Proof Transformations and Structural Invariance*

Stefan Hetzl and Alexander Leitsch

Institute of Computer Languages (E185),
Vienna University of Technology, Favoritenstraße 9,
1040 Vienna, Austria
{hetzl|leitsch}@logic.at

Abstract. In this paper we define the concept of a profile, which is a characteristic clause set, corresponding to an **LK**-proof in first-order logic, which is invariant under rule permutations. It is shown (via cut-elimination) that the profile is even invariant under a large class of proof transformations (called "simple transformations"), which includes transformations to negation normal form. As proofs having the same profile show the same behavior w.r.t. cut-elimination (which can be formally defined via the method CERES), proofs obtained by simple transformations can be considered as equal in this sense. A comparison with related results based on proof nets is given: in particular it is shown that proofs having the same profile define a larger equivalence class than those having the same proof net.

1 Introduction

Cut-elimination introduced by Gerhard Gentzen [7] is the most prominent form of proof transformation in logic and plays an important role in automating the analysis of mathematical proofs. The removal of cuts corresponds to the elimination of intermediate statements (lemmas) from proofs resulting in a proof which is analytic in the sense, that all statements in the proof are subformulas of the result. Therefore, the proof of a combinatorial statement is converted into a purely combinatorial proof. Cut-elimination is therefore an essential tool for the analysis of proofs, especially to make implicit parameters explicit.

In [3] the cut-elimination method CERES has been defined that works by employing the resolution technique from automated theorem proving. It has been shown in [4] that it can be considered as a generalization of the usual reductive cut-elimination methods. The main proof-theoretic tool of CERES is the *characteristic clause set* which gives a concise representation of the logical material that is used to build the cut-formulas. From the fact that two proofs have the same characteristic clause set one can deduce that they basically have the same set of cut-free proofs under the CERES-method.

In this paper we define the *profile* of a proof as an improved version of the characteristic clause set that, among others, has the property of being invariant

* supported by the Austrian Science Fund (project no. P17995-N12)

under arbitrary rule permutations. This implies that two proofs having the same proof net (in the sense of [10]) also have the same profile.

The central part of this paper is an investigation of a certain class of proof transformations, so called simple transformations, containing as a special case for example the transformation of formulas into negation-normal-form. We show that the profile is invariant under application of simple transformations to cut formulas. This result means that proofs differing only by such a transformation show the same behavior w.r.t. cut-elimination (by the method CERES).

1.1 Related Work

In [5] Danos, Joinet and Schellinx give an elegant formulation of a class of confluent and strongly terminating cut-elimination procedures for classical logic. In [6] they build on this work to show that the normal forms are not changed after application of transformations called computational isomorphisms. Our work is similar to [6] 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: [6] builds on the confluence (and termination) result established in [5] 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 [6] 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, but proving this will be more difficult because the profile changes in a more complicated way.

2 Sequent Calculus

In order to distinguish different occurrences of the same formula in a sequent without having to introduce exchange rules to the calculus, we formally use sequents of indexed formulas.

Definition 1 (indexed formula). *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 multisets of formulas. An indexed sequent is a pair of sets of indexed formulas.

We distinguish countable sets of *free* and *bound* variables.

We use the following variant of sequent calculus for classical first-order logic:

Definition 2 (LK-proof). *An* **LK***-proof φ is a tree. The nodes of φ are labelled with indexed sequents, the edges are labelled with rules and the leaves are axiom sequents. Furthermore each formula index occurs at most once in a proof.*

1. *Axiom sequents are of the form*

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

2. *Logical Rules*
   (a) *Conjunction*

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

   (b) *Disjunction*

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

   (c) *Implication*

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

   (d) *Negation*

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

   (e) *Universal Quantification*

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

   For the variable α and the term t the following must hold:
   i. *t must not contain bound variables,*
   ii. *α is a free variable, called* eigenvariable*, which must not occur in $\Gamma \cup \Delta \cup \{A\}$ (eigenvariable condition).*

   (f) *Existential Quantification*

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

   The restrictions on α and t are the same as for universal quantification.

3. *Structural Rules*
   (a) *Weakening*

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

   (b) *Contraction*

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

   (c) *Cut*

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

Definition 3 (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:*

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

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

2. *Cut by pseudo-cut:*

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

   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 (see [3] and Section 3) can be generalized to pseudo-proofs without any problems.

Definition 4. *An* **LKps***-proof is called* regular *if all eigenvariables are different from each other.*

Definition 5 (main and auxiliary occurrence). *Let φ be an* **LK***-proof and let ρ be a rule in φ. The formula occurrence whose main symbol has been introduced by ρ in the sequent immediately below ρ is called the* main *occurrence of ρ. The formula occurrence(s) that has/have been used to compose the main occurrence of ρ is/are called* auxiliary *occurrence(s) of ρ.*

Definition 6 ($\to_{\mathrm{G}}$). *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:*

$$\frac{\begin{matrix}(\varphi_1)\\ \Gamma \vdash \Delta, A\end{matrix} \quad \begin{matrix}(\varphi_2)\\ A, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ cut$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\dfrac{\dfrac{\overset{(\varphi_1')}{\Gamma \vdash \Delta, B\{x \leftarrow \alpha\}}}{\Gamma \vdash \Delta, (\forall x)B}\; \forall : r \qquad \dfrac{\overset{(\varphi_2')}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{(\forall x)B, \Pi \vdash \Lambda}\; \forall : l}{\Gamma, \Pi \vdash \Delta, \Lambda}\; cut$$

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

$$\dfrac{\overset{(\varphi_1'\{\alpha \leftarrow t\})}{\Gamma \vdash \Delta, B\{x \leftarrow t\}} \quad \overset{(\varphi_2')}{B\{x \leftarrow t\}, \Pi \vdash \Lambda}}{\Gamma, \Pi \vdash \Delta, \Lambda}\; cut$$

   (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,* $\varphi =$

$$\dfrac{A \vdash A \quad \overset{(\varphi_2)}{A, \Pi \vdash \Lambda}}{A, \Pi \vdash \Lambda}\ cut$$

   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* $w : r$, $\varphi =$

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

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

$$\dfrac{\overset{(\varphi_1')}{\Gamma \vdash \Delta}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ w : *$$

   (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* $c : r$, $\varphi =$

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

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

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

   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* $\rightarrow_{\mathrm{G_r}}$*:*
   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,* $\varphi =$

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

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

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

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, $\varphi =$

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

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

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

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 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 [3] which also eliminates pseudo-cuts).

3 The Profile

The profile of an **LKps**-proof is a set of labelled clauses. In order to give the definition of the profile, we first explain labelled clause logic.

3.1 Labelled Clauses

We use $\mathcal{L}$ to denote a countable infinite set of labels (e.g. $\mathcal{L} = \mathbb{N}$).

Definition 7 (clause). *A clause is a sequent consisting only of atomic formulas. A labelled clause is a clause that is assigned a non-empty set of labels from $\mathcal{L}$. For a clause c we write $\mathcal{L}(c)$ to denote this set.*

We will use the notation $A_1, \ldots, A_n \vdash^{\{l_1,\ldots,l_k\}} B_1, \ldots, B_m$ for the clause $A_1, \ldots, A_n \vdash B_1, \ldots, B_m$ with the set of labels $\{l_1, \ldots, l_k\}$. For the sake of readability we will sometimes omit the curly braces.

Definition 8 (merge, product). *Let $c = \Gamma \vdash^{L_1} \Delta$ and $d = \Pi \vdash^{L_2} \Lambda$ be labelled clauses. We define the* merge *of c and d as $c \circ d := \Gamma, \Pi \vdash^{L_1 \cup L_2} \Delta, \Lambda$. Let C, D be sets of labelled clauses. We define the* product *of C and D as $C \times D := \{c \circ d \mid c \in C, d \in D\}$.*

The labels will be used in order to describe subsets of sets of labelled clauses as follows: 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 $\mathcal{L}(c)$.

Definition 9 (clause selection based on labels). *Let C be a set of labelled clauses. Let F, G be propositional formulas built up from label sets $L, L_1, L_2, \ldots$ as atoms and the connectives $\wedge, \vee, \neg$. We define C^F as follows:*

1. $C^L := \{c \in C \mid c \text{ is an } L\text{-clause}\}$
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 1. Let $C := \{\vdash^1 P\, ;\, P \vdash^{2,3} R\, ;\, R \vdash^3\, ;\, P \vdash^{2,3,4} Q\, ;\, Q \vdash^{3,4}\}$. Then

$$C^{\{4\} \vee \neg \{3\}} = C^{\{4\}} \cup (C \setminus C^{\{3\}}) = \{\vdash^1 P\, ;\, P \vdash^{2,3,4} Q\, ;\, Q \vdash^{3,4}\}$$

Definition 10 (restricted product). *Let C, D be sets of labelled clauses and L be a set of labels. We define the operation $\times_L$ as*

$$C \times_L D := (C^L \times D^L) \cup C^{\neg L} \cup D^{\neg L}$$

Example 2. Let $C = \{P \vdash^1\, ;\, Q \vdash^2\}, D = \{\vdash^3 P\, ;\, \vdash^4 Q\}$. Then

$$\begin{aligned} C \cup D &= \{P \vdash^1\, ;\, Q \vdash^2\, ;\, \vdash^3 P\, ;\, \vdash^4 Q\} \\ C \times D &= \{P \vdash^{1,3} P\, ;\, P \vdash^{1,4} Q\, ;\, Q \vdash^{2,3} P\, ;\, Q \vdash^{2,4} Q\} \\ C \times_{\{1,4\}} D &= \{P \vdash^{1,4} Q\, ;\, Q \vdash^2\, ;\, \vdash^3 P\} \end{aligned}$$

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 $L \subseteq \mathcal{L}$.

Lemma 1. *Let C, D, E be sets of labelled clauses and $L, L_1, L_2 \subseteq \mathcal{L}$. Then*

1. $C \times_L D = D \times_L C$
2. *If 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. 1. follows easily from commutativity of × and ∪

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

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

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:

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

Distributing × over ∪ we get:

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

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.
q.e.d.

3.2 Definition of the Profile

In addition to labelled clauses we will consider labelled **LKps**-proofs to define the profile of a proof.

Definition 11 (labelled LKps-proof). *A* labelled **LKps**-proof *is a pseudo-proof where each axiom is assigned a unique label from $\mathcal{L}$. Furthermore each formula occurrence μ is assigned a set of labels in the following way:*

1. *If μ occurs in an axiom its set of labels is the singleton set containing the axiom label.*
2. *If μ does not occur in an axiom its set of labels is the union of the sets of labels of its immediate ancestor formula occurrences.*

So the set of labels of a formula occurrence describes the set of axioms that were used to build up this formula occurrence. For a formula occurrence μ in a labelled **LKps**-proof we write $\mathcal{L}(\mu)$ for its set of labels. For a rule ρ in a labelled **LK**-proof $\mathcal{L}(\rho)$ denotes the union of the label sets of the auxiliary formula occurrences of ρ. The cut-elimination rules defined in Definition 6 can be carried over to labelled **LK**-proofs with only minor modifications: in case of contraction elimination ($\rightarrow_{\mathrm{G_c}}$) the renaming of eigenvariables has to be extended to the renaming of labels.

From now on we consider only proofs with skolemized end-sequents; skolemization is necessary for cut-elimination based on profiles and characteristic clause sets [3]. Note that every proof can be transformed into a skolemized version [2].

Let Ω denote the set of all formula occurrences which are ancestors of pseudo-cut formulas. A rule with auxiliary formulas in Ω is called an Ω-rule, with auxiliary formulas not in Ω a Σ-rule. For a sequent occurrence ν and a set of formula occurrences M, let $\mathrm{S}(\nu, M)$ denote the sub-sequent of the sequent at ν that contains only the formulas whose occurrences are in M.

Definition 12 (proof profile). *Let φ be a regular labelled* **LKps**-*proof. We define the profile $\mathrm{P}(\varphi)$ of φ by induction on a position ν in φ.*

1. *If ν is an axiom:*
$$\mathrm{P}(\varphi).\nu := \{\mathrm{S}(\nu, \Omega)\}.$$
2. *If ν is a unary rule with ancestor rule μ, then:*
$$\mathrm{P}(\varphi).\nu := \mathrm{P}(\varphi).\mu$$
3. *If ν is a binary rule with ancestor rules μ_1, μ_2 then*
   (a) If ν is an Ω-rule:
$$\mathrm{P}(\varphi).\nu := \mathrm{P}(\varphi).\mu_1 \cup \mathrm{P}(\varphi).\mu_2$$
   (b) If ν is a Σ-rule:
$$\mathrm{P}(\varphi).\nu := \mathrm{P}(\varphi).\mu_1 \times_{\mathcal{L}(\nu)} \mathrm{P}(\varphi).\mu_2$$

Note that this definition of a proof profile does not depend on syntactic details of the sequent calculus variant. Exactly the same definition can be used for example for additive calculi or for a calculus with arbitrary atomic axiom sequents, etc. Another important feature of the proof profile is that for the CERES method [3] it can be used instead of the characteristic clause set and will always yield cut-free proofs that are at most as long as those corresponding to the characteristic clause set.

3.3 Compatibility

Lemma 2 (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 $i = 1, \ldots, n : \mathcal{L}(\sigma'_i) = \mathcal{L}(\sigma_i)$*

then

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

Proof. 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 $\mathcal{L}(\nu') = \mathcal{L}(\nu)$.

Now, using $\mathcal{L}(\nu') = \mathcal{L}(\nu)$ 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 $\mathrm{P}(\chi') = \mathrm{P}(\chi)\theta$ q.e.d.

3.4 Permutation of Independent Rules

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. [8]). In this section we will formally define these rule permutations and show that the proof profile is not changed by permuting rules.

Definition 13 (adjacent). *Two rules in an* **LKps***-proof are said to be* adjacent *if one occurs immediately above the other.*

Definition 14 (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 15 (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 $\sim_\pi$.

Lemma 3 (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 transitivity of $=$, it suffices to show the invariance of P 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 $\mathrm{P}(\chi').\mu = \mathrm{P}(\chi).\mu$.

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

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

For some set of labelled clauses C.

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

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

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

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

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):

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

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

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

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 $\mathrm{P}(\chi).\mu = \mathrm{P}(\chi').\mu$ 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 1 to obtain $\mathrm{P}(\chi).\mu = \mathrm{P}(\chi').\mu$.

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 we know that $E^L = \emptyset$ and $E^{\neg L} = E$ and so

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

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

In [10] E. Robinson defines proof nets for classical propositional logic and shows ([10], proposition 6.2):

Proposition 1. *Two* **LK***-proofs* φ *and* φ' *(for classical propositional logic) induce isomorphic proof nets iff* $\varphi \approx_\pi \varphi'$.

Building on this and Lemma 3 we can easily conclude

Corollary 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 [9] an extension of Robinson's proof nets to first-order classical logic by treating quantifiers with boxes. We conjecture that the result of Corollary 1 also extends to this notion of proof net.

4 The Profile and Cut-Elimination

In [4] 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 [4] 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). 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 4 (rank-reduction).

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

Proof. As rank-reduction $\rightarrow_{\mathrm{G_r}}$ is contained in the permutation of adjacent independent rules $\approx_\pi$, we can apply Lemma 3. q.e.d.

Lemma 5 (propositional reduction).

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

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

1. Conjunction: Then φ has the form:

$$\dfrac{\dfrac{\begin{matrix}(\varphi_1, C) & (\varphi_2, D)\\ \Gamma \vdash \Delta, A & \Pi \vdash \Lambda, B\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda, A \wedge B}\wedge : r \qquad \dfrac{\begin{matrix}(\varphi_3, E)\\ A, B, \Theta \vdash \Sigma\end{matrix}}{A \wedge B, \Theta \vdash \Sigma}\wedge : l}{\Gamma, \Pi, \Theta \vdash \Delta, \Lambda, \Sigma}\,\mathit{cut}$$

   and φ' has the form:

$$\dfrac{\begin{matrix}(\varphi_2, D)\\ \Pi \vdash \Lambda, B\end{matrix} \qquad \dfrac{\begin{matrix}(\varphi_1, C) & (\varphi_3, E)\\ \Gamma \vdash \Delta, A & A, B, \Theta \vdash \Sigma\end{matrix}}{B, \Gamma, \Theta \vdash \Delta, \Sigma}\,\mathit{cut}}{\Gamma, \Pi, \Theta \vdash \Delta, \Lambda, \Sigma}\,\mathit{cut}$$

   So we have

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

   and

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

   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 2 is fulfilled because $\rightarrow_{\mathrm{G_p}}$ does not change the ancestor axioms of the formula occurrences in the end-sequent of the rewritten part. So we can use Lemma 2 to conclude $\mathrm{P}(\chi') = \mathrm{P}(\chi)$ q.e.d.

Lemma 6 (quantifier reduction). *Let χ be a regular* **LKps***-proof and let*

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

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. 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

$$\dfrac{\dfrac{\begin{array}{c}(\varphi_1, C)\\ \Gamma \vdash \Delta, B\{x \leftarrow \alpha\}\end{array}}{\Gamma \vdash \Delta, (\forall x)B}\,\forall : r \qquad \dfrac{\begin{array}{c}(\varphi_2, D)\\ B\{x \leftarrow t\}, \Pi \vdash \Lambda\end{array}}{(\forall x)B, \Pi \vdash \Lambda}\,\forall : l}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathit{cut}$$

and φ' has the form

$$\dfrac{\begin{array}{c}(\varphi_1\{\alpha \leftarrow t\}, C\{\alpha \leftarrow t\})\\ \Gamma \vdash \Delta, B\{x \leftarrow t\}\end{array} \qquad \begin{array}{c}(\varphi_2, D)\\ B\{x \leftarrow t\}, \Pi \vdash \Lambda\end{array}}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathit{cut}$$

So we have

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

and

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

but α does not occur in D so

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

And as the label sets of the formula occurrences in the sequent at μ do not change we can apply Lemma 2. q.e.d.

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

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

We write χ' for $\chi[\varphi']_\mu$. Let D be the set of axiom labels of the sub-proof deleted by this $\rightarrow_{\mathrm{G_w}}$-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. 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 $\mathrm{P}(\chi') = \mathrm{P}(\chi)^{D^*}$ again by induction on the length l of the path between μ and the end-sequent.

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

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 (IH). If ρ is a binary Ω-rule then $\mathrm{P}(\chi) = X \cup Y$ and $\mathrm{P}(\chi') = X^{D^*} \cup Y$, but Y contains no labels from D nor any from $L_1, \ldots, L_n$, so $Y = Y^{D^*}$ and thus $\mathrm{P}(\chi') = X^{D^*} \cup Y = X^{D^*} \cup Y^{D^*} = (X \cup Y)^{D^*} = \mathrm{P}(\chi)^{D^*}$. 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 $\mathrm{P}(\chi) = X \times_{\mathcal{L}(\alpha) \cup L_{n+1}} Y$ and by $(\star)$ and (IH) that $\mathrm{P}(\chi') = X^{D^*} \times_{L_{n+1}} Y$. By algebraic manipulations one shows that $\mathrm{P}(\chi') = (X \cup Y)^{D^* \wedge \neg L_{n+1}}$ and $\mathrm{P}(\chi)^{D^* \wedge \neg L_{n+1}} = X^{\neg \mathcal{L}(\alpha) \wedge D^* \wedge \neg L_{n+1}} \cup Y^{D^* \wedge \neg L_{n+1}}$. 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 $\mathrm{P}(\chi)^{D^* \wedge \neg L_{n+1}} = X^{D^* \wedge \neg L_{n+1}} \cup Y^{D^* \wedge \neg L_{n+1}} = (X \cup Y)^{D^* \wedge \neg L_{n+1}}$.
2. $\mathcal{L}(\alpha) \not\subseteq D$: In this case we have $\mathrm{P}(\chi) = X \times_L Y$ for a set of labels L, and by $(\star)$ and (IH) that $\mathrm{P}(\chi') = X^{D^*} \times_{L \setminus D} Y$. 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 $\mathrm{P}(\chi') = (X^L \times Y^L)^{D^*} \cup X^{D^* \wedge \neg (L \wedge \neg D)} \cup Y^{\neg (L \wedge \neg D)}$. By further simplifications one shows that $\mathrm{P}(\chi') = (X^L \times Y^L)^{D^*} \cup (X^{\neg L})^{D^*} \cup (Y^{\neg L})^{D^*} = \mathrm{P}(\chi)^{D^*}$ q.e.d.

Corollary 2. *Let χ be an* **LKps***-proof and μ a position in χ of a cut that can be reduced by $\rightarrow_{\mathrm{G_w}}$. Let D be the set of axiom labels of the sub-proof deleted by this $\rightarrow_{\mathrm{G_w}}$-step. If all formula occurrences in the deleted sub-proof are ancestors of cut formulas then*

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

Proof. By applying Lemma 7 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 $\mathrm{P}(\chi') = \mathrm{P}(\chi)^{\neg D}$ q.e.d.

Lemma 8 (contraction reduction). *Let χ be an* **LKps***-proof and μ a position in χ of a cut that can be reduced by $\rightarrow_{\mathrm{G_c}}$. Then*

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

Let D be the set of axiom labels of the sub-proof duplicated by this $\rightarrow_{\mathrm{G_c}}$-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. 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 $\mathrm{P}(\chi') = \mathrm{P}(\chi) \cup \mathrm{P}(\chi)^D\pi$ again by induction on the length l of the path between μ and the end-sequent. If $l = 0$ then $\mathrm{P}(\chi) = X \cup Y$ and $\mathrm{P}(\chi') = X \cup X\pi \cup Y$ but as $(X \cup Y)^D = X$ we obtain $\mathrm{P}(\chi)^D\pi = X\pi$. 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 (IH). If ρ is a binary Ω-rule then $\mathrm{P}(\chi) = X \cup Y$ and by (IH): $\mathrm{P}(\chi') = X \cup X^D\pi \cup Y$ but as Y contains no labels from D we have $\mathrm{P}(\chi)^D\pi = X^D\pi$.

If ρ is a binary Σ-rule then $\mathrm{P}(\chi) = X \times_L Y$ and by (IH) and ($\star$): $\mathrm{P}(\chi') = (X \cup X^D\pi) \times_{L\cup(L\cap D)\pi} Y$. 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

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

So it remains to show

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

As Y cannot contain any labels from D, we have

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

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

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

q.e.d.

5 A General Invariance Property

Definition 16. *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 $\rightarrow_{\mathrm{G}}$ and corresponding normal forms:

Definition 17. *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 $T(\varphi, \tau_{A,B})$:*

$$\dfrac{\overset{\varphi}{\Gamma \vdash \Delta, A} \quad \overset{\tau_{A,B}}{A \vdash B}}{\Gamma \vdash \Delta, B}\ cut$$

and $T(\tau_{A,B},\psi)$:

$$\cfrac{\overset{\tau_{A,B}}{A \vdash B} \quad \overset{\psi}{B, \Pi \vdash \Lambda}}{A, \Pi \vdash \Lambda}\ cut$$

We mark in $T(\varphi,\tau_{A,B})(T(\tau_{A,B},\psi))$ all ancestors of the final cut and refine $\rightarrow_{\mathrm{G}}$ to $\rightarrow_{\mathrm{G_t}}$ 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

$$\cfrac{B^{\{i\}} \vdash B^{\{i\}} \quad B^{\{j\}} \vdash B^{\{j\}}}{B^{\{i\}} \vdash B^{\{j\}}}\ cut$$

(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 $T(\tau_{A,B},\psi)$ $(T(\varphi,\tau_{A,B}))$.

Remark 1. 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 18. *Two formulas A, B are called* V-equivalent *if they contain the same variables.*

Definition 19. *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.

Remark 2. 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 3. The following transformation τ is Q-simple:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(\alpha_1,\alpha_2) \vdash P(\alpha_1,\alpha_2)}{\vdash \neg P(\alpha_1,\alpha_2), P(\alpha_1,\alpha_2)}\ \neg : r}{\vdash \neg P(\alpha_1,\alpha_2), (\exists y)P(\alpha_1,y)}\ \exists : r}{\vdash (\forall y)\neg P(\alpha_1,y), (\exists y)P(\alpha_1,y)}\ \forall : r}{\vdash (\exists x)(\forall y)\neg P(x,y), (\exists y)P(\alpha_1,y)}\ \exists : r}{\vdash (\exists x)(\forall y)\neg P(x,y), (\forall x)(\exists y)P(x,y)}\ \forall : r}{\neg(\forall x)(\exists y)P(x,y) \vdash (\exists x)(\forall y)\neg P(x,y)}\ \neg : l$$

No transformation with end-sequent $(\forall x)Q(x) \vdash (\exists x)Q(x)$ is Q-simple.

Definition 20. *A transformation $\tau_{A,B}$ is called* simple *if it is Q-simple and does not contain structural rules.*

Example 4. The transformation τ defined in Example 3 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.

$$I(B \to C) = \dfrac{\dfrac{\begin{matrix} I(B) & I(C) \\ B \vdash B & C \vdash C \end{matrix}}{B, B \to C \vdash C}\ \to : l}{B \to C \vdash B \to C}\ \to : r \qquad I((\forall x)B) = \dfrac{\dfrac{\begin{matrix} I(B\{x \leftarrow \alpha\}) \\ B\{x \leftarrow \alpha\} \vdash B\{x \leftarrow \alpha\} \end{matrix}}{(\forall x)B \vdash B\{x \leftarrow \alpha\}}\ \forall : l}{(\forall x)B \vdash (\forall x)B}\ \forall : r$$

Definition 21. *Two formulas A, B are called strongly equivalent (notation $A \sim_s B$) if there exist simple transformations $\tau_{A,B}$ and $\tau_{B,A}$.*

Remark 3. 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. 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 $(\forall x)(P(x) \wedge Q)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(\alpha) \vdash P(\alpha) \quad Q \vdash Q}{P(\alpha), Q \vdash P(\alpha) \wedge Q}\ \wedge : r}{(\forall x)P(x), Q \vdash P(\alpha) \wedge Q}\ \forall : l}{(\forall x)P(x) \wedge Q \vdash P(\alpha) \wedge Q}\ \wedge : l}{(\forall x)P(x) \wedge Q \vdash (\forall x)(P(x) \wedge Q)}\ \forall : r$$

But there is no simple transformation from $(\forall x)(P(x) \wedge Q)$ to $(\forall x)P(x) \wedge Q$.

Definition 22. *A binary relation $\bigtriangledown$ on formulas is called* compatible *if, for all formulas A and B, $A \bigtriangledown B$ implies $C[A]_\lambda \bigtriangledown C[B]_\lambda$ for any formula context $C[\ ]_\lambda$.*

Proposition 2. *$\sim_s$ 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}:

$$\frac{\overset{\tau_{A,B}}{A \vdash B} \quad \overset{\tau_{B,C}}{B \vdash C}}{A \vdash C}\ cut$$

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: $\{x_1, \ldots, x_n\}$ 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

$$X_{AB}\colon < (y_1, \ldots, y_m), (z_1, \ldots, z_k), (z_1, \ldots, z_k), (y_1, \ldots, y_m) > .$$

Now consider the tuple X_{AB} under substitution of the bound variables by the quantifier substitutions. Then we obtain the *quantifier-introduction vector* for $\tau_{A,B}$:

$$Y_{AB}\colon < (\alpha_1, \ldots, \alpha_m), (\beta_1, \ldots, \beta_k), (\beta_1, \ldots, \beta_k), (\alpha_1, \ldots, \alpha_m) > .$$

For $\tau_{B,C}$ we obtain (replacing A by B, B by C in the tuple notation)

$$X_{BC}\colon < (y_1,\ldots,y_m),(z_1,\ldots,z_k),(z_1,\ldots,z_k),(y_1,\ldots,y_m) > .$$

and the quantifier introduction vector

$$Y_{BC}\colon < (\beta'_1,\ldots,\beta'_m),(\gamma_1,\ldots,\gamma_k),(\gamma_1,\ldots,\gamma_k),(\beta'_1,\ldots,\beta'_m) > .$$

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

$$Y_{AC}\colon < (\alpha_1,\ldots,\alpha_m),(\gamma_1,\ldots,\gamma_k),(\gamma_1,\ldots,\gamma_k),(\alpha_1,\ldots,\alpha_m) > .$$

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.

(IH) Let $C[A]_\lambda \sim_s C[B]_\lambda$ 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

$$(a)\ C \equiv C_1 \wedge C_2,\ (b)\ C \equiv C_1 \vee C_2,\ (c)\ C \equiv C_1 \rightarrow C_2,$$
$$(d)\ C \equiv \neg C',\qquad (e)\ C \equiv (\forall x)C',\ \ (f)\ C \equiv (\exists x)C'.$$

We only show the cases c,d,e, the others are analogous.

(c) We consider the formulas $(C_1 \rightarrow C_2)[A]_\mu$ and $(C_1 \rightarrow C_2)[B]_\mu$. 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.

$$C[A]_\mu = C_1[A]_\lambda \rightarrow C_2,\ C[B]_\mu = C_1[B]_\lambda \rightarrow C_2.$$

We define a transformation τ transforming $C_1[A]_\lambda \rightarrow C_2$ into $C_1[B]_\lambda \rightarrow C_2$ (the other direction can be obtained by exchanging A and B).

$$\dfrac{\dfrac{\overset{\tau'}{C_1[B]_\lambda \vdash C_1[A]_\lambda} \quad \overset{I(C_2)}{C_2 \vdash C_2}}{C_1[B]_\lambda, C_1[A]_\lambda \rightarrow C_2 \vdash C_2}\ \rightarrow: l}{C_1[A]_\lambda \rightarrow C_2 \vdash C_1[B]_\lambda \rightarrow C_2}\ \rightarrow: r$$

By (IH) 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

$$\dfrac{\dfrac{\overset{\tau'}{C'[B]_\lambda \vdash C'[A]_\lambda}}{\neg C'[A]_\lambda, C'[B]_\lambda \vdash}\ \neg : l}{\neg C'[A]_\lambda \vdash \neg C'[B]_\lambda}\ \neg : r$$

By (IH) 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

$$\dfrac{\dfrac{\overset{\tau'}{C'[A]_\lambda\{x \leftarrow \alpha\} \vdash C'[B]_\lambda\{x \leftarrow \alpha\}}}{(\forall x)C'[A]_\lambda \vdash C'[B]_\lambda\{x \leftarrow \alpha\}}\ \forall : l}{(\forall x)C'[A]_\lambda \vdash (\forall x)C'[B]_\lambda}\ \forall : r$$

A simple transformation τ' exists by (IH).
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 q.e.d.

Example 6. $\neg(\forall x)(\exists y)P(x,y) \sim_s (\exists x)(\forall y)\neg P(x,y)$:
we have shown in Example 3 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 23. *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 9. *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):*

$$\begin{array}{l}(1)\ \neg\neg A \Rightarrow A,\ (2)\ \neg(A \wedge B) \Rightarrow \neg A \vee \neg B,\ (3)\ \neg(A \vee B) \Rightarrow \neg A \wedge \neg B,\\ (4)\ A \to B \Rightarrow \neg A \vee B,\ (5)\ \neg(\forall x)A \Rightarrow (\exists x)\neg A,\ (6)\ \neg(\exists x)A \Rightarrow (\forall x)\neg A.\end{array}$$

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 [1], proposition 4.6.

Proposition 3. *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 9, the left and right sides are strongly equivalent. Then the result follows from Lemma 9 and the fact that $\sim_s$ is compatible and transitive (Proposition 2).

We give the simple transformations corresponding to the rules in $\mathcal{R}$:

(1) $\neg\neg A \sim_s A$:

$$\dfrac{\dfrac{\begin{array}{c}I(A)\\ A \vdash A\end{array}}{\vdash A, \neg A}\ \neg : r}{\neg\neg A \vdash A}\ \neg : l \qquad \dfrac{\dfrac{\begin{array}{c}I(A)\\ A \vdash A\end{array}}{\neg A, A \vdash}\ \neg : l}{A \vdash \neg\neg A}\ \neg : r$$

(2) $\neg(A \wedge B) \sim_s \neg A \vee \neg B$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}I(A)\\ A \vdash A\end{array}\quad\begin{array}{c}I(B)\\ B \vdash B\end{array}}{A, B \vdash A \wedge B}\ \wedge : r}{A, B, \neg(A \wedge B) \vdash}\ \neg : l}{A, \neg(A \wedge B) \vdash \neg B}\ \neg : r}{\neg(A \wedge B) \vdash \neg A, \neg B}\ \neg : r}{\neg(A \wedge B) \vdash \neg A \vee \neg B}\ \vee : r \qquad \dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}I(A)\\ A \vdash A\end{array}}{A, \neg A \vdash}\ \neg : l \quad \dfrac{\begin{array}{c}I(B)\\ B \vdash B\end{array}}{B, \neg B \vdash}\ \neg : l}{A, B, \neg A \vee \neg B \vdash}\ \vee : l}{A \wedge B, \neg A \vee \neg B \vdash}\ \wedge : l}{\neg A \vee \neg B \vdash \neg(A \wedge B)}\ \neg : r$$

(3) $\neg(A \vee B) \sim_s \neg A \wedge \neg B$: symmetric to (2).
(4) $A \to B \sim_s \neg A \vee B$:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}I(A)\\ A \vdash A\end{array}\quad\begin{array}{c}I(B)\\ B \vdash B\end{array}}{A, A \to B \vdash B}\ \to : l}{A \to B \vdash \neg A, B}\ \neg : r}{A \to B \vdash \neg A \vee B}\ \vee : r \qquad \dfrac{\dfrac{\dfrac{\begin{array}{c}I(A)\\ A \vdash A\end{array}}{A, \neg A \vdash}\ \neg : l \quad \begin{array}{c}I(B)\\ B \vdash B\end{array}}{A, \neg A \vee B \vdash B}\ \vee : l}{\neg A \vee B \vdash A \to B}\ \to : r$$

(5) $\neg(\forall x)A \sim_s (\exists x)\neg A$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overset{I(A\{x \leftarrow \alpha\})}{A\{x \leftarrow \alpha\} \vdash A\{x \leftarrow \alpha\}}}{\vdash \neg A\{x \leftarrow \alpha\}, A\{x \leftarrow \alpha\}}\ \neg : r}{\vdash (\exists x)\neg A, A\{x \leftarrow \alpha\}}\ \exists : r}{\vdash (\exists x)\neg A, (\forall x)A}\ \forall : r}{\neg(\forall x)A \vdash (\exists x)\neg A}\ \neg : l \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overset{I(A\{x \leftarrow \alpha\})}{A\{x \leftarrow \alpha\} \vdash A\{x \leftarrow \alpha\}}}{A\{x \leftarrow \alpha\}, \neg A\{x \leftarrow \alpha\} \vdash}\ \neg : l}{(\forall x)A, \neg A\{x \leftarrow \alpha\} \vdash}\ \forall : l}{(\forall x)A, (\exists x)\neg A \vdash}\ \exists : l}{(\exists x)\neg A \vdash \neg(\forall x)A}\ \neg : r$$

(6) $\neg(\exists x)A \sim_s (\forall x)\neg A$: symmetric to (5).

q.e.d.

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 10. *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 4. 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 proceed by cut-elimination on the proof $T(\varphi', \tau_{A,B})$:

$$\dfrac{\overset{\varphi'}{\Gamma \vdash \Delta, A} \quad \overset{\tau_{A,B}}{A \vdash B}}{\Gamma \vdash \Delta, B}\ cut$$

The profile at the node ν is of the form

$$\mathrm{P}(\varphi).\nu = C' \cup D, \quad \text{where } D = \{A_1 \vdash^{l_1} A_1, \ldots, A_m \vdash^{l_n} A_m\}$$

for a set of atoms A_i and labels l_i. Note that all binary inferences in $\tau_{A,B}$ work on ancestors of a cut, so D is the union of all axiom sequents in $\tau_{A,B}$.

Moreover we obtain

$$\mathrm{P}(\varphi) = C \cup D$$

For a clause set C, because – on successors of B (which goes into a pseudo-cut) – only unions are performed in the construction of the proof profile.

We apply cut-elimination based on $\rightarrow_{\mathrm{G_t}}$ in two phases (as defined in Definition 17): 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 $\rightarrow_{\mathrm{G_t}}$ we distinguish a φ'-part (i.e. the part labelled by F, 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:

$$\dfrac{\overset{\rho}{\Pi \vdash \Lambda, C} \quad \overset{\sigma}{C, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ cut$$

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 my change by elimination on negated formulas).

We prove that for all χ with $(\varphi')\tau_{A,B} \rightarrow^{*}_{\mathrm{G_t}} \chi$,we have

$$(\star)\ \mathrm{P}(\varphi[\chi]_\nu) = C\pi \cup D^*,$$

where π is a permutation of eigenvariables and D^* is a set of instances of clauses (modulo label renaming) in D.

We know by Lemmas 4 and 5 that $\rightarrow_{\mathrm{G_r}}$ and $\rightarrow_{\mathrm{G_p}}$ 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.

(1) ξ is of the form

$$\dfrac{\dfrac{\overset{\rho'}{\Pi \vdash \Lambda}}{\Pi \vdash \Lambda, C}\ w:r \quad \overset{\sigma}{C, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ cut$$

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 $\xi' =$

$$\dfrac{\overset{\rho'}{\Pi \vdash \Lambda}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ w^*$$

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 a cut, we may apply Corollary 2 and obtain

$$\mathrm{P}(\varphi[\chi']_\mu) = C\pi \cup D',$$

where D' is a subset of D^*.

(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

$$\dfrac{\dfrac{\overset{\rho'}{\Pi \vdash \Lambda, C, C}}{\Pi \vdash \Lambda, C}\ c:r \quad \overset{\sigma}{C, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\ cut$$

Then $\xi \rightarrow_{\mathrm{G_t}} \xi'$ for $\xi' =$

$$\dfrac{\dfrac{\dfrac{\overset{\rho'}{\Pi \vdash \Lambda, C, C} \quad \overset{\sigma}{C, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda', C}\,\mathit{cut} \qquad \overset{\sigma'}{C, \Pi' \vdash \Lambda'}}{\Pi, \Pi', \Pi' \vdash \Lambda, \Lambda', \Lambda'}\,\mathit{cut}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\,c^*$$

where σ' is σ after renaming of eigenvariables and labels. Again, let $\chi' = \chi[\xi']_\mu$. Then, by Lemma 8,

$$\mathrm{P}(\varphi[\chi']_\nu) = C\pi \cup D^* \cup D',$$

where D' is a set of instances of clauses in D^*.

(3) Elimination of a quantifier:

(3a) $\xi =$

$$\dfrac{\dfrac{\overset{\rho'}{\Pi \vdash \Lambda, A\{x \leftarrow t\}}}{\Pi \vdash \Lambda, (\exists x)A}\,\exists : r \qquad \dfrac{\overset{\sigma'}{A\{x \leftarrow \alpha\}, \Pi' \vdash \Lambda'}}{(\exists x)A, \Pi' \vdash \Lambda'}\,\exists : l}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\,\mathit{cut}$$

Then $\xi \rightarrow_{\mathrm{G_t}} \xi'$ for $\xi' =$

$$\dfrac{\overset{\rho'}{\Pi \vdash \Lambda, A\{x \leftarrow t\}} \quad \overset{\sigma'\{\alpha \leftarrow t\}}{A\{x \leftarrow t\}, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\,\mathit{cut}$$

Then, by Lemma 6,

$$\mathrm{P}(\varphi[\chi']_\nu) = C\pi \cup D^*\{\alpha \leftarrow t\}.$$

Note that α does not occur in $C\pi$! Again, the φ'-part remains unchanged, and the $\tau_{A,B}$-part is instantiated.

(3b) $\xi =$

$$\dfrac{\dfrac{\overset{\rho'}{\Pi \vdash \Lambda, A\{x \leftarrow \alpha\}}}{\Pi \vdash \Lambda, (\forall x)A}\,\forall : r \qquad \dfrac{\overset{\sigma'}{A\{x \leftarrow \beta\}, \Pi' \vdash \Lambda'}}{(\forall x)A, \Pi' \vdash \Lambda'}\,\forall : l}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\,\mathit{cut}$$

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 $\xi \rightarrow_{\mathrm{G_t}} \xi'$ for $\xi' =$

$$\dfrac{\overset{\rho'\{\alpha \leftarrow \beta\}}{\Pi \vdash \Lambda, A\{x \leftarrow \beta\}} \quad \overset{\sigma'}{A\{x \leftarrow \beta\}, \Pi' \vdash \Lambda'}}{\Pi, \Pi' \vdash \Lambda, \Lambda'}\,\mathit{cut}$$

Again, by Lemma 6, we obtain

$$\mathrm{P}(\varphi[\chi']_\nu) = C\pi\{\alpha \leftarrow \beta\} \cup D^*.$$

We know that β is a variable. But β cannot occur in $C\pi$ (i.e. in the φ'-part of the proof) as β is an eigenvariable in $\tau_{A,B}$-part and the proof χ is regular. So we obtain

$$C\pi\{\alpha \leftarrow \beta\} = C\pi\{\alpha \leftarrow \beta,\ \beta \leftarrow \alpha\}$$

where $\pi\{\alpha \leftarrow \beta,\ \beta \leftarrow \alpha\}$ is a 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

$$\mathrm{P}(\varphi[\chi^*]_\nu) = C\pi \cup D^*.$$

where π is a permutation and

$$D^* = \{B_1 \vdash^{j_1} B_1, \ldots, B_r \vdash^{j_r} B_r\}.$$

Now the only cuts left in χ^* are of the form $\xi =$

$$\frac{B^{\{i\}} \vdash B^{\{i\}} \quad B^{\{j\}} \vdash B^{\{j\}}}{B^{\{i\}} \vdash B^{\{j\}}}\ cut$$

Where i is a label in the φ'-part and j is a label in the $\tau_{A,B}$-part. According to the definition of $\rightarrow_{\mathrm{G_t}}$ (Definition 17), ξ is replaced by $\xi' =$

$$B^{\{i\}} \vdash B^{\{i\}}.$$

Let μ be the node of this cut and $\chi' = \chi^*[\xi']$. Then

$$\mathrm{P}(\varphi[\chi']_\nu) = C\pi \cup D^* - \{B \vdash^j B\}.$$

This procedure is repeated till all the clauses in the set D^* are used up. Let us call the resulting proof ψ, which does not contain any marked cuts. Then

$$\mathrm{P}(\varphi[\psi]_\nu) = C\pi.$$

q.e.d.

Corollary 3. *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 10.

Lemma 11. *Let φ be an* **LK***-proof and σ be a subproof of φ (at node ν) of the form*

$$\dfrac{\overset{\sigma_1}{\varGamma \vdash \varDelta, A} \qquad \overset{\sigma_2}{A, \varPi \vdash \varLambda}}{\varGamma, \varPi \vdash \varDelta, \varLambda}\ cut$$

and let A be strongly equivalent to B. Then there exists an **LK***-proof ψ of the form*

$$\dfrac{\overset{\psi_1}{\varGamma \vdash \varDelta, B} \qquad \overset{\psi_2}{B, \varPi \vdash \varLambda}}{\varGamma, \varPi \vdash \varDelta, \varLambda}\ cut$$

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 10 to the subproof σ_1 with the transformation $\tau_{A,B}$. The result is a pseudo-proof $\varphi_1 \colon \varphi[\rho]_\nu$ with $\mathrm{P}(\varphi_1) = \mathrm{P}(\varphi)\pi_1$ for a permutation π_1 and for $\rho =$

$$\dfrac{\overset{\psi_1}{\varGamma \vdash \varDelta, B} \qquad \overset{\sigma_2}{A, \varPi \vdash \varLambda}}{\varGamma, \varPi \vdash \varDelta, \varLambda}\ pscut$$

Then apply Corollary 3 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 $\psi =$

$$\dfrac{\overset{\psi_1}{\varGamma \vdash \varDelta, B} \qquad \overset{\psi_2}{B, \varPi \vdash \varLambda}}{\varGamma, \varPi \vdash \varDelta, \varLambda}\ cut$$

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) q.e.d.

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 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 11, 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 q.e.d.

Corollary 4. *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 3 and Theorem 1.

Corollary 4 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 6); so Theorem 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 [2]).

In Section 3.4 we have shown that profiles define equivalence classes of proofs at least as large as proof nets. Theorem 1 proves that the equivalence classes defined by profiles are in fact larger, due to the strong abstraction from the syntax of cuts.

6 Summary

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 did *not* prove that the profile remains the same when the whole proof (i.e. also the formulas in the end-sequent) undergoes simple transformations. We conjecture that even this stronger result holds (e.g. 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.

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.

Furthermore, it is possible to apply redundancy-elimination techniques from automated theorem proving like tautology-deletion and subsumption to the profile which results in a smaller and thus more readable version of it. While these transformations formally change the set of normal forms, the logical meaning of them is preserved. On the other hand we clearly can regard profiles as equal if they are equivalent w.r.t. variable renaming. Moreover we believe that the analysis can be carried over to **LK**-proofs in second-order logic.

References

1. M. Baaz, U. Egly, A. Leitsch Normal Form Transformations *Handbook of Automated Reasoning*, pp. 273–333, 2001.

2. M. Baaz, A. Leitsch: Cut normal forms and proof complexity, *Annals of Pure and Applied Logic*, 97, pp. 127-177, 1999.
3. M. Baaz, A. Leitsch: Cut-elimination and Redundancy-elimination by Resolution *Journal of Symbolic Computation*, 29(2), pp. 149-176, 2000.
4. M. Baaz, A. Leitsch: Towards a Clausal Analysis of Cut-Elimination, *Journal of Symbolic Computation*, 41, pp. 381–410, 2006.
5. V. Danos, J.-B. Joinet, H. Schellinx: A New Deconstructive Logic: Linear Logic *Journal of Symbolic Logic*, 62(3), pp. 755–807, 1997.
6. V. Danos, J.-B. Joinet, H. Schellinx: Computational isomorphisms in classical logic *Theoretical Computer Science*, 294(3), pp. 353–378, 2003.
7. G. Gentzen: Untersuchungen über das logische Schließen, *Mathematische Zeitschrift* 39, pp. 405–431, 1934–1935.
8. S.C. Kleene: Permutability of Inferences in Gentzen's Calculi LK and LJ, *Memoirs of the American Mathematical Society*, 10, pp. 1–26, 1952.
9. R. McKinley: Categorical Model for First-Order Classical Proofs *PhD thesis, University of Bath*, 2006
10. E. Robinson: Proof Nets for Classical Logic, *Journal of Logic and Computation*, 13(5), pp. 777–797, 2003