ and $\between_{\nu\in N}\mathcal{HC}(\nu) = \{\mathrm{S}(s,N)\}$. So, for the rest of this proof, 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) All $\nu \in N$ occur in the context of ρ.
  (a) If ρ is a unary rule, then by the induction hypothesis

$$\mathcal{C}^{\mathrm{IT}}_{\langle M'\uplus N'\rangle}(\varphi') \;\trianglelefteq\; \mathcal{C}^{\mathrm{IT}}_{\langle M'\rangle}(\varphi') \between_{\nu\in N'} \mathcal{HC}(\nu),$$

  $\mathcal{C}^{\mathrm{IT}}_{\langle M'\uplus N'\rangle}(\varphi') = \mathcal{C}^{\mathrm{IT}}_{\langle M\uplus N\rangle}(\varphi)$, $\mathcal{C}^{\mathrm{IT}}_{\langle M'\rangle}(\varphi') = \mathcal{C}^{\mathrm{IT}}_{\langle M\rangle}(\varphi)$ immediately by definition and $\between_{\nu\in N}\mathcal{HC}(\nu) = \between_{\nu\in N'}\mathcal{HC}(\nu)$ because each $\nu \in N$ has exactly one immediate ancestor $\nu' \in N'$, so $\mathcal{HC}(\nu) = \mathcal{HC}(\nu')$.

(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

$$\mathcal{C}^{\mathrm{IT}}_{\langle M_1 \uplus N_1 \rangle}(\varphi_1) \diamond \mathcal{C}^{\mathrm{IT}}_{\langle M_2 \uplus N_2 \rangle}(\varphi_2) \trianglelefteq (\mathcal{C}^{\mathrm{IT}}_{\langle M_1 \rangle}(\varphi_1) \bigtimes_{\nu \in N_1} \mathcal{HC}(\nu)) \diamond (\mathcal{C}^{\mathrm{IT}}_{\langle M_2 \rangle}(\varphi_2) \bigtimes_{\nu \in N_2} \mathcal{HC}(\nu)).$$

But by definition of $\mathcal{C}^{\mathrm{IT}}_{\langle M \uplus N \rangle}(\varphi)$ and as $(A \times B) \cup (C \times D) \trianglelefteq (A \cup C) \times B \times D$ we obtain

$$\mathcal{C}^{\mathrm{IT}}_{\langle M \uplus N \rangle}(\varphi) \trianglelefteq (\mathcal{C}^{\mathrm{IT}}_{\langle M_1 \rangle}(\varphi_1) \diamond \mathcal{C}^{\mathrm{IT}}_{\langle M_2 \rangle}(\varphi_2)) \bigtimes_{\nu \in N_1} \mathcal{HC}(\nu) \bigtimes_{\nu \in N_2} \mathcal{HC}(\nu).$$

By definition of $\mathcal{C}^{\mathrm{IT}}_{\langle M \rangle}(\varphi)$ and the observation that all $\nu \in N$ have exactly one ancestor we obtain

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

(2) The rule ρ has a main occurrence $\nu_0 \in N$. 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 and the result follows from the induction hypothesis and the observation that $\bigtimes_{\nu \in N'} \mathcal{HC}(\nu) = \bigtimes_{\nu \in N} \mathcal{HC}(\nu)$ because $\mathcal{HC}(\nu_0) = \{\emptyset\}$.
   (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 they occur in the same sequent, then ρ is unary and the result follows from the induction hypothesis and the observation that $\bigtimes_{\nu \in N'} \mathcal{HC}(\nu) = \bigtimes_{\nu \in N} \mathcal{HC}(\nu)$ because $\mathcal{HC}(\nu_0) = \mathcal{HC}(\nu_0^1) \times \mathcal{HC}(\nu_0^2)$.
   (d) If ν_0 has exactly two immediate ancestors ν_0^1, ν_0^2 and they 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 the induction hypothesis

$$\mathcal{C}^{\mathrm{IT}}_{\langle M_1 \uplus N_1 \rangle}(\varphi_1) \cup \mathcal{C}^{\mathrm{IT}}_{\langle M_2 \uplus N_2 \rangle}(\varphi_2) \trianglelefteq (\mathcal{C}^{\mathrm{IT}}_{\langle M_1 \rangle}(\varphi_1) \bigtimes_{\nu \in N_1} \mathcal{HC}(\nu)) \cup (\mathcal{C}^{\mathrm{IT}}_{\langle M_2 \rangle}(\varphi_2) \bigtimes_{\nu \in N_2} \mathcal{HC}(\nu)).$$

But by definition of $\mathcal{C}^{\mathrm{IT}}_{\langle M \uplus N \rangle}(\varphi)$, by separating ν_0^1 and ν_0^2 from the rest of N_1, N_2 and applying $(A \times B) \cup (C \times D) \trianglelefteq (A \cup C) \times B \times D$ we obtain

$$\mathcal{C}^{\mathrm{IT}}_{\langle M \uplus N \rangle}(\varphi) \trianglelefteq ((\mathcal{C}^{\mathrm{IT}}_{\langle M_1 \rangle}(\varphi_1) \times \mathcal{HC}(\nu_0^1)) \cup (\mathcal{C}^{\mathrm{IT}}_{\langle M_2 \rangle}(\varphi_2) \times \mathcal{HC}(\nu_0^2))) \bigtimes_{\nu \in N_1 \setminus \{\nu_0^1\}} \mathcal{HC}(\nu) \bigtimes_{\nu \in N_2 \setminus \{\nu_0^2\}} \mathcal{HC}(\nu).$$

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

$$\bigtimes_{\nu \in N_1 \setminus \{\nu_0^1\}} \mathcal{HC}(\nu) \bigtimes_{\nu \in N_2 \setminus \{\nu_0^2\}} \mathcal{HC}(\nu) = \bigtimes_{\nu \in N \setminus \{\nu_0\}} \mathcal{HC}(\nu),$$

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

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

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

$$\mathcal{C}^{\mathrm{IT}}_{\langle M \uplus N \rangle}(\varphi) \trianglelefteq \mathcal{C}^{\mathrm{IT}}_{\langle M \rangle}(\varphi) \curlyvee_{\nu \in N} \mathcal{HC}(\nu).$$

□

We are now ready to prove the main lemma on the implicit part: $\mathcal{C}^{\mathrm{IT}}(\varphi)$ 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.

Lemma 5 *Let φ be a prenex $\mathbf{LK}^{\mathsf{j}}$-proof and let $\{\omega_1^+, \omega_1^-, \ldots, \omega_n^+, \omega_n^-\}$ be the cut occurrences of φ. Then*

$$\mathcal{C}^{\mathrm{IT}}(\varphi) \trianglelefteq \curlyvee_{i=1}^{n}(\mathrm{CNF}(\mathcal{H}(\omega_i^-)) \cup \mathrm{CNF}(\mathcal{H}(\omega_i^+)))$$

Proof. By Lemma 3 it suffices to show

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

We proceed by induction on n. If $n = 0$ then φ does not contain cuts, $\mathcal{C}^{\mathrm{IT}}(\varphi) = \{\emptyset\}$ 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 $\mathcal{C}^{\mathrm{IT}}(\varphi) = \mathcal{C}^{\mathrm{IT}}(\psi[\varphi])$ for each cut-free context $\psi[]$.

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 cut occurrences 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

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

Applying Lemma 4 and the induction hypothesis we obtain

$$\mathcal{C}^{\mathrm{IT}}(\varphi) \trianglelefteq \Big((\curlyvee_{i=1}^{k}(\mathcal{HC}(\omega_i^+) \cup \mathcal{HC}(\omega_i^-))) \times \mathcal{HC}(\omega_n^+)\Big) \cup \\ \Big((\curlyvee_{i=k+1}^{n-1}(\mathcal{HC}(\omega_i^+) \cup \mathcal{HC}(\omega_i^-))) \times \mathcal{HC}(\omega_n^-)\Big)$$

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

If ρ is not a cut, then

$$\mathcal{C}^{\mathrm{IT}}(\varphi) = \mathcal{C}^{\mathrm{IT}}(\varphi_1) \times \mathcal{C}^{\mathrm{IT}}(\varphi_2)$$

and the result follows immediately from the induction hypothesis. □

4.3 The explicit part of a proof

In this section we will treat the explicit part of a proof, leading to a description of the instances of formulas of the end-sequent by characteristic clause sets $\mathcal{C}^{\mathrm{E}}$ and $\mathcal{C}^{\mathrm{ET}}$.

Definition 19 (explicit clause sets) *Let φ be an* $\mathbf{LK}^{\mathsf{j}}$*-proof, let N be a closed set of formula occurrences. We define the clause sets $\mathcal{C}^{\mathrm{E}}_N(\varphi)$ and $\mathcal{C}^{\mathrm{ET}}_N(\varphi)$ by induction on φ:*

(1) φ is an axiom s. Let $\nu_1, \ldots, \nu_n$ be the literals[3] *in $S(s, N)$. Define*

$$\mathcal{C}^{\mathrm{ET}}_N(\varphi) := \{\{\nu_1\}, \ldots, \{\nu_n\}\} \qquad \mathcal{C}^{\mathrm{E}}_N(\varphi) := \begin{cases} \{\emptyset\} \text{ if } S(s,N) = s \\ \mathcal{C}^{\mathrm{ET}}_N(\varphi) \text{ otherwise} \end{cases}$$

For the rest of this definition let $X \in \{\mathrm{E}, \mathrm{ET}\}$ 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

$$\mathcal{C}^X_N(\varphi) := \mathcal{C}^X_{N'}(\varphi')$$

(3) φ ends with a binary rule ρ. Let φ_1 and φ_2 be the immediate sub-proofs 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

$$\mathcal{C}^X_N(\varphi) := \mathcal{C}^X_{N_1}(\varphi_1) \times \mathcal{C}^X_{N_2}(\varphi_2)$$

(b) ρ does not operate on N. Then

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

For a proof φ we denote with $\mathrm{E}(\varphi)$ the closure of the set of end occurrences and abbreviate $\mathcal{C}^{\mathrm{E}}(\varphi) := \mathcal{C}^{\mathrm{E}}_{\mathrm{E}(\varphi)}(\varphi)$ and $\mathcal{C}^{\mathrm{ET}}(\varphi) := \mathcal{C}^{\mathrm{ET}}_{\mathrm{E}(\varphi)}(\varphi)$.

[3] Note that $n \leq 2$.

Definition 20 (resolution) *Let C and D be clause sets. 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 clause set E with $C = E \uplus \{c\}$ and $D = E \uplus \{d_1, d_2\}$. We write $\leq^{\mathrm{R}}$ for the reflexive and transitive closure of $\leq^{\mathrm{R}^1}$.*

The relation $\leq^{\mathrm{R}^1}$ corresponds to application of propositional resolution (i.e. without unification). For $C \leq^{\mathrm{R}} D$ the formulas $\mathrm{CD}(C)$ and $\mathrm{CD}(D)$ as well as $\mathrm{DC}(C)$ and $\mathrm{DC}(D)$ are logically equivalent. Note that $\leq^{\mathrm{R}}$ is compatible with $\cup$ and $\times$, i.e. if $C \leq^{\mathrm{R}} C'$ and $D \leq^{\mathrm{R}} D'$ then $C \cup D \leq^{\mathrm{R}} C' \cup D'$ and $C \times D \leq^{\mathrm{R}} C' \times D'$. By induction on the size of the proof it is easy to show the following lemma.

Lemma 6 *Let φ be an $\mathbf{LK}^{\mathsf{j}}$-proof and let N be a closed set of formula occurrences. Then*

$$\mathcal{C}^{\mathrm{E}}_N(\varphi) \leq^{\mathrm{R}} \mathcal{C}^{\mathrm{ET}}_N(\varphi)$$

4.3.1 Subsumption

We will consider the partial proof $\varphi \mid \mathrm{E}(\varphi)$ of the end-sequent (i.e. we drop all implicit rules) and relate its mid-sequent to the $\mathcal{C}^{\mathrm{ET}}$-clause set of the original proof. First we show that dropping the implicit part does not change the clause set of the explicit part.

Lemma 7 *Let φ be an $\mathbf{LK}$-proof. Then*

$$\mathcal{C}^{\mathrm{ET}}(\varphi) = \mathcal{C}^{\mathrm{ET}}(\varphi \mid \mathrm{E}(\varphi))$$

Proof Sketch. The following stronger statement is easily shown by induction on φ: Let N be a set of end occurrences, then

$$\mathcal{C}^{\mathrm{ET}}_{\langle N \rangle}(\varphi) = \mathcal{C}^{\mathrm{ET}}(\varphi \mid \langle N \rangle).$$

□

We will now show that the disjunctive normal form of the end-sequent of a cut-free propositional proof subsumes $\mathcal{C}^{\mathrm{ET}}$. This lemma will later be applied to the upper part of a proof in mid-sequent normal form.

Lemma 8 *Let φ be a cut-free $\mathbf{LK}^{\mathsf{j}}$-proof with quantifier-free end-sequent s. Then*

$$\mathrm{DNF}(s) \trianglelefteq \mathcal{C}^{\mathrm{ET}}(\varphi)$$

Proof. By induction on φ: If φ is an axiom sequent then $\mathrm{DNF}(s) = \mathcal{C}^{\mathrm{ET}}(\varphi)$. 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, $\mathcal{C}^{\mathrm{ET}}(\varphi) = \mathcal{C}^{\mathrm{ET}}(\varphi')$ and by using

the induction hypothesis it remains to show that $\mathrm{DNF}(s) \trianglelefteq \mathrm{DNF}(s')$. For the unary propositional rules, 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 clause sets C, D and $D \cup C \trianglelefteq D$. If ρ is a contraction, then $\mathrm{DNF}(s) = D \cup C = D \cup C \cup C = \mathrm{DNF}(s')$.

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 $\mathcal{C}^{\mathrm{ET}}(\varphi) = \mathcal{C}^{\mathrm{ET}}(\varphi_1) \cup \mathcal{C}^{\mathrm{ET}}(\varphi_2)$ 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, it has the form:

$$\dfrac{\begin{matrix}(\varphi_1) & (\varphi_2) \\ \Gamma \vdash \Delta, A & \Pi \vdash \Lambda, B\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda, A \wedge B}\ \wedge\text{: r}$$

where

$$\mathcal{C}^{\mathrm{ET}}(\varphi) = \mathcal{C}^{\mathrm{ET}}(\varphi_1) \times \mathcal{C}^{\mathrm{ET}}(\varphi_2).$$

Furthermore

$$\mathrm{DNF}(s) = \mathrm{DNF}(\Gamma \vdash \Delta) \cup \mathrm{DNF}(\Pi \vdash \Lambda) \cup \mathrm{DNF}(\vdash A \wedge B),$$
$$\mathrm{DNF}(s_1) = \mathrm{DNF}(\Gamma \vdash \Delta) \cup \mathrm{DNF}(\vdash A) \text{ and}$$
$$\mathrm{DNF}(s_2) = \mathrm{DNF}(\Pi \vdash \Lambda) \cup \mathrm{DNF}(\vdash B).$$

We will now show that $\forall d \in \mathcal{C}^{\mathrm{ET}}(\varphi)\ \exists c \in \mathrm{DNF}(s)$ s.t. $\mathrm{set}(c) \subseteq \mathrm{set}(d)$. Let $d = d_1 \circ d_2$ with $d_1 \in \mathcal{C}^{\mathrm{ET}}(\varphi_1)$ and $d_2 \in \mathcal{C}^{\mathrm{ET}}(\varphi_2)$. 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 $\mathrm{set}(c_i) \subseteq \mathrm{set}(d_i)$ for $i = 1, 2$. So for both c_i we have $\mathrm{set}(c_i) \subseteq \mathrm{set}(d)$. 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 $c_1 \circ c_2 \in \mathrm{DNF}(\vdash A) \times \mathrm{DNF}(\vdash B) = \mathrm{DNF}(\vdash A \wedge B) \subseteq \mathrm{DNF}(s)$ and also $\mathrm{set}(c_1 \circ c_2) \subseteq \mathrm{set}(d)$. For the other binary rules we proceed analogously. □

The main lemma on the explicit part now establishes a subsumption relation between $\mathcal{C}^{\mathrm{ET}}$ and the instances of the end-sequent in a way that is analogous to the relation in the implicit part shown in Lemma 5.

Lemma 9 *Let φ be a prenex* **LK***-proof. Then*

$$\mathcal{C}^{\mathrm{ET}}(\varphi) \trianglerighteq \mathrm{DNF}(\mathcal{H}(\varphi \mid \mathrm{E}(\varphi)))$$

Proof. Let φ' be the $\mathbf{LK}^{\mathsf{j}}$-proof $\varphi \mid \mathrm{E}(\varphi)$, then by Lemma 7 we have $\mathcal{C}^{\mathrm{ET}}(\varphi) = \mathcal{C}^{\mathrm{ET}}(\varphi')$. Let φ'' be a mid-sequent normal form of φ'. Mid-sequent reduction does not change the ET-clause set, so $\mathcal{C}^{\mathrm{ET}}(\varphi'') = \mathcal{C}^{\mathrm{ET}}(\varphi')$ and also $\mathcal{H}(\varphi'') = \mathcal{H}(\varphi')$. As φ'' is a mid-sequent normal form, there is a lowest propositional or

juxtaposition rule ρ s.t. 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 $\mathcal{C}^{\mathrm{ET}}(\varphi'') = \mathcal{C}^{\mathrm{ET}}(\chi)$ and $\mathcal{H}(\varphi'') = \mathcal{H}(\chi)$.

Let s be the end-sequent of χ. By shifting weakening rules downwards, we obtain a proof χ' of $s' = \mathrm{U}(s)$ with $\mathcal{C}^{\mathrm{ET}}(\chi') = \mathcal{C}^{\mathrm{ET}}(\chi)$. By adding contractions to the end of χ' we obtain a proof χ'' of $s'' = \mathrm{set}(\mathrm{U}(s))$ with $\mathcal{C}^{\mathrm{ET}}(\chi'') = \mathcal{C}^{\mathrm{ET}}(\chi')$. Applying now Lemma 8 to χ'' gives $\mathcal{C}^{\mathrm{ET}}(\chi'') \trianglerighteq \mathrm{DNF}(s'')$ but by definition s'' is the Herbrand-sequent $\mathcal{H}(\chi) = \mathcal{H}(\varphi')$ which concludes the proof. □

5 The Extended Herbrand Theorem

Finally, we will now observe a simple duality between $\mathcal{C}^{\mathrm{E}}(\varphi)$ and $\mathcal{C}^{\mathrm{I}}(\varphi)$ which will allow to connect the results of the two previous sections in order to form a short tautology from the instances of the cut formulas and the end-sequent.

Lemma 10 (Duality) *Let φ be an* **LK***-proof. Then*

$$\overline{\mathcal{C}^{\mathrm{I}}(\varphi)} = \mathcal{C}^{\mathrm{E}}(\varphi) \quad \textit{and} \quad \overline{\mathcal{C}^{\mathrm{E}}(\varphi)} = \mathcal{C}^{\mathrm{I}}(\varphi)$$

Proof. We call a partition $M \uplus N$ of the formula occurrences of φ *proper* if both M and N are closed and all cut occurrences are in M. We will show the following stronger statement by induction on φ: Let $M \uplus N$ be a proper partition of φ. Then

$$\overline{\mathcal{C}^{\mathrm{I}}_M(\varphi)} = \mathcal{C}^{\mathrm{E}}_N(\varphi) \quad \text{and} \quad \overline{\mathcal{C}^{\mathrm{E}}_N(\varphi)} = \mathcal{C}^{\mathrm{I}}_M(\varphi)$$

If φ is an axiom, there are three cases: (1) If $N = \emptyset$ then $\mathcal{C}^{\mathrm{E}}_N(\varphi) = \emptyset$ and $\mathcal{C}^{\mathrm{I}}_M(\varphi) = \emptyset$. (2) If $M = \emptyset$ then $\mathcal{C}^{\mathrm{I}}_M(\varphi) = \{\emptyset\}$ and $\mathcal{C}^{\mathrm{E}}_N(\varphi) = \{\emptyset\}$. (3) If both $M \neq \emptyset$ and $N \neq \emptyset$, then there is a literal L s.t. $\mathcal{C}^{\mathrm{I}}_M(\varphi) = \{\{L\}\}$ and $\mathcal{C}^{\mathrm{E}}_N(\varphi) = \{\{\overline{L}\}\}$.

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

$$\mathcal{C}^{\mathrm{I}}_M(\varphi) \;=\; \mathcal{C}^{\mathrm{I}}_{M_1}(\varphi_1) \cup \mathcal{C}^{\mathrm{I}}_{M_2}(\varphi_2) \quad \text{and} \quad \mathcal{C}^{\mathrm{E}}_N(\varphi) \;=\; \mathcal{C}^{\mathrm{E}}_{N_1}(\varphi_1) \cup \mathcal{C}^{\mathrm{E}}_{N_2}(\varphi_2)$$

or

$$\mathcal{C}^{\mathrm{I}}_M(\varphi) \;=\; \mathcal{C}^{\mathrm{I}}_{M_1}(\varphi_1) \times \mathcal{C}^{\mathrm{I}}_{M_2}(\varphi_2) \quad \text{and} \quad \mathcal{C}^{\mathrm{E}}_N(\varphi) \;=\; \mathcal{C}^{\mathrm{E}}_{N_1}(\varphi_1) \times \mathcal{C}^{\mathrm{E}}_{N_2}(\varphi_2).$$

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_2. The result then follows from distributing dualization over $\times$ and $\cup$. $\square$

Definition 21 *Let φ be a prenex proof with cut formulas $C_1, \ldots, C_n$. For all $i \in \{1, \ldots, n\}$ let $C_{i,1}, \ldots, C_{i,k_i}$ ($D_{i,1}, \ldots, D_{i,l_i}$) be the used quantifier-free instances of the positive (negative) occurrence of C_i. We define the formula*

$$\mathcal{H}^{\mathrm{I}}(\varphi) := \bigwedge_{i=1}^{n} \Big((\bigvee_{j=1}^{k_i} C_{i,j}) \to (\bigwedge_{j=1}^{l_i} D_{i,j}) \Big)$$

Definition 22 *Let φ be a prenex proof of $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$. For $i \in \{1, \ldots, m\}$ ($i \in \{1, \ldots, n\}$) let $A_{i,1}, \ldots, A_{i,k_i}$ ($B_{i,1}, \ldots, B_{i,l_i}$) be the used quantifier-free instances of A_i (B_i). We define the formula*

$$\mathcal{H}^{\mathrm{E}}(\varphi) := (\bigwedge_{i=1}^{m} \bigwedge_{j=1}^{k_i} A_{i,j}) \to (\bigvee_{i=1}^{n} \bigvee_{j=1}^{l_i} B_{i,j})$$

For the case of cut-free proofs, $\mathcal{H}^{\mathrm{E}}(\varphi)$ is the mid-sequent of φ. Note that, in general, neither $\mathcal{H}^{\mathrm{E}}(\varphi)$ nor $\mathcal{H}^{\mathrm{I}}(\varphi)$ is a tautology, it is only by combining both that a tautology can be obtained.

Theorem 1 (Extended Herbrand) *Let φ be a prenex* **LK***-proof. Then*

$$\mathcal{H}^{\mathrm{I}}(\varphi) \to \mathcal{H}^{\mathrm{E}}(\varphi)$$

is a tautology.

Proof. Let $\omega_1^-, \omega_1^+, \ldots, \omega_n^-, \omega_n^+$ be the cut occurrences of φ. The conjunctive normal form of $\neg\mathcal{H}^{\mathrm{I}}(\varphi)$ is

$$\mathrm{CD}(\bigtimes_{i=1}^{n}(\mathrm{CNF}(\mathcal{H}(\omega_i^-)) \cup \mathrm{CNF}(\mathcal{H}(\omega_i^+)))),$$

so $\mathcal{H}^{\mathrm{I}}(\varphi)$ is equivalent to

$$\neg\mathrm{CD}(\bigtimes_{i=1}^{n}(\mathrm{CNF}(\mathcal{H}(\omega_i^-)) \cup \mathrm{CNF}(\mathcal{H}(\omega_i^+)))).$$

By Lemma 5 the above formula implies $\neg\mathrm{CD}(\mathcal{C}^{\mathrm{IT}}(\varphi))$ which – by Lemma 2 – is equivalent to $\neg\mathrm{CD}(\mathcal{C}^{\mathrm{I}}(\varphi))$. Due to the duality between $\mathcal{C}^{\mathrm{I}}$ and $\mathcal{C}^{\mathrm{E}}$ (Lemma 10) we have the equivalence

$$\neg\mathrm{CD}(\mathcal{C}^{\mathrm{I}}(\varphi)) \Leftrightarrow \mathrm{DC}(\mathcal{C}^{\mathrm{E}}(\varphi)).$$

But $\mathrm{DC}(\mathcal{C}^{\mathrm{E}}(\varphi))$ is – by Lemma 6 – equivalent to $\mathrm{DC}(\mathcal{C}^{\mathrm{ET}}(\varphi))$ which – by Lemma 9 – implies $\mathrm{DC}(\mathrm{DNF}(\mathcal{H}^{\mathrm{E}}(\varphi)))$ which is finally equivalent to $\mathcal{H}^{\mathrm{E}}(\varphi)$. $\square$

Clearly, the number of logical symbols in the implication $\mathcal{H}^{\mathrm{I}}(\varphi) \to \mathcal{H}^{\mathrm{E}}(\varphi)$ is linearly bounded in the number of rules in φ. Also note that this formula can easily be read off from the proof without the need of using the clause set formalism.

Example 2 *In order to illustrate the structure of these short tautologies, we consider a sequence $(\tau_k)_{k\geq 0}$ of proofs (from [4]) where τ_k proves the sequent $T, (\forall x)P(f(x), x) \vdash (\forall x)P(f^{2^k}(x), x)$ and $T = (\forall x)(\forall y)(\forall z)((P(x, y) \wedge P(y, z)) \to P(x, z))$ states the transitivity of P. Note that all Herbrand-disjunctions of these sequents have an exponential number of disjuncts (and all cut-free proofs therefore an exponential number of rules). We define short proofs with cuts as $\tau_0 :=$*

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

and for $k > 0$ we define $\tau_k :=$

$$\dfrac{\dfrac{\overset{(\tau_{k-1})}{T, (\forall x)P(f(x), x) \vdash (\forall x)P(f^{2^{k-1}}(x), x)} \quad \overset{(\psi_k)}{(\forall x)P(f^{2^{k-1}}(x), x), T \vdash (\forall x)P(f^{2^k}(x), x)}}{T, T, (\forall x)P(f(x), x) \vdash (\forall x)P(f^{2^k}(x), x)}}{T, (\forall x)P(f(x), x) \vdash (\forall x)P(f^{2^k}(x), x)}\ \mathrm{c} : \mathrm{l}$$

where $\psi_k :=$

$$\dfrac{\dfrac{\overset{(\chi_k)}{P(f^{2^k}(\alpha_k), f^{2^{k-1}}(\alpha_k)), P(f^{2^{k-1}}(\alpha_k), \alpha_k), T \vdash P(f^{2^k}(\alpha_k), \alpha_k)}}{(\forall x)P(f^{2^{k-1}}(x), x), T \vdash P(f^{2^k}(\alpha_k), \alpha_k)}\ \forall\text{: r}}{(\forall x)P(f^{2^{k-1}}(x), x), T \vdash (\forall x)P(f^{2^k}(x), x)}\ \mathrm{c} : \mathrm{l}, \forall\text{: l}, \forall\text{: l}$$

and χ_k consists of the obvious application of transitivity. We then have

$$\mathcal{H}^{\mathrm{I}}(\tau_k) = \bigwedge_{i=1}^{k} \Big(P(f^{2^{i-1}}(\alpha_{i-1}), \alpha_{i-1}) \to (P(f^{2^i}(\alpha_i), f^{2^{i-1}}(\alpha_i)) \wedge P(f^{2^{i-1}}(\alpha_i), \alpha_i))\Big)$$

where each cut induces one implication (and the empty conjunction is $\top$). $\mathcal{H}^{\mathrm{E}}(\tau_k)$ contains $k - 1$ instances of transitivity plus one instance for each of the two universally quantified atoms in the end-sequent; $\mathcal{H}^{\mathrm{E}}(\tau_k) =$

$$\left(\begin{array}{l} \bigwedge_{i=1}^{k} \Big((P(f^{2^i}(\alpha_i), f^{2^{i-1}}(\alpha_i)) \wedge P(f^{2^{i-1}}(\alpha_i), \alpha_i)) \to P(f^{2^i}(\alpha_i), \alpha_i)\Big) \\ \wedge\ P(f(\alpha_0), \alpha_0) \end{array}\right) \\ \to P(f^{2^k}(\alpha_k), \alpha_k)$$

The reader is invited to follow the logical implications from $P(f(\alpha_0), \alpha_0)$ in the explicit part via an alternation of the implications induced by the cuts and the instances of transitivity to the atom $P(f^{2^k}(\alpha_k), \alpha_k)$. Observe the crucial interplay between $\mathcal{H}^{\mathrm{E}}(\tau_k)$ and $\mathcal{H}^{\mathrm{I}}(\tau_k)$ for proving the implication $\mathcal{H}^{\mathrm{I}}(\tau_k) \to \mathcal{H}^{\mathrm{E}}(\tau_k)$.

6 Cut-Elimination on Short Tautologies

The extended Herbrand theorem proved above will now be used to describe how a proof is changed by cut-elimination. A cut-elimination sequence induces a sequence of tautologies of the above form, the last of which is the Herbrand-sequent of the cut-free proof, containing only instances of the end-sequent. This sequence of short tautologies thus allows to observe how the Herbrand-sequent is computed step-by-step. We will show that the knowledge of only the first-order substitutions applied during cut-elimination is already sufficient for computing the Herbrand-sequent of the cut-free proof.

A substitution is a function mapping variables to terms. Given a substitution σ, the set of variables changed by σ is called the domain of σ.

Definition 23 *Let $\sigma_1, \ldots, \sigma_n$ be substitutions having the same domain. Then the set $\sigma := \{\sigma_1, \ldots, \sigma_n\}$ is called* multi-substitution *and can be applied to a formula F in its conjunctive form $\sigma_\wedge$ or in its disjunctive form $\sigma_\vee$ as*

$$F\sigma_\wedge := \bigwedge_{i=1}^{n} F\sigma_i \qquad \text{and} \qquad F\sigma_\vee := \bigvee_{i=1}^{n} F\sigma_i$$

respectively.

We write id for the singleton set whose only element is the identity substitution.

Definition 24 *We define a cut-reduction relation on regular prenex proofs that will remove all quantifiers from the cuts. To each cut-reduction step from a proof χ to a proof χ', a multi-substitution σ will be associated. Such a step is denoted as $\chi \to^{\sigma} \chi'$. Let χ be an* **LK***-proof of the form:*

$$\dfrac{\begin{matrix}(\chi_1) & (\chi_2) \\ \Gamma \vdash \Delta, A & A, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}$$

(1) Reduction of quantifier rules: The cut formula is introduced by quantifier

rules on both sides immediately above the cut. If $A = (\forall x)B$*, then* $\chi =$

$$\dfrac{\dfrac{\overset{(\chi_1')}{\Gamma \vdash \Delta, B\{x \leftarrow \alpha\}}}{\Gamma \vdash \Delta, (\forall x)B}\ \forall\text{: r} \quad \dfrac{\overset{(\chi_2')}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{(\forall x)B, \Pi \vdash \Lambda}\ \forall\text{: l}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

and define $\chi \to^{\sigma} \chi' :=$

$$\dfrac{\overset{(\chi_1'\{\alpha \leftarrow t\})}{\Gamma \vdash \Delta, B\{x \leftarrow t\}} \quad \overset{(\chi_2')}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

where $\sigma = \{\{\alpha \leftarrow t\}\}$*. The case of* $A = (\exists x)B$ *is treated analogously.*

(2) Reduction of a contraction: The cut formula is introduced by a contraction on (at least) one of the two sides immediately above the cut. If χ_1 *ends with* $c : r$*, then* $\chi =$

$$\dfrac{\dfrac{\overset{(\chi_1')}{\Gamma \vdash \Delta, A, A}}{\Gamma \vdash \Delta, A}\ \text{c : r} \quad \dfrac{\overset{(\chi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

Let $\gamma_1, \ldots, \gamma_n$ *be the eigenvariables introduced by strong quantifier rules in* χ_2*. For* $i = 1, \ldots, n$ *let* γ_i' *and* γ_i'' *be fresh variables, define* $\sigma' := \{\gamma_1 \leftarrow \gamma_1', \ldots, \gamma_n \leftarrow \gamma_n'\}$*,* $\sigma'' := \{\gamma_1 \leftarrow \gamma_1'', \ldots, \gamma_n \leftarrow \gamma_n''\}$*, the multi-substitution* $\sigma := \{\sigma', \sigma''\}$ *and finally* $\chi \to^{\sigma} \chi' :=$

$$\dfrac{\dfrac{\dfrac{\overset{(\chi_1')}{\Gamma \vdash \Delta, A, A} \quad \overset{(\chi_2\sigma')}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda, A}\ \text{cut} \quad \overset{(\chi_2\sigma'')}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi, \Pi \vdash \Delta, \Lambda, \Lambda}\ \text{cut}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{c : *}$$

which is regular. If χ_2 *ends with* c : l*, proceed symmetrically.*

(3) Reduction of weakening: The cut formula is introduced by weakening on (at least) one of the two sides immediately above the cut. If χ_1 *ends with* $w : r$*, then* $\chi =$

$$\dfrac{\dfrac{\overset{(\chi_1')}{\Gamma \vdash \Delta}}{\Gamma \vdash \Delta, A}\ \text{w : r} \quad \dfrac{\overset{(\chi_2)}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

and define $\chi \to^{\text{id}} \chi' :=$

$$\dfrac{\overset{(\chi_1')}{\Gamma \vdash \Delta}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{w : *}$$

If χ_2 *ends with* w : l*, proceed symmetrically.*

(4) Rule permutation: The cut formula is not *introduced immediately above the cut on (at least) one of the two sides. If χ_2 ends with a rule r which does not introduce the cut formula and r is unary, then $\chi =$*

$$\dfrac{\dfrac{(\chi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{\dfrac{(\chi_2')}{A, \Pi' \vdash \Lambda'}\, r}{A, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

and define $\chi \to^{\text{id}} \chi' :=$

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

which is an **LK***-proof. Note that regularity ensures that the eigenvariable condition cannot be violated. If r is binary and the ancestor of the cut formula is in the left premise, then $\chi =$*

$$\dfrac{\dfrac{(\chi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{\dfrac{(\chi_2')}{A, \Pi_1' \vdash \Lambda_1'} \quad \dfrac{(\chi_2'')}{\Pi_2' \vdash \Lambda_2'}}{A, \Pi \vdash \Lambda}\, r}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \text{cut}$$

and define $\chi \to^{\text{id}} \chi' :=$

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{(\chi_2')}{A, \Pi_1' \vdash \Lambda_1'}}{\Gamma, \Pi_1' \vdash \Delta, \Lambda_1'}\ \text{cut} \quad \dfrac{(\chi_2'')}{\Pi_2' \vdash \Lambda_2'}}{\Gamma, \Pi \vdash \Delta, \Lambda}\, r$$

which is an **LK***-proof. If the ancestor of the cut formula is on the right side we proceed symmetrically. Analogous reductions apply for the case of χ_1 ending with a rule which does not introduce the cut formula.*

We consider the compatible closure of $\to^\sigma$ and write $\varphi[\chi] \to^\sigma \varphi[\chi']$ if $\chi \to^\sigma \chi'$ and $\varphi[\,]$ is any proof context keeping the regularity of both $\varphi[\chi]$ and $\varphi[\chi']$. In order to consider the transitive closure of $\to^\sigma$, define the composition of two multi-substitutions μ and ν as

$$\mu\nu := \{\sigma\theta \mid \sigma \in \mu, \theta \in \nu\}$$

which is again a multi-substitution as all $\sigma\theta$ have the same domain. We write $\varphi_1 \to^{\mu\nu} \varphi_3$ if there exists a φ_2 with $\varphi_1 \to^\mu \varphi_2$ and $\varphi_2 \to^\nu \varphi_3$.

Before proving the main theorem of this section we mention some basic facts

about multi-substitutions which will be useful later. For formulas A and B we write $A \Rightarrow B$ as shorthand for "$A \to B$ is valid" and similarly for $\Leftrightarrow$.

Lemma 11 *Let A, B, C be quantifier-free formulas and let $\sigma = \{\sigma_1, \ldots, \sigma_n\}$ and $\theta = \{\theta_1, \ldots, \theta_m\}$ be multi-substitutions. Then*

(1) $A(\sigma\theta)_\wedge \Leftrightarrow (A\sigma_\wedge)\theta_\wedge$ *and* $A(\sigma\theta)_\vee \Leftrightarrow (A\sigma_\vee)\theta_\vee$
(2) $(A \wedge B)\sigma_\wedge \Leftrightarrow A\sigma_\wedge \wedge B\sigma_\wedge$, $(A \vee B)\sigma_\vee \Leftrightarrow A\sigma_\vee \vee B\sigma_\vee$, $(\neg A)\sigma_\vee \Leftrightarrow \neg(A\sigma_\wedge)$, $(\neg A)\sigma_\wedge \Leftrightarrow \neg(A\sigma_\vee)$ *and* $(A \to B)\sigma_\vee \Leftrightarrow A\sigma_\wedge \to B\sigma_\vee$
(3) If A does not contain a variable from the domain of σ, then $(A \to B)\sigma_\wedge \Leftrightarrow A \to B\sigma_\wedge$ *and* $(B \to A)\sigma_\vee \Leftrightarrow B\sigma_\vee \to A$.
(4) If $A \Rightarrow B$ then $A\sigma_\wedge \Rightarrow B\sigma_\wedge$ and $A\sigma_\vee \Rightarrow B\sigma_\vee$.
(5) If $A\sigma_\wedge \Rightarrow B$ and $B\theta_\wedge \Rightarrow C$ then $A(\sigma\theta)_\wedge \Rightarrow C$.
(6) If $A \Rightarrow B\sigma_\vee$ and $B \Rightarrow C\theta_\vee$ then $A \Rightarrow C(\theta\sigma)_\vee$.

Proof. For 1 observe that

$$A(\sigma\theta)_\wedge \;=\; \bigwedge_{\substack{1\le i\le n\\ 1\le j\le m}} A(\sigma_i\theta_j) \;\Leftrightarrow\; \bigwedge_{j=1}^{m}\Big(\bigwedge_{i=1}^{n} A\sigma_i\Big)\theta_j \;=\; (A\sigma_\wedge)\theta_\wedge.$$

The disjunction case is analogous. For 2 consider as an example the case of the implication:

$$\begin{aligned}(A \to B)\sigma_\vee = \bigvee_{i=1}^{n}(A\sigma_i \to B\sigma_i) \;&\Leftrightarrow\; \bigvee_{i=1}^{n}(\neg(A\sigma_i) \vee B\sigma_i)\\ &\Leftrightarrow \bigvee_{i=1}^{n}\neg(A\sigma_i) \vee \bigvee_{i=1}^{n} B\sigma_i \;\Leftrightarrow\; (\neg\bigwedge_{i=1}^{n} A\sigma_i) \vee \bigvee_{i=1}^{n} B\sigma_i\\ &= A\sigma_\wedge \to B\sigma_\vee.\end{aligned}$$

For 3 note that:

$$(A \to B)\sigma_\wedge \;=\; \bigwedge_{i=1}^{n}(A \to B\sigma_i) \;\Leftrightarrow\; A \to \bigwedge_{i=1}^{n} B\sigma_i \;=\; A \to B\sigma_\wedge.$$

In order to show 4 assume $A \Rightarrow B$. Then for any substitution σ_i: $A\sigma_i \Rightarrow B\sigma_i$, so also $\bigwedge_{i=1}^n A\sigma_i \Rightarrow \bigwedge_{i=1}^n B\sigma_i$ and $\bigvee_{i=1}^n A\sigma_i \Rightarrow \bigvee_{i=1}^n B\sigma_i$. To show 5, apply first 4 to obtain $(A\sigma_\wedge)\theta_\wedge \Rightarrow B\theta_\wedge$ and then 1 to obtain $A(\sigma\theta)_\wedge \Rightarrow C$. The argument for 6 is symmetric. □

Theorem 2 *Let φ, φ' be prenex* **LK***-proofs. If $\varphi \to^\sigma \varphi'$ then $\mathcal{H}^{\mathrm{E}}(\varphi') \Rightarrow \mathcal{H}^{\mathrm{E}}(\varphi)\sigma_\vee$ and $\mathcal{H}^{\mathrm{I}}(\varphi)\sigma_\wedge \Rightarrow \mathcal{H}^{\mathrm{I}}(\varphi')$.*

Proof. Consider a single cut-reduction step $\varphi = \varphi[\chi] \to^\sigma \varphi[\chi'] = \varphi'$. The full result then follows by induction and cases 5 and 6 of Lemma 11.

(1) Reduction of a quantifier rule: Let $\sigma = \{\{\alpha \leftarrow t\}\}$, then $\mathcal{H}^{\mathrm{E}}(\varphi') = \mathcal{H}^{\mathrm{E}}(\varphi)\{\alpha \leftarrow t\} = \mathcal{H}^{\mathrm{E}}(\varphi)\sigma_\vee$ and $\mathcal{H}^{\mathrm{I}}(\varphi') = \mathcal{H}^{\mathrm{I}}(\varphi)\{\alpha \leftarrow t\} = \mathcal{H}^{\mathrm{I}}(\varphi)\sigma_\wedge$.
(2) Reduction of a contraction: Let

$$\mathcal{H}^{\mathrm{E}}(\varphi) = (\bigwedge_{i=1}^{n} A_i \bigwedge_{i=n+1}^{n'} A_i) \to (\bigvee_{j=1}^{m} B_j \bigvee_{j=m+1}^{m'} B_j)$$

where – with the notation of Definition 24, case 2 – A_i for $i = n+1, \ldots, n'$ and B_j for $j = m+1, \ldots, m'$ are the used quantifier-free instances of end-sequent formulas that are auxiliary formulas of rules in χ_2. Then

$$\begin{aligned}\mathcal{H}^{\mathrm{E}}(\varphi') &= (\bigwedge_{i=1}^{n} A_i \bigwedge_{i=n+1}^{n'} A_i\sigma' \bigwedge_{i=n+1}^{n'} A_i\sigma'') \to (\bigvee_{j=1}^{m} B_j \bigvee_{j=m+1}^{m'} B_j\sigma' \bigvee_{j=m+1}^{m'} B_j\sigma'') \\ &\Leftrightarrow (\bigwedge_{i=1}^{n} A_i \bigwedge_{i=n+1}^{n'} A_i)\sigma_\wedge \to (\bigvee_{j=1}^{m} B_j \bigvee_{j=m+1}^{m'} B_j)\sigma_\vee \\ &\Leftrightarrow \mathcal{H}^{\mathrm{E}}(\varphi)\sigma_\vee\end{aligned}$$

Furthermore, let

$$\mathcal{H}^{\mathrm{I}}(\varphi) = \bigwedge_{i=1}^{n}((\bigvee_{j=1}^{m_i'} C_{i,j}) \to (\bigwedge_{k=1}^{l_i'} D_{i,k})) \bigwedge_{i=n+1}^{n'} E_i$$

where – as above – $m_i \leq m_i'$ and $l_i \leq l_i'$ are chosen s.t. the $C_{i,j}$ for $j = m_i+1, \ldots, m_i'$ and the $D_{i,k}$ for $k = l_i+1, \ldots, l_i'$ are auxiliary formulas of rules in χ_2 and instances of cuts outside of χ. E_i for $i = n+1, \ldots, n'$ are the formulas containing the instances of the cuts in χ_2. Then

$$\begin{aligned}\mathcal{H}^{\mathrm{I}}(\varphi') &= \bigwedge_{i=1}^{n}((\bigvee_{j=1}^{m_i} C_{i,j} \bigvee_{j=m_i+1}^{m_i'} C_{i,j}\sigma_\vee) \to (\bigwedge_{k=1}^{l_i} D_{i,k} \bigwedge_{k=l_i+1}^{l_i'} D_{i,k}\sigma_\wedge)) \bigwedge_{i=n+1}^{n'} E_i\sigma_\wedge \\ &\Leftrightarrow \bigwedge_{i=1}^{n}((\bigvee_{j=1}^{m_i'} C_{i,j})\sigma_\vee \to (\bigwedge_{k=1}^{l_i'} D_{i,k})\sigma_\wedge) \bigwedge_{i=n+1}^{n'} E_i\sigma_\wedge\end{aligned}$$

Write C_i for $\bigvee_{j=1}^{m_i'} C_{i,j}$ and D_i for $\bigwedge_{k=1}^{l_i'} D_{i,k}$ and, for $i = 1, \ldots, n$, let ρ_i be the cut with instances $C_i\sigma_\vee$ and $D_i\sigma_\wedge$. If ρ_i is parallel to χ in φ, then by regularity both C_i and D_i do not contain a variable from the domain of σ. If χ is above ρ_i on the left side, then D_i does not contain a variable from the domain of σ and we have $C_i\sigma_\vee \to D_i\sigma_\wedge \Leftrightarrow (C_i \to D_i)\sigma_\wedge$ by 3 of Lemma 11 and symmetrically for χ being above ρ_i on the right side. In any case, we obtain

$$\mathcal{H}^{\mathrm{I}}(\varphi') \;\Leftrightarrow\; \bigwedge_{i=1}^{n}(C_i \to D_i)\sigma_\wedge \bigwedge_{i=n+1}^{n'} E_i\sigma_\wedge \;\Leftrightarrow\; \mathcal{H}^{\mathrm{I}}(\varphi)\sigma_\wedge.$$

(3) Reduction of weakening: Let $\mathcal{H}^{\mathrm{E}}(\varphi) = (\bigwedge_{i=1}^{n'} A_i) \to (\bigvee_{j=1}^{m'} B_j)$ with $n \leq n'$ and $m \leq m'$ chosen s.t. A_i for $i = n{+}1, \ldots, n'$ and B_j for $j = m{+}1, \ldots, m'$ are the used quantifier-free instances that are auxiliary formulas of rules in χ_2. Then $\mathcal{H}^{\mathrm{E}}(\varphi') = (\bigwedge_{i=1}^{n} A_i) \to (\bigvee_{j=1}^{m} B_j)$ and therefore $\mathcal{H}^{\mathrm{E}}(\varphi') \Rightarrow \mathcal{H}^{\mathrm{E}}(\varphi)$. Let

$$\mathcal{H}^{\mathrm{I}}(\varphi) = \bigwedge_{i=1}^{n}((\bigvee_{j=1}^{m'_i} C_{i,j}) \to (\bigvee_{k=1}^{l'_i} D_{i,j})) \bigwedge_{i=n+1}^{n'} E_i$$

with $m_i \leq m'_i$ and $l_i \leq l'_i$ chosen s.t. $C_{i,j}$ for $j = m_i + 1, \ldots, m'_i$ and $D_{i,k}$ for $k = l_i + 1, \ldots, l'_i$ are 1. the used quantifier-free instances that are auxiliary formulas of rules in χ_2 and 2. the quantifier-free instances that are auxiliary formulas of rules below χ which are used in φ but not used in φ'. E_i for $i = n + 1, \ldots, n'$ contains the instances of the cuts in χ_2. Then

$$\mathcal{H}^{\mathrm{I}}(\varphi') = \bigwedge_{i=1}^{n}((\bigvee_{j=1}^{m_i} C_{i,j}) \to (\bigvee_{k=1}^{l_i} D_{i,j}))$$

and we obtain $\mathcal{H}^{\mathrm{I}}(\varphi) \Rightarrow \mathcal{H}^{\mathrm{I}}(\varphi')$.

(4) Rule permutation: As neither the set of instances nor their usedness is changed, we immediately obtain $\mathcal{H}^{\mathrm{E}}(\varphi') = \mathcal{H}^{\mathrm{E}}(\varphi)$ and $\mathcal{H}^{\mathrm{I}}(\varphi') = \mathcal{H}^{\mathrm{I}}(\varphi)$.

□

Corollary 1 *Let φ, φ' be prenex* **LK***-proofs. If $\varphi \to^{\sigma} \varphi'$ and φ' has only quantifier-free cuts, then $\mathcal{H}^{\mathrm{E}}(\varphi)\sigma_{\vee}$ is a tautology.*

Proof. By Theorem 1, $\mathcal{H}^{\mathrm{I}}(\varphi') \to \mathcal{H}^{\mathrm{E}}(\varphi')$ is a tautology. But as all cuts are quantifier-free, $\mathcal{H}^{\mathrm{I}}(\varphi')$ is a tautology and therefore also $\mathcal{H}^{\mathrm{E}}(\varphi')$. By Theorem 2, $\mathcal{H}^{\mathrm{E}}(\varphi') \Rightarrow \mathcal{H}^{\mathrm{E}}(\varphi)\sigma_{\vee}$ which is therefore a tautology too. □

The above corollary shows that for computing an Herbrand-disjunction the knowledge of a multi-substitution σ induced by a cut-elimination sequence is sufficient. This result paves the way for more streamlined cut-elimination procedures: By choosing appropriate multi-substitutions, a short tautology read off from a proof with cuts can be transformed into an Herbrand-disjunction directly and without doing the tedious local rewrite steps of cut-elimination. Such a procedure would provide a new middle ground between cut-elimination and Hilbert's ε- calculus [12].

7 Conclusion

We have shown that, from a proof with cuts, one can read off a short propositional tautology composed of instances of the end-sequent and the cut formulas

which describes the proof in a natural way. This demonstrates that the divisibility of inference in first-order logic into a propositional and a quantifier part is a very general property: It does not only apply to cut-free proofs (as in Gentzen's mid-sequent theorem) but also to proofs with cuts and to whole cut-elimination sequences. The first-order part of a cut-elimination sequence is a multi-substitution combining all substitutions and variable-renamings.

Important future work consists in devising a procedure which computes an Herbrand-disjunction directly from a short tautology extracted from a proof by applying appropriate multi-substitions. Such a procedure is similar to both, cut-elimination in the sequent calculus and Hilbert's ε-calculus and may therefore be used for better understanding their relationship. In addition, such a procedure can be expected to be computationally superior to cut-elimination, as it is not based on local proof rewrite steps. It will therefore be useful for concrete computations of Herbrand-disjunctions for the analysis of proofs as e.g. in [1].

The results in this paper are limited to prenex proofs because the mid-sequent reduction by rule permutations as defined in Section 3 requires prenex formulas. Note, however, that the results about the characteristic clause sets do not require the assumption of prenex formulas. As future work, we also plan to extend our results also to the non-prenex case, constructing Herbrand-sequents with a technique from [3]. This extension is useful as the transformation of proofs into prenex form can be expensive [4].

Acknowledgements
The author would like to thank Matthias Baaz and Alexander Leitsch for useful comments on earlier versions of this article.

References

[1] M. Baaz, S. Hetzl, A. Leitsch, C. Richter, H. Spohr, CERES: An Analysis of Fürstenberg's Proof of the Infinity of Primes, to appear in Theoretical Computer Science.

[2] M. Baaz, S. Hetzl, A. Leitsch, C. Richter, H. Spohr, Proof Transformation by CERES, in: J. M. Borwein, W. M. Farmer (eds.), Mathematical Knowledge Management (MKM) 2006, vol. 4108 of Lecture Notes in Artificial Intelligence, Springer, 2006.

[3] M. Baaz, A. Leitsch, On Skolemization and Proof Complexity, Fundamenta Informaticae 20 (4) (1994) 353–379.

[4] M. Baaz, A. Leitsch, Cut Normal Forms and Proof Complexity, Annals of Pure and Applied Logic 97 (1999) 127–177.

[5] M. Baaz, A. Leitsch, Cut-elimination and Redundancy-elimination by Resolution, Journal of Symbolic Computation 29 (2) (2000) 149–176.

[6] S. R. Buss, On Herbrand's Theorem, in: Logic and Computational Complexity, vol. 960 of Lecture Notes in Computer Science, Springer, 1995, pp. 195–209.

[7] A. Carbone, Interpolants, cut elimination and flow graphs for the propositional calculus, Annals of Pure and Applied Logic 83 (1997) 249–299.

[8] G. Gentzen, Untersuchungen über das logische Schließen, Mathematische Zeitschrift 39 (1934–1935) 176–210,405–431.

[9] S. Hetzl, Characteristic Clause Sets and Proof Transformations, Ph.D. thesis, Vienna University of Technology (2007).

[10] S. Hetzl, Proof Profiles. Characteristic Clause Sets and Proof Transformations, VDM, 2008.

[11] S. Hetzl, A. Leitsch, Proof Transformations and Structural Invariance, in: S. Aguzzoli, A. Ciabattoni, B. Gerla, C. Manara, V. Marra (eds.), Algebraic and Proof-theoretic Aspects of Non-classical Logics, vol. 4460 of Lecture Notes in Artificial Intelligence, Springer, 2007.

[12] D. Hilbert, P. Bernays, Grundlagen der Mathematik II, Springer, 1939.

[13] H. Luckhardt, Herbrand-Analysen zweier Beweise des Satzes von Roth: Polynomiale Anzahlschranken, Journal of Symbolic Logic 54 (1) (1989) 234–263.

[14] P. Pudlák, The Lengths of Proofs, in: S. Buss (ed.), Handbook of Proof Theory, Elsevier, 1998, pp. 547–637.

[15] G. Takeuti, Proof Theory, 2nd ed., North-Holland, Amsterdam, 1987.