Proof Fragments, Cut-Elimination and Cut-Introduction

Stefan Hetzl
Laboratoire Preuves, Programmes et Systèmes (PPS)
Université Paris Diderot
175 Rue du Chevaleret, 75013 Paris, France
stefan.hetzl@pps.jussieu.fr

December 17, 2010

Abstract

Cut-elimination is usually presented as a set of local proof reduction steps together with a terminating strategy thus showing the existence of cut-free proofs for all provable sequents. Viewing cut-elimination as a transformation of mathematical proofs, not only the existence but also the structure and content of the cut-free proofs deserves investigation. In this paper we use proof skeletons to describe the abstract structure of a proof and the changes it undergoes during cut-elimination. We show that a proof can be split up into several minimal fragments which themselves are not modified but merely rearranged and instantiated. This result allows to characterize a certain kind of redundancy whose presence is necessary for a cut-free proof to allow compression by introduction of cuts. We formulate the cut-introduction problem in terms of a variant of Kolmogorov complexity and prove a lower bound based on this characterization.

1 Introduction

Cut-elimination is a proof transformation of fundamental importance. It has been introduced by Gentzen in [12] together with the sequent calculus. A cut-elimination theorem for a calculus has a number of important corollaries among which is the consistency of the system. Viewed as a transformation of mathematical proofs, cut-elimination corresponds to the removal of intermediate statements (lemmas) from a proof. The mathematical interest in this transformation lies in the fact that frequently these lemmas may contain mathematical concepts which do not occur in the theorem that is shown. Removing these lemmas also removes these concepts therefore allowing the computation of an elementary proof from a more abstract one. Such a transformation has for example been applied by Girard in [13, Annex 4.A] to demonstrate that from the topological Fürstenberg-Weiss proof of van der Waerden's theorem the original combinatorial proof can be obtained. As a transformation of formal proofs, cut-elimination

is usually presented as a set of local reduction steps. The changes to the global structure of the proof that are caused by these local rewrite steps are strongly influenced by the original cut formulas. Therefore, on the mathematical level, the abstract concepts – up to a certain degree – determine the form of the elementary argument.

The inverse problem of structuring a given cut-free proof by the introduction of cuts is interesting for the following two reasons: Firstly for the above-mentioned interplay between the structure of the elementary proof and the formulas defining the concepts of the abstract proof. The crucial question in that respect is: Is it possible to read off formulas describing abstract mathematical concepts from the structure of an elementary mathematical proof ? Secondly, it is well-known that cut-elimination (in first-order classical logic) may lead to a non-elementary increase in the size of proofs [23, 21, 22]. It is clear that not all sequences of large (i.e. non-elementarily growing) cut-free proofs admit corresponding sequences of small (i.e. elementarily growing) counterparts with cuts. Some kind of structural regularity, of redundancy, must be necessary for such a strong abbreviation to be possible. The question here is to find a characterization of the redundancy of a proof w.r.t. the introduction of cuts. A partial answer to this question will be provided in this paper by exhibiting a necessary (although not sufficient) condition for a proof to allow an abbreviation by the introduction of cuts. Cut-introduction has also applications in computer science since computer-generated proofs are typically analytic. In [9] several preprocessing and optimization techniques for automated theorem proving are shown to be representable by inserting cuts into a proof. In [20], the introduction of atomic cuts is used in the context of proof search for logic programming.

We will treat the above questions based on the level of *proof skeletons*, i.e. trees representing the structure of a proof. Proof skeletons allow to split a first-order proof into two levels: The propositional structure and the term structure. The relation between these two levels is interesting, often surprising and has been studied for example in [18, 10, 8, 7]. We will show that a proof skeleton can be divided into several minimal fragments which themselves are not modified by cut-elimination but only rearranged and instantiated. Therefore, a cut-free proof is shown to be a composition of instances of the minimal fragments of the original proof. This in turn allows to read off the possible building blocks of the skeleton of the proof with cuts from the one without cuts. Therefore it is possible to compute a lower bound on the size of a proof with cuts leading to a given cut-free proof. Although our analysis concerns usual cut-elimination by local rewrite steps, many of our proofs are strongly based on another, more general, cut-elimination method: Cut-elimination by resolution (Ceres), which has been introduced in [4] and will be explained in Section 2. In Section 3 we will establish the relation between the Ceres-method and the proof skeletons. In Section 4 we will use constructions of the Ceres-method to prove the above mentioned behavior of the minimal fragments. In Section 5 the problem of cut-introduction will be formalized in terms of a variant of Kolmogorov complexity and a lower bound will be provided.

2 Cut-Elimination by Resolution

Cut-elimination by resolution (Ceres) is a method for cut-elimination which has been introduced in [4]. It has been extended considerably to cover calculi enriched with definition handling and equality reasoning [1] and also many-valued logics [5]. An implementation of this method (and several examples) are available at `http://www.logic.at/ceres/`. It has been used to analyze a formalization of Fürstenberg's topological proof of the infinity of primes [11] showing that Euclid's elementary argument can be obtained by cut-elimination, see [2]. In the author's PhD thesis [14, 15] a refinement of the method, taking dependencies between rules and axioms into account, has been developed. This refinement, whose usage is crucial to obtain the results presented in this paper, is briefly described in this section.

2.1 The Sequent Calculus

We will investigate various proof transformations which would be very inconvenient in a calculus including explicit exchange- or permutation-rules. Still we want to track different occurrences of the same formula, which leads us to using a sequent calculus based on indexed formulas. An indexed formula is a pair consisting of a formula F and an index $i \in \mathbb{N}$ and is written as $F_{[i]}$. A sequent is a pair of sets of indexed formulas. In a sequent calculus proof each formula occurrence is an ancestor either of a cut or of a formula in the end-sequent. Following [24] we call the former *implicit* and the latter *explicit*. For our purposes it will be convenient to express this distinction already at the level of formula indices. Therefore we assume a partition $\mathcal{I} \uplus \mathcal{E} = \mathbb{N}$ for the indices, e.g. $\mathcal{I} := \{2k \mid k \in \mathbb{N}\}$ and $\mathcal{E} := \{2k+1 \mid k \in \mathbb{N}\}$.

Definition 1. The rules of **LK** are the following:

1. Axiom sequents are of the form:

$$A_{[i]} \vdash A_{[j]} \quad \text{for an atomic formula } A$$

2. Logical Rules

$$\frac{\Gamma \vdash \Delta, A_{[i]} \quad \Pi \vdash \Lambda, B_{[j]}}{\Gamma, \Pi \vdash \Delta, \Lambda, (A \wedge B)_{[k]}} \wedge : \mathrm{r}$$

$$\frac{A_{[i]}, \Gamma \vdash \Delta}{(A \wedge B)_{[k]}, \Gamma \vdash \Delta} \wedge : \mathrm{l1} \qquad \frac{B_{[i]}, \Gamma \vdash \Delta}{(A \wedge B)_{[k]}, \Gamma \vdash \Delta} \wedge : \mathrm{l2}$$

$$\frac{A_{[i]}, \Gamma \vdash \Delta \quad B_{[j]}, \Pi \vdash \Lambda}{(A \vee B)_{[k]}, \Gamma, \Pi \vdash \Delta, \Lambda} \vee : \mathrm{l}$$

$$\frac{\Gamma \vdash \Delta, A_{[i]}}{\Gamma \vdash \Delta, (A \vee B)_{[k]}} \vee : \mathrm{r1} \qquad \frac{\Gamma \vdash \Delta, B_{[i]}}{\Gamma \vdash \Delta, (A \vee B)_{[k]}} \vee : \mathrm{r2}$$

$$\frac{\Gamma \vdash \Delta, A_{[i]} \quad B_{[j]}, \Pi \vdash \Lambda}{(A \to B)_{[k]}, \Gamma, \Pi \vdash \Delta, \Lambda} \to : \mathrm{l}$$

$$\frac{A_{[i]}, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, (A \to B)_{[k]}} \to : \mathrm{r1} \qquad \frac{\Gamma \vdash \Delta, B_{[i]}}{\Gamma \vdash \Delta, (A \to B)_{[k]}} \to : \mathrm{r2}$$

$$\frac{\Gamma \vdash \Delta, A_{[i]}}{(\neg A)_{[k]}, \Gamma \vdash \Delta}\ \neg : \mathrm{l} \qquad \frac{A_{[i]}, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, (\neg A)_{[k]}}\ \neg : \mathrm{r}$$

$$\frac{A\{x \leftarrow t\}_{[i]}, \Gamma \vdash \Delta}{((\forall x)A)_{[k]}, \Gamma \vdash \Delta}\ \forall : \mathrm{l} \qquad \frac{\Gamma \vdash \Delta, A\{x \leftarrow \alpha\}_{[i]}}{\Gamma \vdash \Delta, ((\forall x)A)_{[k]}}\ \forall : \mathrm{r}$$

$$\frac{\Gamma \vdash \Delta, A\{x \leftarrow t\}_{[i]}}{\Gamma \vdash \Delta, ((\exists x)A)_{[k]}}\ \exists : \mathrm{r} \qquad \frac{A\{x \leftarrow \alpha\}_{[i]}, \Gamma \vdash \Delta}{((\exists x)A)_{[k]}, \Gamma \vdash \Delta}\ \exists : \mathrm{l}$$

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

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

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

3. Structural Rules

$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A_{[k]}}\ \mathrm{w} : \mathrm{r} \qquad \frac{\Gamma \vdash \Delta}{A_{[k]}, \Gamma \vdash \Delta}\ \mathrm{w} : \mathrm{l}$$

$$\frac{A_{[i]}, A_{[j]}, \Gamma \vdash \Delta}{A_{[k]}, \Gamma \vdash \Delta}\ \mathrm{c} : \mathrm{l} \qquad \frac{\Gamma \vdash \Delta, A_{[i]}, A_{[j]}}{\Gamma \vdash \Delta, A_{[k]}}\ \mathrm{c} : \mathrm{r}$$

$$\frac{\Gamma \vdash \Delta, A_{[i]} \quad A_{[j]}, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{cut}$$

An **LK**-proof is a tree where each node is labelled by a rule and its conclusion sequent fulfilling the following conditions:

1. For each axiom: $i \neq j$, for each other rule: the introduced index k is new, i.e. it does not occur in the proof above. For each binary rule: there is no index that occurs in both subproofs.

2. For each cut: $i, j \in \mathcal{I}$, for each rule except cut: either $i, j, k \in \mathcal{I}$ or $i, j, k \in \mathcal{E}$.

We treat axioms as nullary rules. An axiom has therefore two main indices but no auxiliary index. For the other (including the structural) rules, auxiliary and main indices are defined as usual. An index i is active in a rule if it is main or auxiliary, otherwise it is called context index. A rule will be called explicit or implicit according to the type of its main and auxiliary indices. An axiom will be called explicit if at least one index is in $\mathcal{E}$ and implicit otherwise. In writing down proofs or defining proof transformations we will often omit the indices if their choice is obvious or irrelevant. For defining the Ceres-method it will be useful to track axiom occurrences in a proof and in structures derived from it. This will be done by using an element of $\mathbb{N} \times \mathbb{N}$ as *axiom identifier*. The identifier of an axiom is the pair of formula indices in this axiom.

2.2 Clause Logic

A clause is a sequent containing only atomic formulas. We will consider clauses which are labelled by sets of axiom identifiers. For a clause c we write $\mathcal{A}(c)$ to denote this set. We will use the notation $\Gamma \vdash^A \Delta$ for the clause $\Gamma \vdash \Delta$ labelled with the set A of axiom identifiers. The *merge* of two clauses $\Gamma \vdash^A \Delta$ and $\Pi \vdash^B \Lambda$ is $\Gamma \vdash^A \Delta \circ \Pi \vdash^B \Lambda := \Gamma, \Pi \vdash^{A \cup B} \Delta, \Lambda$. The merge operation will also be used on sequents in an analogous way. Let C, D be clause sets. The *product* of C and D is $C \times D := \{c \circ d \mid c \in C, d \in D\}$. A *clause selection formula* is a propositional formula built up from sets of axiom identifiers as atoms and the connectives $\wedge, \vee, \neg$. For a clause c and a set of axiom identifiers A we will say that c *is an* A*-clause* if $A \cap \mathcal{A}(c) \neq \emptyset$.

Definition 2. Let C be a clause set, let A be a set of axiom identifiers and let F and G be clause selection formulas. We define:

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

Note that $C^{A_1 \wedge A_2} \neq C^{A_1 \cap A_2}$. Consider for example $C = \{P \vdash^{\{a_1, a_2\}} Q\}$. Then $C^{\{a_1\} \wedge \{a_2\}} = C$ but $C^{\{a_1\} \cap \{a_2\}} = C^\emptyset = \emptyset$. In contrast $C^{A_1 \vee A_2} = C^{A_1 \cup A_2}$ as can be easily verified.

Definition 3. Let C, D be clause sets and F be a clause selection formula. We define the restricted product as

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

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 $C \times_F D$ which in turn implies $C \times D$ for all clause selection formulas F.

2.3 The Ceres-Method

The Ceres-method is based on the resolution calculus. As a preprocessing we skolemize the input proof with cuts. The skolemization of a proof consists in removing the strong quantifiers (i.e. positive $\forall$ and negative $\exists$) from its end-sequent and replacing the variables bound by these quantifiers by skolem terms. A skolemized proof therefore is one which does not contain strong quantifiers in its end-sequent. The interested reader is referred to [3] for a description of an algorithm for proof skolemization. Denoting with $|\pi|$ the number of rules in π, the main theorem of the Ceres-method can be stated as follows:

Theorem 1. Let π be a skolemized proof of $\Gamma \vdash \Delta$. Then

1. there is an unsatisfiable set of clauses $\mathrm{P}(\pi)$ s.t.
2. for all $c \in \mathrm{P}(\pi)$ there is a proof ψ of $(\Gamma \vdash \Delta) \circ c$ s.t.
   (a) ψ is cut-free and (b) $|\psi| \leq |\pi|$.

The clause set $\mathrm{P}(\pi)$ is called *profile* of π, the proof ψ is called *projection* (of π to the clause c). This theorem gives rise to a cut-elimination method as follows: Compute a resolution refutation γ of $\mathrm{P}(\pi)$. Compute a ground resolution refutation γ' of a set of instances of $\mathrm{P}(\pi)$. Convert γ' to a sequent calculus proof by replacing resolution by cut and the instances of $\mathrm{P}(\pi)$ by instances of the respective projections. The result is a proof of $\Gamma \vdash \Delta$ using only atomic cuts.

Starting with a skolemized proof is necessary for the following two reasons: Firstly it ensures that in γ there are no substitutions which replace eigenvariables of strong quantifiers in the end-sequent (as there are no such quantifiers anymore). Secondly, it ensures that the projections do not contain violations of eigenvariable conditions. Starting from a non-skolemized proof, the definitions of the profile and the projections can still be applied, however Theorem 1 fails, in particular, a projection will only be a *semi-proof*, i.e. a proof possibly containing violations of eigenvariable conditions. In this paper however, we will use the profile and the projections not for the purpose of cut-elimination by resolution, but instead as tools for analyzing the structure of proofs. Therefore we do not need Theorem 1 and our investigation applies to all, i.e. also the non-skolemized, proofs.

We now turn to the details of the Ceres-method: For a proof π and a formula index i we define $\mathcal{A}_\pi(i) \subseteq \mathbb{N} \times \mathbb{N}$ as the set of axiom identifiers containing an ancestor of i in π. For a rule ρ we define $\mathcal{A}_\pi(\rho)$ as $\mathcal{A}_\pi(i) \cup \mathcal{A}_\pi(j)$ if ρ has the two auxiliary indices i and j and as $\mathcal{A}_\pi(i)$ if ρ has only one auxiliary index i. For a rule ρ and a set of indices U we say that ρ *operates on* U if all the active indices of ρ are in U. For a sequent s and a set of formula indices M, we write $\mathrm{S}(s, M)$ for the subsequent of s indexed by elements of M.

Definition 4. Let π be a proof. We define the *profile* $\mathrm{P}(\pi)$ by induction on the structure of π.

1. If π is an axiom s, then
$$\mathrm{P}(\pi) := \begin{cases} \emptyset & \text{if } \mathrm{S}(s, \mathcal{I}) = s \\ \{\mathrm{S}(s, \mathcal{I})\} & \text{if } \mathrm{S}(s, \mathcal{I}) \neq s \end{cases}$$
2. If π ends with a unary rule, let π' be its immediate subproof and define
$$\mathrm{P}(\pi) := \mathrm{P}(\pi')$$
3. If π ends with a binary rule ρ, let π_1, π_2 be its immediate subproofs.
   (a) If ρ is implicit, then
   $$\mathrm{P}(\pi) := \mathrm{P}(\pi_1) \cup \mathrm{P}(\pi_2)$$
   (b) If ρ is explicit, then
   $$\mathrm{P}(\pi) := \mathrm{P}(\pi_1) \times_{\mathcal{A}_\pi(\rho)} \mathrm{P}(\pi_2)$$

We will now describe the projections of a proof. A proof π induces an ancestor relation on the set of formula indices occurring in π: An auxiliary index is direct ancestor of the main index of the same rule. The ancestor relation is the reflexive and transitive closure of the direct ancestor relation. The part of the ancestor relation that is induced by contraction-rules only will play an important part later on, so it deserves its own notation.

Definition 5. Let π be a proof and i and j indices. We define $i \leq^1_\pi j$ if π contains a contraction with main index i and an auxiliary index j. We write $\leq_\pi$ for the reflexive and transitive closure of $\leq^1_\pi$.

Let s and s' be sequents and π a proof. We write $s' \leq_\pi s$ if there is a bijection f from the indices of s' into those of s s.t. the formulas are preserved by f and $i \leq_\pi f(i)$ for all i. Note that if $s' \leq_\pi s$ then s' and s only differ in the indices. Let π be a proof, U be a set of indices and let $c \in \mathrm{P}(\pi)$. Then we write $U_\pi(c)$ for the set $\{i \in U \mid \mathcal{A}_\pi(i) \cap \mathcal{A}(c) \neq \emptyset\}$.

Proposition 1. Let π be a proof of a sequent s and let $c \in \mathrm{P}(\pi)$. Then there is a cut-free semi-proof $\Psi(\pi, c)$, the *projection* of π to c, of a sequent s' with $\mathrm{S}(s, \mathcal{E}_\pi(c)) \circ c \ \leq_\pi \ s'$ and furthermore $|\Psi(\pi, c)| \leq |\pi|$.

Proof. We proceed by induction on π. The claim $\mathrm{S}(s, \mathcal{E}_\pi(c)) \circ c \ \leq_\pi \ s'$ will follow from choosing the indices introduced into $\Psi(\pi, c)$ appropriately. The claim $|\Psi(\pi, c)| \leq |\pi|$ will follow from the observation that we add at most one rule to $\Psi(\pi, c)$ for each rule of π.

1. If π is an axiom, define $\Psi(\pi, c) := \pi$.
2. If π ends with a unary rule ρ, let π' be π without ρ. For $c \in \mathrm{P}(\pi)$ we also have $c \in \mathrm{P}(\pi')$.
   (a) If ρ does not operate on $\mathcal{E}_\pi(c)$, define $\Psi(\pi, c) := \Psi(\pi', c)$.
   (b) If ρ operates on $\mathcal{E}_\pi(c)$, then ρ cannot be weakening as the main index of a weakening has no ancestor axioms.
      i. If ρ is a logical rule, then it has exactly one auxiliary index i in π. The formula of i occurs in the end-sequent of $\Psi(\pi', c)$ with an index $j \geq_\pi i$. Define
      $$\Psi(\pi, c) := \frac{\Psi(\pi', c)}{} \ \rho$$
      applying ρ to j creating the same main index as in π.
      ii. If ρ is a contraction, let k be its main index and i_1, i_2 its auxiliary indices. As $\mathcal{A}_\pi(k) \cap \mathcal{A}(c) \neq \emptyset$ also $\mathcal{A}_\pi(i_n) \cap \mathcal{A}(c) \neq \emptyset$ for at least one $n \in \{1, 2\}$, let w.l.o.g. $n = 1$.
         A. If also $\mathcal{A}_\pi(i_2) \cap \mathcal{A}(c) \neq \emptyset$, then the end-sequent of $\Psi(\pi', c)$ contains indices $j_1 \geq_\pi i_1$ and $j_2 \geq_\pi i_2$. Define
         $$\Psi(\pi, c) := \frac{\Psi(\pi', c)}{} \ \rho$$
         applying ρ to j_1, j_2 creating the same main index as in π.

B. If $\mathcal{A}_\pi(i_2) \cap \mathcal{A}(c) = \emptyset$, define $\Psi(\pi, c) := \Psi(\pi', c)$.

3. If π ends with a binary rule ρ, let π_1, π_2 be the immediate sub-proofs of π.

   (a) If ρ does not operate on $\mathcal{E}_\pi(c)$, then either ρ operates on $\mathcal{I}$, in which case $c \in \mathrm{P}(\pi_1) \cup \mathrm{P}(\pi_2)$ or it operates on $\mathcal{E} \setminus \mathcal{E}_\pi(c)$ in which case even $c \in \mathrm{P}(\pi_1)^{\neg \mathcal{A}_\pi(\rho)} \cup \mathrm{P}(\pi_2)^{\neg \mathcal{A}_\pi(\rho)}$. In any case, for $c \in \mathrm{P}(\pi_i)$ define $\Psi(\pi, c) := \Psi(\pi_i, c)$.

   (b) If ρ operates on $\mathcal{E}_\pi(c)$, then $\mathcal{A}(c) \cap \mathcal{A}_\pi(\rho) \neq \emptyset$ and $c = c_1 \circ c_2$ with $c_n \in \mathrm{P}(\pi_n)$ and $\mathcal{A}(c) \cap \mathcal{A}_\pi(\rho) \neq \emptyset$ for both $n \in \{1, 2\}$. Letting i_n be the auxiliary index of ρ in π_n, by the induction hypothesis the end-sequent of $\Psi(\pi_n, c_n)$ contains an index $j_n \geq_\pi i_n$. Define

$$\Psi(\pi, c) := \frac{\Psi(\pi_1, c_1) \quad \Psi(\pi_2, c_2)}{} \; \rho$$

   applying ρ to j_1, j_2 creating the same main index as in π.

□

We will write $\Psi(\pi)$ for $\{\Psi(\pi, c) \mid c \in \mathrm{P}(\pi)\}$.

Proof Sketch of Theorem 1. The unsatisfiability of $\mathrm{P}(\pi)$ is shown by constructing a sequent calculus derivation of $\vdash$ using clauses from $\mathrm{P}(\pi)$ as initial sequents as in [4, Proposition 3.2]. The projections are constructed as in the above proof of Proposition 1 where the assumption of a skolemized input proof ensures that step 2(b)i does not introduce an eigenvariable violation. The end-sequents $s \circ c$ as stated in Theorem 1 can be derived from the sequents $s' \geq_\pi \mathrm{S}(s, \mathcal{E}_\pi(c)) \circ c$ by weakening (and renaming of indices). □

3 Proof Fragments and Projections

3.1 Proof Fragments

The skeleton of a proof is – roughly speaking – the proof tree with rule labels but without formulas. Skeletons are usually (e.g. in [18] and [8]) defined based on a calculus which contains a permutation rule which has the consequence that not only the tree structure of the proof is determined by the skeleton but also the ancestor relation of the formula occurrences, a fact which is crucial for various decidability results. In our setting we are working without permutation rules to allow a more flexible treatment of proof transformations. This however has the consequence that formula indices are to be carried over into skeletons which makes their definition technically more complex. Nevertheless the notion of skeleton defined below has the same natural correspondence to our calculus as the skeleton notion of [18, 8] to the respective calculus.

Definition 6. A proof skeleton S together with two associated sets of indices $\mathrm{Idx}^-(S)$ and $\mathrm{Idx}^+(S)$ is defined by induction as follows:

1. For any indices i and j, $S := \bullet\ \mathrm{ax}_{(i,j)}$ is a skeleton, $\mathrm{Idx}^-(S) := \{i\}$ and $\mathrm{Idx}^+(S) := \{j\}$.

2. If S' is a skeleton with $i \in \mathrm{Idx}^-(S')$ and $j \in \mathrm{Idx}^+(S')$, then

$$S := \begin{array}{c} S' \\ | \\ \bullet \; \to : \mathrm{r}_{(i,j;k)} \end{array}$$

is a skeleton with $\mathrm{Idx}^-(S) := \mathrm{Idx}^-(S') \setminus \{i\}$ and $\mathrm{Idx}^+(S) := (\mathrm{Idx}^+(S') \setminus \{j\}) \cup \{k\}$.

3. If S_1 and S_2 are skeletons with $i \in \mathrm{Idx}^+(S_1)$ and $j \in \mathrm{Idx}^-(S_2)$, then

$$S := \begin{array}{ccc} S_1 & & S_2 \\ & \diagdown \quad \diagup & \\ & \bullet \; \to : \mathrm{l}_{(i,j;k)} & \end{array}$$

is a skeleton with $\mathrm{Idx}^-(S) := \mathrm{Idx}^-(S_1) \cup (\mathrm{Idx}^-(S_2) \setminus \{j\}) \cup \{k\}$ and $\mathrm{Idx}^+(S) := (\mathrm{Idx}^+(S_1) \setminus \{i\}) \cup \mathrm{Idx}^+(S_2)$.

Continue analogously for the all other rules of **LK**. Furthermore, skeletons must fulfill the conditions 1 and 2 of the sequent calculus on indices.

A skeleton will often be denoted as $S = (V, E, \tau)$ where V and E are the vertices and edges of the underlying tree and τ assigns rule labels to the vertices. The skeleton of a proof π is denoted as $\mathrm{S}(\pi)$ and defined in the obvious way by removing all formulas. The notation $i \leq_\pi j$ for a proof π and indices i, j is carried over to skeletons analogously.

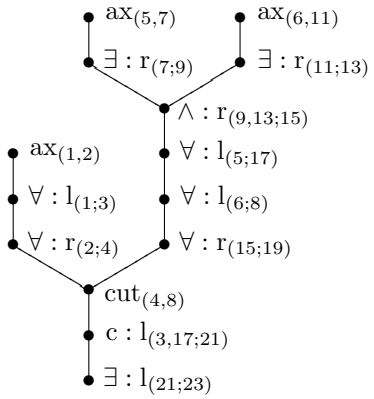
Example 1. Consider the proof $\pi =$

$$\dfrac{\dfrac{\dfrac{\dfrac{P(\alpha, f(\beta)) \vdash P(\alpha, f(\beta))}{(\forall y)P(\alpha, y) \vdash P(\alpha, f(\beta))}\,\forall : \mathrm{l}}{(\forall y)P(\alpha, y) \vdash (\forall y)P(\alpha, f(y))}\,\forall : \mathrm{r} \qquad (\pi') \\ (\forall y)P(\alpha, y), (\forall y)P(\alpha, y) \vdash (\forall y)((\exists x)P(x, y) \wedge (\exists x)P(x, f(y)))}\,\mathrm{cut} \qquad (\forall y)P(\alpha, f(y)), \ldots \vdash \ldots \\ (\forall y)P(\alpha, y) \vdash (\forall y)((\exists x)P(x, y) \wedge (\exists x)P(x, f(y)))}\,\mathrm{c} : \mathrm{l} \\ (\exists x)(\forall y)P(x, y) \vdash (\forall y)((\exists x)P(x, y) \wedge (\exists x)P(x, f(y)))}\,\exists : \mathrm{l}$$

where $\pi' =$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(\alpha, \gamma) \vdash P(\alpha, \gamma)}{P(\alpha, \gamma) \vdash (\exists x)P(x, \gamma)}\,\exists : \mathrm{r} \qquad \dfrac{P(\alpha, f(\gamma)) \vdash P(\alpha, f(\gamma))}{P(\alpha, f(\gamma)) \vdash (\exists x)P(x, f(\gamma))}\,\exists : \mathrm{r}}{P(\alpha, f(\gamma)), P(\alpha, \gamma) \vdash (\exists x)P(x, \gamma) \wedge (\exists x)P(x, f(\gamma))}\,\wedge : \mathrm{r}}{P(\alpha, f(\gamma)), (\forall y)P(\alpha, y) \vdash (\exists x)P(x, \gamma) \wedge (\exists x)P(x, f(\gamma))}\,\forall : \mathrm{l}}{(\forall y)P(\alpha, f(y)), (\forall y)P(\alpha, y) \vdash (\exists x)P(x, \gamma) \wedge (\exists x)P(x, f(\gamma))}\,\forall : \mathrm{l}}{(\forall y)P(\alpha, f(y)), (\forall y)P(\alpha, y) \vdash (\forall y)((\exists x)P(x, y) \wedge (\exists x)P(x, f(y)))}\,\forall : \mathrm{r}$$

Assuming an appropriate choice of the formula indices, the skeleton S(π) is



In the above proof we have $21 \leq_\pi 3$ and $21 \leq_\pi 17$. All other pairs i, j of indices with $i \leq_\pi j$ are trivial, i.e. $i = j$.

Just as rules in a sequent calculus proof are either implicit or explicit, so are nodes in a proof skeleton. Again, we use the convention to call an axiom node explicit if at least one of its main occurrences is ancestor of the end-sequent and implicit otherwise. Given a graph $G = (V; E)$, paths(E) is defined as the transitive closure of E. For a set X, a relation $R \subseteq X \times X$ and a set $Y \subseteq X$ we write $R \restriction Y$ for $\{(x_1, x_2) \in R \mid x_1, x_2 \in Y\}$. So, in particular, for a graph $G = (V; E)$ and a set of vertices $V' \subseteq V$, paths(E) $\restriction V'$ are all pairs of nodes from V' which are connected by a path in G.

Definition 7. Let $T = (V; E)$ be a tree. A graph $T' = (V'; E')$ is called *inner tree* of T if $V' \subseteq V$ and paths(E') = paths(E) $\restriction V'$.

Note that T' is a tree too and that being inner tree is a transitive relation.

Definition 8. Let $S_1 = (V_1, E_1, \tau_1)$ and $S_2 = (V_2, E_2, \tau_2)$ be skeletons. S_1 is called *subskeleton* of S_2, written as $S_1 \subseteq S_2$, if

1. (V_1, E_1) is inner tree of (V_2, E_2) and
2. For all $v \in V_1$:
   (a) $\tau_1(v)$ and $\tau_2(v)$ have the same rule type
   (b) For a main index i_1 in $\tau_1(v)$ and the corresponding main index i_2 in $\tau_2(v)$: $i_1 = i_2$.
   (c) For an auxiliary index i_1 in $\tau_1(v)$ and the corresponding index i_2 in $\tau_2(v)$: $i_2 \leq_{S_2} i_1$.

The rationale for the above point 2c is that in a subskeleton certain parts of the proof do no longer exist. This in turn makes certain contractions superfluous which therefore also do no longer exist in the subskeleton. The missing contractions are reflected on the level on indices by updating the indices below these contractions to point to $\leq_{S_2}$-larger indices. This effect is illustrated in Example 2 below.

Lemma 1. Let $S_1 = (V_1, E_1, \tau_1)$, $S_2 = (V_2, E_2, \tau_2)$ and $S_3 = (V_3, E_3, \tau_3)$ be skeletons and i, k indices. Then

1. If $S_1 \subseteq S_2$ then $k \leq_{S_1} i$ implies $k \leq_{S_2} i$.
2. If $S_1 \subseteq S_2$ and $S_2 \subseteq S_3$ then $S_1 \subseteq S_3$.

Proof. 1 is shown easily by using the subskeleton conditions and 2 follows from 1 and the transitivity of being inner tree.

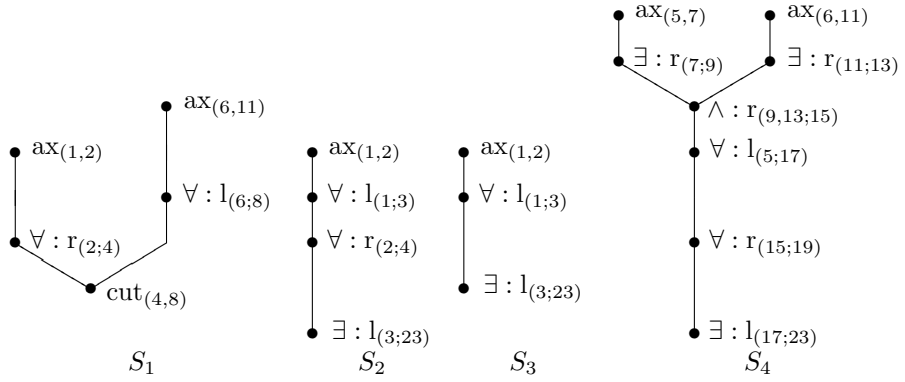
□

S' is a *proper subskeleton* of S, written as $S' \subset S$, if $S' \subseteq S$ and $S' \neq S$

Definition 9. Let $S \subseteq S'$ be proof skeletons and let U be a set of indices. S is called *U-closed w.r.t. S'* if: For all non-contraction nodes $v \in S$ and $w \in S'$ s.t. v has a main index $i \in U$ and w has an auxiliary index $j \leq_{S'} i$ also $w \in S$.

Definition 10. Let S be a proof skeleton. A subskeleton $F \subseteq S$ is called *fragment* of S if it contains at least one explicit node and is $\mathcal{E}$-closed w.r.t. S. A fragment F is called *minimal* if there is no fragment F' which is a proper subskeleton of F. The set of fragments of S is denoted as $\mathcal{F}(S)$, the set of minimal fragments of S as $\mathcal{M}(S)$.

Example 2. Consider the following proof skeletons:



All of them are subskeletons of $\mathrm{S}(\pi)$ of Example 1. Observe that the auxiliary index of the $\exists$: l-rule at the root of π changes according to the subskeleton condition: Its original value in π is 21 but as $21 \leq_\pi 3$ and $21 \leq_\pi 17$ it can in addition take the values 3 and 17 in subskeletons (which corresponds to the deletion of different parts in the skeleton above). S_1 is not a fragment of $\mathrm{S}(\pi)$ because $1 \in \mathcal{E}$ and the node labelled with $\mathrm{ax}_{(1,2)}$ appears in S_1 but the one labelled with $\forall$: $\mathrm{l}_{(1;3)}$ does not. S_2 is a fragment of $\mathrm{S}(\pi)$ but it is not a minimal fragment because $S_3 \subset S_2$ and S_3 is a fragment. The set of minimal fragments of π is $\mathcal{M}(\mathrm{S}(\pi)) = \{S_3, S_4\}$.

3.2 Characterization of the Minimal Fragments

In this and the next section, we will show that the minimal fragments of a proof are exactly the skeletons of the projections by characterizing both as those fragments which contain only explicit nodes and no weakening.

Definition 11. Let $T = (V; E)$ and $T' = (V'; E')$ be trees. T' is called *subtree-residue of* T if there are subtrees $T_1 = (V_1; E_1), \ldots, T_n = (V_n; E_n)$ of T s.t. $V' = V \setminus (V_1 \cup \ldots \cup V_n)$ and $E' = E \restriction V'$.

For a graph G, let $\mathrm{V}(G)$ denote the vertices and $\mathrm{E}(G)$ the edges of G. The cardinality of a graph is defined as $|G| := |\mathrm{V}(G)|$.

Lemma 2. Let S be a skeleton. If F is a fragment of S s.t. 1. F contains only explicit nodes and 2. F does not contain weakening, then F is a minimal fragment of S.

Proof. Given F fulfilling 1 and 2, assume there would be a fragment F' with $F' \subset F$. We show that this assumption leads to a contradiction by exhibiting a list of subtree-residues $R_{|F|}, R_{|F|-1}, \ldots, R_1, R_0$ of F which is decreasing in the sense that $|R_k| = k$ until $R_0 = (\emptyset, \emptyset)$ and for all $k \in \{0, \ldots, |F|\}$: $F' \subseteq R_k$. Let $R_{|F|} := F$ and observe that it fulfills the desired properties.

For constructing the rest of the sequence, let us assume that there is a subtree-residue R of size $n + 1$ with $F' \subseteq R$ and show that there is also a subtree-residue R' of size n with $F' \subseteq R'$. R' is defined as follows: If there is a $v \in \mathrm{leaves}(R) \setminus \mathrm{leaves}(F)$ then – as $v \notin \mathrm{leaves}(F)$ – v is not an axiom. In a proof skeleton however a non-axiom node cannot be a leaf, and as F' is a proof skeleton and $F' \subseteq R$, we have $v \notin F'$ and can define $V^- := \mathrm{V}(R) \setminus \{v\}$, $E^- := \mathrm{E}(R) \restriction V^-$ and $R' := (V^-; E^-)$ which has the desired property $F' \subseteq R'$.

If $\mathrm{leaves}(R) \setminus \mathrm{leaves}(F) = \emptyset$, i.e. $\mathrm{leaves}(R) \subseteq \mathrm{leaves}(F)$, then we claim that there is a $w \in R$ which is unary (i.e. has exactly one child) in R and binary (i.e. has two exactly children) in F. To show this, let X be any maximal (w.r.t. $\subseteq$ on the vertices) tree that is contained in $F \setminus R$. Such a tree exists because R is a subtree-residue of F. Let w be the first node below X that is in R. Then w must be binary in F for assume it would be unary, then w would be in $\mathrm{leaves}(R) \setminus \mathrm{leaves}(F)$ which is empty by assumption. But w is unary in R because no node from X is in R.

Let now w_1 be an uppermost node that is unary in R and binary in F, let X be the subtree immediately above w_1 which is in $F \setminus R$ and let Y be the other subtree which is in R as w_1 was chosen uppermost. Let i be the auxiliary index of w_1 on the side of X. As $F' \subseteq R$ and $X \cap R = \emptyset$, i does not occur as main index of a node in F' and therefore w_1 cannot occur in F' at all. As Y is a weakening-free skeleton, there is a list of vertices $w_1, \ldots, w_k$ with $w_2, \ldots, w_k \in Y$ s.t. w_k is an axiom and $\forall j \in \{1, \ldots, k-1\}$ there are indices i, i' s.t. i is auxiliary index for w_j, i' is main index of w_{j+1} and $i \leq_F i'$. But F' is $\mathcal{E}$-closed w.r.t. S and contains only explicit rules, so none of the w_j can be in F' because w_1 is not in F'. Define $V^- := \mathrm{V}(R) \setminus \{w_k\}$, $E^- := \mathrm{E}(R) \restriction V^-$, $R' := (V^-; E^-)$ and observe that R' is a subtree-residue of size n with $F' \subseteq R'$. □

In order to prove the converse of the above lemma, we need some preparatory notions about the removal of weakening-rules from a proof.

Definition 12. We define a reduction relation $\to^{\mathrm{w}}$ on proofs as follows: Let ρ

be a weakening rule. If ρ is the last rule in the proof, define

$$\dfrac{\dfrac{(\chi)}{\Gamma \vdash \Delta}}{\Gamma \vdash \Delta, A}\ \mathrm{w:r} \qquad \to^{\mathrm{w}} \qquad \dfrac{(\chi)}{\Gamma \vdash \Delta}$$

Otherwise, there is a rule ρ' immediately below ρ. If the main occurrence of ρ is in the context of ρ', then exchange ρ and ρ', e.g. for ρ' being $\wedge$: l1 define

$$\dfrac{\dfrac{\dfrac{(\chi)}{A, \Gamma \vdash \Delta}}{A, \Gamma \vdash \Delta, C}\ \mathrm{w:r}}{A \wedge B, \Gamma \vdash \Delta, C}\ \wedge : \mathrm{l1} \qquad \to^{\mathrm{w}} \qquad \dfrac{\dfrac{\dfrac{(\chi)}{A, \Gamma \vdash \Delta}}{A \wedge B, \Gamma \vdash \Delta}\ \wedge : \mathrm{l1}}{A \wedge B, \Gamma \vdash \Delta, C}\ \mathrm{w:r}$$

Otherwise the main occurrence of ρ is auxiliary occurrence of ρ'. If ρ' is a contraction, then delete both ρ and ρ', i.e.

$$\dfrac{\dfrac{\dfrac{(\chi)}{\Gamma \vdash \Delta, A_{[i]}}}{\Gamma \vdash \Delta, A_{[i]}, A_{[j]}}\ \mathrm{w:r}}{\Gamma \vdash \Delta, A_{[k]}}\ \mathrm{c:r} \qquad \to^{\mathrm{w}} \qquad \dfrac{(\chi)}{\Gamma \vdash \Delta, A_{[i]}}$$

and rename k to i below the reduced subproof.

If ρ' is a unary logical rule, then delete ρ', e.g. for ρ' being $\vee : r1$ define

$$\dfrac{\dfrac{\dfrac{(\chi)}{\Gamma \vdash \Delta}}{\Gamma \vdash \Delta, A_{[i]}}\ \mathrm{w:r}}{\Gamma \vdash \Delta, (A \vee B)_{[j]}}\ \vee : \mathrm{r1} \qquad \to^{\mathrm{w}} \qquad \dfrac{\dfrac{(\chi)}{\Gamma \vdash \Delta}}{\Gamma \vdash \Delta, (A \vee B)_{[j]}}\ \mathrm{w:r}$$

If ρ' is a binary rule, then delete ρ' and the subproof which does not contain ρ, e.g. for ρ' being $\wedge$: r and ρ being in the left subproof above ρ' define

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \vdash \Delta}}{\Gamma \vdash \Delta, C}\ \mathrm{w:r} \qquad \dfrac{(\chi_2)}{\Pi \vdash \Lambda, D}}{\Gamma, \Pi \vdash \Delta, \Lambda, (C \wedge D)_{[i]}}\ \wedge : \mathrm{r} \qquad \to^{\mathrm{w}} \qquad \dfrac{\dfrac{(\chi_1)}{\Gamma \vdash \Delta}}{\Gamma, \Pi \vdash \Delta, \Lambda, (C \wedge D)_{[i]}}\ \mathrm{w:*}$$

Analogous reductions apply for ρ being w : l and/or ρ' being of another rule type. Note that this reduction relation immediately carries over to skeletons because it depends only on the ancestor relation of the indices and not on the concrete formulas.

Definition 13. Given a skeleton S, the *weakening-residue* $\mathrm{w}(S)$ of S is defined by replacing each subgraph of the form

where $\tau(w)$ is weakening and u and the dotted edges are present iff w is not the root of S.

Definition 14. Let $S_1 = (V_1, E_1, \tau_1)$ and $S_2 = (V_2, E_2, \tau_2)$ be skeletons. S_1 is called *quasi-subskeleton* of S_2 if

1. $\mathrm{w}(S_1)$ is inner tree of $\mathrm{w}(S_2)$ and
2. For all $v \in V_1$ where $\tau_1(v)$ is not weakening:
   (a) $\tau_1(v)$ and $\tau_2(v)$ have the same rule type
   (b) For a main index i_1 in $\tau_1(v)$ and the corresponding main index i_1 in $\tau_2(v)$: $i_1 = i_2$
   (c) For an auxiliary index i_1 in $\tau_1(v)$ and the corresponding index i_2 in $\tau_2(v)$: $i_2 \leq_{S_2} i_1$.

Note that $\mathrm{w}(S)$ is an inner tree of S but in general not a skeleton. Being quasi-subskeleton is a transitive relation which can be proved analogously to Lemma 1.

Lemma 3. Let π be a proof of a sequent s and S be a subskeleton of $\mathrm{S}(\pi)$. Let U be a set of indices s.t. S is U-closed w.r.t. π. Then there is a skeleton S^* s.t.

1. S^* does not contain weakening,
2. $S^* \subseteq S$ and
3. S^* is U-closed w.r.t. π.

Proof. Observe that $\to^{\mathrm{w}}$ is strongly normalizing and that $\to^{\mathrm{w}}$-normal forms do not contain weakening. Letting S^* be a $\to^{\mathrm{w}}$-normal form of S, 1 is done. For 2 and 3 consider a single reduction step $T \to^{\mathrm{w}} T'$. Showing

2'. T' is a quasi-subskeleton of T and

3'. T is U-closed w.r.t. $\pi \implies T'$ is U-closed w.r.t. π

by a case distinction on the $\to^{\mathrm{w}}$-step is a matter of routine checking. Then 3 follows from 3' by induction. Claim 2 follows from 2' because by induction S^* is a quasi-subskeleton of S. So $\mathrm{w}(S^*)$ is inner tree of $\mathrm{w}(S)$ but $\mathrm{w}(S^*) = S^*$ because S^* does not contain weakening. Furthermore $\mathrm{w}(S)$ is inner tree of S and therefore S^* is inner tree of S. The subskeleton-conditions on the node-labellings τ of S and τ^* of S^* follow immediately from the quasi-subskeleton relation between S^* and S as there are no weakening nodes in S^*. □

Lemma 4. Let S be a skeleton and $F \in \mathcal{M}(S)$. Then 1. F contains only explicit nodes and 2. F does not contain weakening.

Proof. For 1 assume $F \in \mathcal{F}(S)$ and F contains an implicit rule. Let v be a lowermost such rule. If v is a cut, then $F \setminus \{v\}$ is a fragment, so F is not minimal. If v is not a cut, then it has a main index i and there is no node in F having i as auxiliary index because v was lowermost. Therefore – again – $F \setminus \{v\}$ is a fragment and F not minimal.

For 2 let $F \in \mathcal{F}(S)$ and assume that F contains weakening. Then by Lemma 3 there is a subskeleton F' of F which is $\mathcal{E}$-closed w.r.t. S and therefore a fragment of S. As F' does not contain weakening, it is a proper subskeleton of F and therefore F is not a minimal fragment of S. □

3.3 Characterization of the Projections

Lemma 5. Let π be a proof and $c \in \mathrm{P}(\pi)$. Then the skeleton of $\Psi(\pi, c)$ is a fragment of π, contains only explicit nodes and does not contain weakening.

Proof. By inspecting the definition of $\Psi(\pi, c)$ in the proof of Proposition 1, it is easy to check that $\mathrm{S}(\Psi(\pi, c))$ is a subskeleton of $\mathrm{S}(\pi)$ containing only explicit rules and no weakening. For $\mathcal{E}$-closedness, observe that $\mathrm{S}(\Psi(\pi, c))$ contains exactly the rules that operate on $\mathcal{E}_\pi(c)$. Furthermore, given two nodes $v \in \mathrm{S}(\pi)$ with main index i and $w \in \mathrm{S}(\pi)$ with auxiliary index j s.t. $j \leq_\pi i$, observe that $\mathcal{A}_\pi(v) \subseteq \mathcal{A}_\pi(w)$. Now for such v, w being explicit non-contraction nodes, v operating on $\mathcal{E}_\pi(c)$ implies that also w operates on $\mathcal{E}_\pi(c)$ and therefore that w is in $\mathrm{S}(\Psi(\pi, c))$. □

For a proof π, the set of axiom identifiers in π is denoted by $\mathcal{A}(\pi)$. For a set of proofs P, $\mathrm{S}(P)$ denotes the set $\{\mathrm{S}(\pi) \mid \pi \in P\}$.

Lemma 6. Let π be a proof and $c \in \mathrm{P}(\pi)$. Then $\mathcal{A}(\Psi(\pi, c)) = \mathcal{A}(c)$.

Proof. By induction on the construction of $\Psi(\pi, c)$. □

Lemma 7. Let π be a proof and F be a fragment of π s.t. 1. F contains only explicit nodes and 2. F does not contain weakening. Then F is the skeleton of a projection of π.

Proof. Let $F = (V_F, E_F, \tau_F)$ and $\mathrm{S}(\pi) = (V_\pi, E_\pi, \tau_\pi)$. We will show by induction on π that $\exists c \in \mathrm{P}(\pi)$ s.t. $F = \mathrm{S}(\Psi(\pi, c))$: If π is an axiom and $F \in \mathcal{F}(\pi)$ then $F = \mathrm{S}(\pi)$. By 1 the axiom contains an explicit index, so $\mathrm{P}(\pi) = \{c\}$ for some clause c and $\Psi(\pi, c) = \pi$. For the rest of this proof, assume that π ends with a non-axiom rule ρ and let $F \in \mathcal{F}(\pi)$ fulfilling 1 and 2 be given.

1. If ρ is in F: Let i be an auxiliary index in $\tau_\pi(\rho)$, let π' be the immediate subproof of π that contains i and let F' be the part of F in π'. By induction hypothesis $\exists c' \in \mathrm{P}(\pi')$ s.t. $F' = \mathrm{S}(\Psi(\pi', c'))$. We will first show that
$$\mathcal{A}_\pi(i) \cap \mathcal{A}(c') \neq \emptyset \qquad (*)$$
For the index j in $\tau_F(\rho)$ that corresponds to i we have $i \leq_\pi j$. As F' does not contain weakening, $\exists a \in \mathcal{A}_\pi(j) \cap \mathcal{A}(F')$. But $\mathcal{A}_\pi(j) \subseteq \mathcal{A}_\pi(i)$ and by induction hypothesis $\mathcal{A}(F') = \mathcal{A}(\mathrm{S}(\Psi(\pi', c')))$ and by Lemma 6 $\mathcal{A}(\mathrm{S}(\Psi(\pi', c'))) = \mathcal{A}(c')$ and therefore $a \in \mathcal{A}_\pi(i) \cap \mathcal{A}(c')$.

   (a) If ρ is a unary rule, then π', F' are π, F without ρ. By 2, ρ cannot be weakening. If ρ is a logical rule it has one auxiliary index i and by $(*)$ $\mathcal{A}_\pi(i) \cap \mathcal{A}(c') \neq \emptyset$. Letting $c := c'$, observe that $c \in \mathrm{P}(\pi)$ and ρ operates on $\mathcal{E}_\pi(c)$, so it is contained in $\Psi(\pi, c)$ and therefore $F = \mathrm{S}(\Psi(\pi, c))$. If ρ is a contraction with auxiliary indices i_1, i_2 then by $(*)$ $\mathcal{A}_\pi(i_1) \cap \mathcal{A}(c') \neq \emptyset$ and $\mathcal{A}_\pi(i_2) \cap \mathcal{A}(c') \neq \emptyset$ so ρ is contained in $\Psi(\pi, c)$ and again $F = \mathrm{S}(\Psi(\pi, c))$.

(b) If ρ is binary, let π_1, F_1 (and π_2, F_2) be the left (and right) part of π, F without ρ. Let $i_1(i_2)$ be the auxiliary index of ρ in $\pi_1(\pi_2)$ and let $c_1(c_2)$ be the clause obtained from applying the induction hypothesis to $\pi_1(\pi_2)$ respectively. Then by $(*)$ $\mathcal{A}_\pi(i_1) \cap \mathcal{A}(c_1) \neq \emptyset$ and $\mathcal{A}_\pi(i_2) \cap \mathcal{A}(c_2) \neq \emptyset$. As ρ is explicit, $\mathrm{P}(\pi) = \mathrm{P}(\pi_1) \times_{\mathcal{A}(\rho)} \mathrm{P}(\pi_2)$ and $c_1 \in \mathrm{P}(\pi_1)^{\mathcal{A}(\rho)}$ and $c_2 \in \mathrm{P}(\pi_2)^{\mathcal{A}(\rho)}$. Define $c := c_1 \circ c_2 \in \mathrm{P}(\pi)$ and observe that ρ operates on $\mathcal{E}_\pi(c)$ so it is contained in in $\Psi(\pi, c)$ and therefore $F = \mathrm{S}(\Psi(\pi, c))$.

2. If ρ is not in F, then F is contained in an immediate subproof of π, denote it with π'. Then $F \in \mathcal{F}(\pi')$ and by the induction hypothesis there is a $c \in \mathrm{P}(\pi')$ s.t. $\mathrm{S}(\Psi(\pi', c)) = F$. We will show that a) $c \in \mathrm{P}(\pi)$ and b) $\Psi(\pi, c) = \Psi(\pi', c)$.

   If ρ is implicit then a) $c \in \mathrm{P}(\pi)$ and $\Psi(\pi, c)$ – containing only explicit rules – does not contain ρ which establishes b). So assume ρ is explicit. Let i be an auxiliary index of $\tau_\pi(\rho)$ that occurs in π'. We will first show

$$\mathcal{A}_{\pi'}(i) \cap \mathcal{A}(c) = \emptyset \qquad (*)$$

   Assume $\exists a \in \mathcal{A}_{\pi'}(i) \cap \mathcal{A}(c)$. By Lemma 6 $\mathcal{A}(c) = \mathcal{A}(\mathrm{S}(\Psi(\pi', c)))$ and by the induction hypothesis $\mathcal{A}(\mathrm{S}(\Psi(\pi', c))) = \mathcal{A}(F)$ so $a \in \mathcal{A}_{\pi'}(i) \cap \mathcal{A}(F)$. This implies that F contains a non-contraction node σ with a main index $j \geq_{\pi'} i$ and $a \in \mathcal{A}_{\pi'}(j)$. But σ – being in F – by 1 is explicit and as F is $\mathcal{E}$-closed w.r.t. π, ρ would have to be in F which contradicts the assumption, so $\mathcal{A}_{\pi'}(i) \cap \mathcal{A}(c) = \emptyset$.

   (a) If ρ is unary, then a) $\mathrm{P}(\pi) = \mathrm{P}(\pi')$. If ρ is weakening then it does not operate on $\mathcal{E}_\pi(c)$ and by definition of the projections b) $\Psi(\pi, c) = \Psi(\pi', c)$. If ρ is a logical rule or a contraction, then by $(*)$ it does not operate on $\mathcal{E}_\pi(c)$ so b) $\Psi(\pi, c) = \Psi(\pi', c)$.

   (b) If ρ is binary then $\mathrm{P}(\pi) = \mathrm{P}(\pi') \times_{\mathcal{A}(\rho)} \mathrm{P}(\pi'')$ where π'' is the other immediate subproof of π. By $(*)$, $c \in \mathrm{P}(\pi')^{\neg\mathcal{A}(\rho)}$ and therefore a) $c \in \mathrm{P}(\pi)$. Also by $(*)$, ρ does not operate on $\mathcal{E}_\pi(c)$ and therefore b) $\Psi(\pi, c) = \Psi(\pi', c)$.

□

Theorem 2. For any proof π, the minimal fragments of π are exactly the projections of π, i.e. $\mathrm{S}(\Psi(\pi)) = \mathcal{M}(\pi)$.

Proof. $\mathrm{S}(\Psi(\pi))$ is by Lemmas 5 and 7 the set of fragments of π that contain only explicit nodes and no weakening. By Lemmas 2 and 4 this set is $\mathcal{M}(\pi)$. □

4 Projections and Cut-Elimination

In this section we will analyze the behavior of the projections under the following cut-elimination relation.

Definition 15. Let χ be a regular proof of the form:

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

We define proof rewrite rules for the reduction of this cut as follows:

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 $\mathrm{w} : \mathrm{r}$, then $\chi =$

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

and we define $\chi \mapsto^{\mathrm{w}} \chi' :=$

$$\dfrac{\begin{matrix}(\chi_1')\\ \Gamma \vdash \Delta\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{w} : *$$

If χ_2 ends with $\mathrm{w} : \mathrm{l}$ we proceed symmetrically.

Reduction of 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 $\mathrm{c} : \mathrm{r}$, then $\chi =$

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

and we define $\chi \mapsto^{\mathrm{c}} \chi' :=$

$$\dfrac{\dfrac{\dfrac{\begin{matrix}(\chi_1')\\ \Gamma \vdash \Delta, A, A\end{matrix} \quad \begin{matrix}(\chi_2)\\ A, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi \vdash \Delta, \Lambda, A}\ \text{cut} \quad \begin{matrix}(\chi_2\theta)\\ A, \Pi \vdash \Lambda\end{matrix}}{\Gamma, \Pi, \Pi \vdash \Delta, \Lambda, \Lambda}\ \text{cut}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ \mathrm{c} : *$$

where θ is a renaming of all eigenvariables and formula indices of χ_2 to fresh ones. If χ_2 ends with $\mathrm{c} : \mathrm{l}$, we proceed symmetrically.

Reduction of propositional rules: The cut formula is introduced by propositional rules on both sides immediately above the cut. If $A = B \wedge C$, then $\chi =$

$$\dfrac{\dfrac{\begin{matrix}(\chi_1')\\ \Gamma_1 \vdash \Delta_1, B\end{matrix} \quad \begin{matrix}(\chi_1'')\\ \Gamma_2 \vdash \Delta_2, C\end{matrix}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, B \wedge C}\ \wedge : \mathrm{r} \quad \dfrac{\begin{matrix}(\chi_2')\\ B, \Pi \vdash \Lambda\end{matrix}}{B \wedge C, \Pi \vdash \Lambda}\ \wedge : \mathrm{l1}}{\Gamma_1, \Gamma_2, \Pi \vdash \Delta_1, \Delta_2, \Lambda}\ \text{cut}$$

and we define $\chi \mapsto^{\mathrm{p}} \chi' :=$

$$\dfrac{\dfrac{\begin{matrix}(\chi_1')\\ \Gamma_1 \vdash \Delta_1, B\end{matrix} \quad \begin{matrix}(\chi_2')\\ B, \Pi \vdash \Lambda\end{matrix}}{\Gamma_1, \Pi \vdash \Delta_1, \Lambda}\ \text{cut}}{\Gamma_1, \Gamma_2, \Pi \vdash \Delta_1, \Delta_2, \Lambda}\ \mathrm{w} : *$$

If $A \wedge B$ is introduced by $\wedge$: l2 we proceed symmetrically. The other propositional connectives, $\vee$, $\rightarrow$ and $\neg$ are treated analogously.

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 $\chi =$

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

and we define $\chi \mapsto^{\mathrm{q}} \chi' :=$

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

The case of $A = (\exists x)B$ is treated analogously.

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

$$\dfrac{\overset{(\chi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{\overset{(\chi_2')}{A, \Pi' \vdash \Lambda'}}{A, \Pi \vdash \Lambda}\,\rho}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}$$

and we define $\chi \mapsto^{\mathrm{r}} \chi' :=$

$$\dfrac{\overset{(\chi_1)}{\Gamma \vdash \Delta, A} \quad \dfrac{\overset{(\chi_2')}{A, \Pi' \vdash \Lambda'}}{\Gamma, \Pi' \vdash \Delta, \Lambda'}\,\rho}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\mathrm{cut}$$

which is a proof. Note that regularity ensures that the eigenvariable condition cannot be violated.

If ρ is binary and the ancestor of the cut formula is in the left premise, then $\chi =$

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

and we define $\chi \mapsto^{\mathrm{r}} \chi' :=$

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

If the ancestor of the cut formula is on the right side we proceed symmetrically. The same rules apply for the case of χ_1 ending with a rule which does not introduce the cut formula.

The reduction relations $\rightarrow^{\mathrm{w}}$ (and $\rightarrow^{\mathrm{c}}, \rightarrow^{\mathrm{p}}, \rightarrow^{\mathrm{q}}, \rightarrow^{\mathrm{r}}$ respectively) are defined as compatible closure of the relations $\mapsto^{\mathrm{w}}$ (and $\mapsto^{\mathrm{c}}, \mapsto^{\mathrm{p}}, \mapsto^{\mathrm{q}}, \mapsto^{\mathrm{r}}$ respectively). The complete Gentzen-style cut-elimination relation $\rightarrow^{\mathrm{G}}$ is defined as reflexive and transitive closure of $\rightarrow^{\mathrm{w}} \cup \rightarrow^{\mathrm{c}} \cup \rightarrow^{\mathrm{p}} \cup \rightarrow^{\mathrm{q}} \cup \rightarrow^{\mathrm{r}}$. Note that the considered relation $\rightarrow^{\mathrm{G}}$ does not eliminate atomic cuts. However, sequent calculus proofs with only atomic cuts have the useful properties of cut-free proofs, in particular the subformula property, so for most applications the elimination of these cuts is irrelevant.

Definition 16. Let P, P' be finite sets of proofs. We define the relations

1. Duplication: $P \leq^{\mathrm{d}} P'$ iff $\exists \psi_1, \ldots, \psi_n \in P$ s.t. $P' = P \cup \{\psi_1\theta, \ldots, \psi_n\theta\}$ where θ is a renaming of eigenvariables and formula indices.
2. Instantiation: $P \leq^{\mathrm{i}} P'$ iff $P' = P\sigma$ where σ is a substitution.
3. Removal: $P \leq^{\mathrm{r}} P'$ iff $P' \subseteq P$

We define $\leq^{\mathrm{dir}}$ as transitive closure of $\leq^{\mathrm{d}} \cup \leq^{\mathrm{r}} \cup \leq^{\mathrm{i}}$ and similarly $\leq^{\mathrm{dr}}$ as that of $\leq^{\mathrm{d}} \cup \leq^{\mathrm{r}}$, etc. For proving the main result of this section we need the following preparatory lemma.

Lemma 8. Let $\pi[\chi]_p$ be a proof and let χ' be a proof with the same end-sequent as χ. Let $i_1, \ldots, i_n$ be the formula indices in the end-sequent of χ and χ'. Let σ be a substitution whose domain is contained in the set of eigenvariables of χ. Write π' for $\pi[\chi']_p$. If

1. $\Psi(\chi') = \Psi(\chi)\sigma$ and
2. $\mathcal{A}_{\pi'}(i_j) = \mathcal{A}_{\pi}(i_j)$ for all $j \in \{1, \ldots, n\}$

then $\Psi(\pi') = \Psi(\pi)\sigma$.

Proof. By induction on the number of rules between the end-sequent of χ and that of π. □

In Theorem 3 below we analyze the behavior of the projections of the Ceres-method under the standard cut-elimination $\rightarrow^{\mathrm{G}}$. The first analysis of this kind has been carried out in [6] for the characteristic clause set of the Ceres-method as introduced in [4]. The result of [6] appeared in a polished form in [17] by using the profile instead of the original characteristic clause set. In the following proof we rely on a variant of the analysis of the profile which appeared in [14, 15].

Theorem 3. If $\pi \rightarrow^{\mathrm{G}} \pi'$, then $\Psi(\pi) \leq^{\mathrm{dir}} \Psi(\pi')$.

Proof. We show the claim for a single cut-reduction step, the full result follows by induction. The induction base of $\pi = \pi'$ is trivial as $\leq^{\mathrm{dir}}$ is reflexive. Let p be the position of the reduced cut and χ be the subproof of π at p. Then $\pi' = \pi[\chi']_p$ with $\chi \rightarrow^{\mathrm{G}} \chi'$. We make a case distinction according to the type of cut-reduction. Throughout this proof we use the notation and proof names of Definition 15.

For *reduction of weakening* we have

$$\Psi(\chi) = \Psi(\chi'_1) \cup \Psi(\chi_2) \quad \text{and} \quad \Psi(\chi') = \Psi(\chi'_1).$$

We proceed by induction on the length of the path between χ and the end-sequent of π. Let $\xi_0 = \chi, \ldots, \xi_n = \pi$ be the subproofs of π along this path. Let $D := \mathcal{A}(\chi_2)$, let $\sigma_1, \ldots, \sigma_l$ be those explicit binary rules along this path that have an auxiliary index i with $\mathcal{A}_\pi(i) \subseteq D$. Let $j_1, \ldots, j_l$ be the other auxiliary indices of these rules, abbreviate $A_k := \mathcal{A}_\pi(j_k)$ and define the clause selection formula $D^* := \neg D \wedge \neg A_1 \wedge \ldots \wedge \neg A_l$. Let $\xi'_0 = \chi', \ldots, \xi'_n = \pi'$ be the subproofs of π' that correspond to $\xi_0, \ldots, \xi_n$.

Now let $k \in \{0, \ldots, n\}$. In [15, Lemma 5.4] it has been shown that

$$\mathrm{P}(\xi'_k) = \mathrm{P}(\xi_k)^{D^*}.$$

So in particular $\mathrm{P}(\pi') \subseteq \mathrm{P}(\pi)$ and to conclude $\Psi(\pi') \subseteq \Psi(\pi)$, it is enough to show that $\forall c \in \mathrm{P}(\pi') : \Psi(\pi', c) = \Psi(\pi, c)$. To that aim, observe that for all indices i we have $\mathcal{A}_{\pi'}(i) \cap D = \emptyset$. Therefore, for all $c \in \mathrm{P}(\pi')$: $i \in \mathcal{E}_\pi(c) \Leftrightarrow i \in \mathcal{E}_{\pi'}(c)$. This is enough for a case distinction on the construction of the projections (Proposition 1) to show that

$$\forall c \in \mathrm{P}(\xi'_k) : \ \Psi(\xi'_k, c) = \Psi(\xi_k, c) \quad \Rightarrow \quad \forall c \in \mathrm{P}(\xi'_{k+1}) : \ \Psi(\xi'_{k+1}, c) = \Psi(\xi_{k+1}, c).$$

for $k = 0, \ldots, n-1$. For $\xi'_0 = \chi'$ observe that $c \in \mathrm{P}(\chi')$ implies that $c \in \mathrm{P}(\chi'_1)$. Therefore $\Psi(\chi', c) = \Psi(\chi, c)$ and we can conclude $\Psi(\pi') \subseteq \Psi(\pi)$.

Reduction of contraction: Let $\xi_0 = \chi, \ldots, \xi_n = \pi$ be the subproofs of π between χ and the endsequent of π. Let $D := \mathcal{A}(\chi_2)$ and let θ be the variable- and index-renaming applied in the reduction. Let $\xi'_0 = \chi', \ldots, \xi'_n = \pi'$ be the subproofs of π' that correspond to $\xi_0, \ldots, \xi_n$. Let $k \in \{0, \ldots, n\}$ and let i be an index in the end-sequent of ξ_k. By induction it is easy to show that

$$\mathcal{A}_{\xi'_k}(i) = \mathcal{A}_{\xi_k}(i) \cup (\mathcal{A}_{\xi_k}(i) \cap D)\theta. \qquad (*)$$

In [15, Lemma 5.5] it has been shown that

$$\mathrm{P}(\xi'_k) = \mathrm{P}(\xi_k) \cup \mathrm{P}(\xi_k)^D\theta.$$

Let $c' \in \mathrm{P}(\xi'_k)$. We will show that

1. If $c' \in \mathrm{P}(\xi_k)$ then $\Psi(\xi'_k, c') = \Psi(\xi_k, c')$ and
2. If $c' \in \mathrm{P}(\xi_k)^D\theta$ then $\Psi(\xi'_k, c') = \Psi(\xi_k, c)\theta$ where $c \in \mathrm{P}(\xi_k)^D$ with $c\theta = c'$.

which implies $\Psi(\pi) \leq^{\mathrm{d}} \Psi(\pi')$.

1 If $c' \in \mathrm{P}(\xi_k)$ then $\mathcal{A}(c')$ does not contain an identifier of an axiom from $\mathcal{A}(\chi_2\theta) = D\theta$, so by $(*)$ we have $\mathcal{A}_{\xi'_k}(i) \cap \mathcal{A}(c') = \mathcal{A}_{\xi_k}(i) \cap \mathcal{A}(c')$ and therefore $i \in \mathcal{E}_{\xi_k}(c') \Leftrightarrow i \in \mathcal{E}_{\xi'_k}(c')$. Claim (a) then follows by induction on the construction of the projections.

2 If $c' \in \mathrm{P}(\xi_k)^D\theta$ then there is a $c \in \mathrm{P}(\xi_k)^D$ with $c\theta = c'$. By $(*)$

$$\mathcal{A}_{\xi'_k}(i) \cap \mathcal{A}(c') = (\mathcal{A}_{\xi_k}(i) \cap \mathcal{A}(c')) \cup ((\mathcal{A}_{\xi_k}(i) \cap D)\theta \cap \mathcal{A}(c'))$$

But $\mathcal{A}_\pi(i)$ contains no indices from the range of θ, so $\mathcal{A}_\pi(i) \cap \mathcal{A}(c') = \mathcal{A}_\pi(i) \cap (\mathcal{A}(c) \setminus D)$ and therefore we have

$$\mathcal{A}_{\xi_k}(i) \cap \mathcal{A}(c') = \mathcal{A}_{\xi_k}(i) \cap \mathcal{A}(c) \cap D^c$$

and as $\mathcal{A}(c') = \mathcal{A}(c)\theta$ also

$$((\mathcal{A}_{\xi_k}(i) \cap D)\theta \cap \mathcal{A}(c')) = (\mathcal{A}_{\xi_k}(i) \cap \mathcal{A}(c) \cap D)\theta$$

Therefore $\mathcal{A}_{\xi'_k}(i) \cap \mathcal{A}(c') \neq \emptyset \Leftrightarrow \mathcal{A}_{\xi_k}(i) \cap \mathcal{A}(c) \neq \emptyset$ and so $i \in \mathcal{E}_{\xi_k}(c) \Leftrightarrow i \in \mathcal{E}_{\xi'_k}(c')$ from which claim (b) can be shown by induction on the construction of the projections.

For the *reduction of $B \wedge C$ to B*,

$$\Psi(\chi) = \Psi(\chi'_1) \cup \Psi(\chi''_1) \cup \Psi(\chi'_2) \quad \text{and} \quad \Psi(\chi') = \Psi(\chi'_1) \cup \Psi(\chi'_2)$$

which is treated in the same way as the reduction of a weakening to show that also $\Psi(\pi') \subseteq \Psi(\pi)$. The other reductions of binary propositional connectives are treated analogously, for negation we obtain $\Psi(\pi') = \Psi(\pi)$.

For the *reduction of a universal quantifier*, we have

$$\Psi(\chi) = \Psi(\chi'_1) \cup \Psi(\chi'_2) \quad \text{and} \quad \Psi(\chi') = \Psi(\chi'_1\{\alpha \leftarrow t\}) \cup \Psi(\chi'_2)$$

But $\Psi(\chi'_1\{\alpha \leftarrow t\}) = \Psi(\chi'_1)\{\alpha \leftarrow t\}$ and by regularity $\Psi(\chi') = \Psi(\chi)\{\alpha \leftarrow t\}$. Let i be an index in the end-sequent of χ and χ', then $\mathcal{A}_{\pi'}(i) = \mathcal{A}_\pi(i)$ and therefore by Lemma 8 we obtain $\Psi(\pi') = \Psi(\pi)\{\alpha \leftarrow t\}$.

For the case of *rule permutation* it has been shown in [15, Lemma 5.1] that

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

We will show that $\forall c \in \mathrm{P}(\chi) : \ \Psi(\chi', c) = \Psi(\chi, c)$ which entails $\Psi(\pi') = \Psi(\pi)$ because we can apply Lemma 8 as $\mathcal{A}_{\pi'}(i) = \mathcal{A}_\pi(i)$ for all indices i in the end-sequent of χ and χ'.

1. Permutation of a unary rule: Then $\mathrm{P}(\chi) = \mathrm{P}(\chi_1) \cup \mathrm{P}(\chi_2)$ and $\Psi(\chi, c) = \Psi(\chi', c)$ can be shown for each c by first distinguishing wether $c \in \mathrm{P}(\chi_1)$ or $c \in \mathrm{P}(\chi_2)$ and – for the latter case – making a case distinction on the last construction step of the projection $\Psi(\chi_2, c)$.

2. Permutation of a binary rule: If ρ is implicit then

   $$\Psi(\chi) = \Psi(\chi_1) \cup \Psi(\chi'_2) \cup \Psi(\chi''_2) = \Psi(\chi').$$

   If ρ is explicit, then – letting $A := \mathcal{A}_\pi(\rho)$ –

   $$\mathrm{P}(\chi) = \mathrm{P}(\chi_1) \cup \mathrm{P}(\chi'_2)^{\neg A} \cup \mathrm{P}(\chi''_2)^{\neg A} \cup (\mathrm{P}(\chi'_2)^A \times \mathrm{P}(\chi''_2)^A)$$

   and $\Psi(\chi, c) = \Psi(\chi', c)$ can be shown for each $c \in \mathrm{P}(\chi)$ by a case distinction on which of the above subsets of $\mathrm{P}(\chi)$ contains c.

□

Definition 17. Let $S_1 = (V_1, E_1, \tau_1)$ and $S_2 = (V_2, E_2, \tau_2)$ be proof skeletons. S_1 and S_2 are *isomorphic*, written as $S_1 \cong S_2$, if there is a graph isomorphism $\varphi : V_1 \to V_2$ and a bijection f mapping the set of indices into itself s.t. for all $v \in V_1 : \tau_2(\varphi(v)) = f(\tau_1(v))$ where the application of f to a rule label is defined in the obvious way, for example $f(\to : \mathrm{l}_{(i,j;k)}) := \to : \mathrm{l}_{(f(i),f(j);f(k))}$.

Let $\mathfrak{S}$ denote the set of all skeletons and $\mathfrak{S}/\cong$ the set of the isomorphism classes of $\mathfrak{S}$. For a set of skeletons $\mathcal{S}$, write $\mathcal{S}^{\cong}$ for $\{\ \mathcal{C} \in \mathfrak{S}/\cong\ \mid\ \mathcal{C} \cap \mathcal{S} \neq \emptyset\}$.

Theorem 4. For proofs π and π': If $\pi \to^{\mathrm{G}} \pi'$ then $\mathcal{M}(\pi')^{\cong} \subseteq \mathcal{M}(\pi)^{\cong}$.

Proof. By Theorem 3, $\Psi(\pi) \leq^{\mathrm{dir}} \Psi(\pi')$, therefore $\mathrm{S}(\Psi(\pi)) \leq^{\mathrm{dr}} \mathrm{S}(\Psi(\pi'))$ and so $\mathrm{S}(\Psi(\pi'))^{\cong} \subseteq \mathrm{S}(\Psi(\pi))^{\cong}$ which by Theorem 2 implies $\mathcal{M}(\pi')^{\cong} \subseteq \mathcal{M}(\pi)^{\cong}$. □

So if we are given a proof π' that we want to shorten by introducing cuts, the only way to do so is to decrease the *number of elements* of the isomorphism classes of $\mathcal{M}(\pi')$, i.e. to merge several minimal fragments. As $\mathcal{M}(\pi') \subseteq \mathcal{M}(\pi)$ we cannot possibly hope to decrease the *number* of isomorphism classes. This is a general restriction for any method of cut-introduction based on $\to^{\mathrm{G}}$ and therefore having such isomorphism classes with more than one element is a necessary condition for a proof to allow abbreviation by the introduction of cuts. A quantification of the compressability of a proof is given in the next section.

As a side remark not connected to the main argument of this paper, note that for the weakening reduction $\to^{\mathrm{w}}$ of Definition 12 an analogous result holds: $\pi \to^{\mathrm{w}} \pi' \Rightarrow \mathcal{M}(\pi') \subseteq \mathcal{M}(\pi)$. This shows that the concept of minimal fragment is also of significance in situations not concerned with cut-elimination.

5 A Lower Bound on Cut-Introduction

It is well-known and has already been mentioned in the introduction that cut-elimination creates a non-elementary increase in proof size. It is simple to observe that not every sequence of large proofs has a sequence of small proofs as counterpart. This situation is similar to the one encountered in general data compression, for example based on binary strings. There, the concept of Kolmogorov complexity is a very useful tool for quantifying the amount of information contained in a binary string and therefore – its compressability. The Kolmogorov complexity of a binary string is the size of its shortest representation [19]. Analogously we can define a variant of Kolmogorov complexity, restricted to proofs and based on cut-elimination instead of (Turing-complete) computation as

$$\mathrm{C}(\pi^*) := \min\{\ |\pi|\ \mid\ \pi \to^{\mathrm{G}} \pi^*\}$$

From the point of view of complexity, the cut-introduction problem can then be stated as:

$$\text{Given a proof } \pi^*, \text{ find a proof } \pi \text{ s.t. } \pi \to^{\mathrm{G}} \pi^* \text{ and } |\pi| = \mathrm{C}(\pi^*).$$

In the rest of this section we prove and apply a lower bound on the complexity of a proof w.r.t. cut-introduction by relying on Theorems 2 and 4 shown above.

For a finite set P of proofs, define $\|P\| := \sum_{\pi \in P} |\pi|$. Two isomorphic skeletons have the same size, i.e. number of nodes. For a class $\mathcal{C} \in \mathfrak{S}/\cong$ we can therefore define $|\mathcal{C}| := |S|$ for an arbitrary $S \in \mathcal{C}$. For a finite set $\mathfrak{P} \subseteq \mathfrak{S}/\cong$ we define $\|\mathfrak{P}\| := \sum_{\mathcal{C} \in \mathfrak{P}} |\mathcal{C}|$.

Lemma 9. For any proof π: $\|\Psi(\pi)\| \leq |\pi| \cdot 2^{|\pi|}$

Proof. $|\mathrm{P}(\pi)| \leq 2^{|\pi|}$ can be shown by a simple induction on the definition of the profile. Furthermore, each $\psi \in \Psi(\pi)$ has at most size $|\pi|$. □

Theorem 5. For any proof π^*:

$$\mathrm{C}(\pi^*) \geq \frac{\log(\|\mathcal{M}(\pi^*)^{\cong}\|)}{2}$$

Proof. For any cut-elimination sequence $\pi \to^{\mathrm{G}} \pi^*$ we have

$$\|\mathcal{M}(\pi^*)^{\cong}\| \leq^{\text{Thm. 4}} \|\mathcal{M}(\pi)^{\cong}\| \;\leq\; \|\mathcal{M}(\pi)\|$$

and furthermore

$$\|\mathcal{M}(\pi)\| \leq^{\text{Thm. 2}} \|\Psi(\pi)\| \;\leq^{\text{Lem. 9}}\; |\pi| \cdot 2^{|\pi|} \;\leq\; 2^{2 \cdot |\pi|}$$

Choosing π s.t. $|\pi| = \mathrm{C}(\pi^*)$ we obtain

$$\log(\|\mathcal{M}(\pi^*)^{\cong}\|) \leq 2 \cdot \mathrm{C}(\pi^*).$$

□

The above relation between $\|\mathcal{M}(\pi^*)^{\cong}\|$ and $\mathrm{C}(\pi^*)$ is exponential and therefore slowly growing compared to the non-elementary worst-case complexity of cut-elimination which motivates the following

Corollary. Let $(\pi_n^*)_{n \geq 1}$ be a sequence of proofs. If there exists a sequence $(\pi_n)_{n \geq 1}$ s.t. $\pi_n \to^{\mathrm{G}} \pi_n^*$ for all $n \geq 1$ and $|\pi_n|$ grows elementarily in n, then $\|\mathcal{M}(\pi_n^*)^{\cong}\|$ grows elementarily in n.

The above corollary is a strong restriction on the structure of the $\to^{\mathrm{G}}$-normal forms of the sequences of [23, 21, 22] and any other sequences with that asymptotic behavior: The large sizes of the normal forms are only due to a non-elementary number of repetitions of the same structural elements, the isomorphism classes of the minimal fragments. Using the corollary in a contrapositive way we obtain a method to demonstrate that a sequence of long proofs does not allow strong compression.

6 Conclusion

The elimination and introduction of cuts allow to navigate in the space of proofs of a theorem in ways which are not fully understood yet. This paper is a contribution to the understanding of the structural effects of these transformations. We have shown that cut-elimination based on local rewrite steps perturbs the

structure of a proof only up to a surprisingly low degree: The minimal fragments of a proof are not changed themselves, they are merely instantiated and rearranged. This strong connection between a proof with cuts and its counterpart without cuts allows to describe a certain kind of redundancy, having large isomorphism classes of minimal fragments, whose presence is necessary for a cut-free proof to allow compression. We have stated this result in the form of a lower bound on the cut-introduction problem.

However, many questions still remain open. For finding conditions which are not only necessary but also sufficient for a cut-free proof to allow compression, the methods employed in this paper have to be extended considerably: As we are dealing with first-order logic, the term-level of a proof is of crucial importance for the introduction of cuts. Taking this level into account needs an investigation of the redundancy of Herbrand-disjunctions and its pre-forms (as in [16]) during cut-elimination.

Acknowledgments
The author would like to thank M. Baaz, A. Leitsch, D. Weller and B. Woltzenlogel Paleo for useful comments on an earlier version of this article.

References

[1] Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter, and Hendrik Spohr. Proof Transformation by CERES. In Jonathan M. Borwein and William M. Farmer, editors, *Mathematical Knowledge Management (MKM) 2006*, volume 4108 of *Lecture Notes in Artificial Intelligence*, pages 82–93. Springer, 2006.

[2] Matthias Baaz, Stefan Hetzl, Alexander Leitsch, Clemens Richter, and Hendrik Spohr. CERES: An Analysis of Fürstenberg's Proof of the Infinity of Primes. *Theoretical Computer Science*, 403(2–3):160–175, 2008.

[3] Matthias Baaz and Alexander Leitsch. On Skolemization and Proof Complexity. *Fundamenta Informaticae*, 20(4):353–379, 1994.

[4] Matthias Baaz and Alexander Leitsch. Cut-elimination and Redundancy-elimination by Resolution. *Journal of Symbolic Computation*, 29(2):149–176, 2000.

[5] Matthias Baaz and Alexander Leitsch. Ceres in many-valued logics. In Franz Baader and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning, LPAR 2004*, volume 3452 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2005.

[6] Matthias Baaz and Alexander Leitsch. Towards a clausal analysis of cut-elimination. *Journal of Symbolic Computation*, 41(3–4):381–410, 2006.

[7] Matthias Baaz and Piotr Wojtylak. Generalizing proofs in monadic languages. *Annals of Pure and Applied Logic*, 154(2):71–138, 2008.

[8] Matthias Baaz and Richard Zach. Algorithmic Structuring of Cut-free Proofs. In *Computer Science Logic (CSL) 1992*, volume 702 of *Lecture Notes in Computer Science*, pages 29–42. Springer, 1993.

[9] Uwe Egly and Karin Genther. Structuring of Computer-Generated Proofs by Cut Introduction. In Georg Gottlob, Alexander Leitsch, and Daniele Mundici, editors, *Kurt Gödel Colloquium*, volume 1289 of *Lecture Notes in Computer Science*, pages 140–152. Springer, 1997.

[10] William M. Farmer. A unification-theoretic method for investigating the k-provability problem. *Annals of Pure and Applied Logic*, 51:173–214, 1991.

[11] H. Fürstenberg. On the infinitude of primes. *American Mathematical Monthly*, 62:353, 1955.

[12] Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210,405–431, 1934–1935.

[13] Jean-Yves Girard. *Proof Theory and Logical Complexity*. Elsevier, 1987.

[14] Stefan Hetzl. *Characteristic Clause Sets and Proof Transformations*. PhD thesis, Vienna University of Technology, 2007.

[15] Stefan Hetzl. *Proof Profiles. Characteristic Clause Sets and Proof Transformations*. VDM, Saarbrücken, 2008.

[16] Stefan Hetzl. Describing proofs by short tautologies. *Annals of Pure and Applied Logic*, 159(1–2):129–145, 2009.

[17] Stefan Hetzl and Alexander Leitsch. Proof Transformations and Structural Invariance. In Stefano Aguzzoli, Agata Ciabattoni, Brunella Gerla, Corrado Manara, and Vincenzo Marra, editors, *Algebraic and Proof-theoretic Aspects of Non-classical Logics*, volume 4460 of *Lecture Notes in Artificial Intelligence*, pages 201–230. Springer, 2007.

[18] Jan Krajíček and Pavel Pudlák. The Number of Proof Lines and the Size of Proofs in First Order Logic. *Archive for Mathematical Logic*, 27:69–84, 1988.

[19] Ming Li and Paul Vitanyi. *An Introduction to Kolmogorov Complexity and Its Applications*. Springer, 2nd edition, 1997.

[20] Dale Miller and Vivek Nigam. Incorporating tables into proofs. In *16th Conference on Computer Science and Logic (CSL07)*, volume 4646 of *Lecture Notes in Computer Science*, pages 466–480. Springer, 2007.

[21] V.P. Orevkov. Lower bounds for increasing complexity of derivations after cut elimination. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta*, 88:137–161, 1979.

[22] Pavel Pudlák. The Lengths of Proofs. In Sam Buss, editor, *Handbook of Proof Theory*, pages 547–637. Elsevier, 1998.

[23] Richard Statman. Lower bounds on Herbrand's theorem. *Proceedings of the American Mathematical Society*, 75:104–107, 1979.

[24] Gaisi Takeuti. *Proof Theory*. North-Holland, Amsterdam, 2nd edition, March 1987.