On categorical equivalence of Gentzen-style derivations in IMLL

Sergei Soloviev\textsuperscript{a,*}, Vladimir Orevkov\textsuperscript{b,1}

\textsuperscript{a}IRIT, Université Paul Sabatier, 118, route de Narbonne, 31062 Toulouse Cedex, France
\textsuperscript{b}POMI, Russian Academy of Sciences, Fontanka, 27, St. Petersbourg, Russia

Dedicated to A.O. Slissenko on his 60th birthday

Abstract

A new deciding algorithm for categorical equivalence of derivations in Intuitionistic Multiplicative Linear Logic (IMLL) is proposed. The algorithm is based uniquely on manipulations with Gentzen-style derivations. The algorithm has low polynomial complexity. The paper also contains results concerning permutability of rules and its connection with categorical equivalence.

\textcopyright 2002 Elsevier Science B.V. All rights reserved.

Keywords: Closed categories; Intuitionistic linear logic

1. Introduction

Our aim is to describe a deciding algorithm for categorical equivalence of derivations in Intuitionistic Multiplicative Linear Logic (IMLL) based uniquely on manipulations with Gentzen-style derivations. The algorithm has low polynomial complexity.

The interest to IMLL in connection with category theory is due to the fact that one may introduce on this system a structure of the free Symmetric Monoidal Closed (SMC) category. The diagrams are represented by the pairs of derivations of the same sequent. The categorical equivalence is generated by the axioms of SMC categories and a deciding algorithm provides a method to check the commutativity of diagrams in free SMC category (for details see, e.g. [14]).

\textsuperscript{*}Corresponding author.
\textsuperscript{1}The work was partly done during the visit of V. Orevkov as invited professor to IRIT (Université P. Sabatier) in March–April 2000.

0304-3975/03/$-see front matter \textcopyright 2002 Elsevier Science B.V. All rights reserved.

PII: S0304-3975(02)00454-1
Several types of deciding algorithms were suggested earlier. For example, the algorithms using natural deduction style systems and normalization [10] (this approach was further developed in [1,2], cf. also [11]); proof-nets [3,16]; a special formal system was studied by Jay [5].

We describe an algorithm that uses cut-elimination, decreasing of the depth of formulas, and substitutions of the constant \( I \) (“tensor unit”). It is the first deciding procedure for the categorical equivalence that works exclusively with Gentzen-style derivations and does not use any “extras” like proof-nets or terms (and thus, revives in a way the old approach by Lambek [9]).

It is generally understood that the complexity of a reasonable algorithm should be of order of a low polynomial. As far as we know, there is no paper considering accurately the complexity bounds of these algorithms. We have similar low-polynomial bound for our algorithm. (The complexity problem is not trivial: while the depth of a cut-free derivation in IMLL has linear bound w.r.t. the size of its final sequent, the number of non-equivalent derivations may still be exponential. The examples may be found in [15].)

The part concerning the algorithm was essentially done by S. Soloviev. Complexity estimations were based on joint research. A theorem proved by V. Orevkov that describes the connection between the categorical equivalence of derivations and the Kleene-style permutations of rules completes the study.

2. Sequent calculus and categorical equivalence

2.1. System \( L \)

The calculus \( L \) (cf. [4]) has two axioms:

\( A \vdash A \) (identity), \( \vdash I \) (unit),

and the following rules:

**Structural rules**

\[
\frac{\Gamma \vdash A \ A, \Delta \vdash B}{\Gamma, \Delta \vdash B} \text{(cut)} \quad \frac{\Delta \vdash I \Sigma \vdash A}{\Delta, \Sigma \vdash A} \text{ (wkn)} \quad \frac{\Gamma \vdash A}{\Gamma' \vdash A} \text{ (perm)}
\]

**Logical rules**

\[
\frac{\Gamma \vdash A A \vdash B}{\Gamma, \Delta \vdash A \otimes B} \text{ (\( \otimes \))} \quad \frac{A, \Delta, \Gamma \vdash C}{A \otimes B, \Gamma \vdash C} \text{ (\( \otimes \vdash \))},
\]

\[
\frac{A, \Gamma \vdash B}{\Gamma \vdash A \rightarrow B} \text{ (\( \rightarrow \))} \quad \frac{\Gamma \vdash A \ B, \Delta \vdash C}{\Gamma, A \rightarrow B, \Delta \vdash C} \text{ (\( \rightarrow \vdash \))}.
\]

We shall call all the rules of \( L \) except permutation \( \text{perm} \) its main rules.
2.2. Categorical equivalence and its properties

The categorical equivalence \(\equiv\) on derivations of \(L\) is introduced via translation of the \(L\)-derivations of a sequent \(A_1,\ldots,A_n \vdash A\) into the arrows \(A_1 \otimes (\cdots \otimes A_n) \to A\) (arrows \(I \to A\) if the list is empty) of the free SMC category \(F\) generated by the set of propositional variables.

The arrows of this category may be considered as derivations in another “Hilbert-style” calculus with the rules representing the action of functors \(\otimes\) (tensor product), \(\to\) (internal hom-functor) and composition, and the axiom-schemes representing basic natural transformations of SMC categories (for example, \(c_{AB} : A \otimes B \to B \otimes A\)).

The equivalence relation on arrows is the smallest equivalence relation generated by the axioms of category, functoriality of \(\otimes\) and \(\to\), naturality of basic transformations, and the axioms specific to SMC categories (such as \(c_{AB}c_{BA} \equiv 1\), the Mac Lane “pentagon” and “hexagon” etc.).

Two derivations in \(L\) are equivalent iff their images are equivalent in \(F\).\(^2\)

Before we describe certain properties of \(\equiv\) that will be used to develop the deciding algorithm, let us consider some examples.

**Example 1.** The following derivations are non-equivalent

\[
\begin{align*}
\frac{a \vdash a}{a, a \vdash a} & \quad \frac{a \vdash a}{a, a \vdash a} \\
\frac{a \vdash a \otimes a}{a, a \vdash a \otimes a} & \quad (\text{perm}).
\end{align*}
\]

**Example 2.** The derivation \(d\) of the sequent

\[
a \otimes b \to I, (a \to I) \to (1), (b \to I) \to (2), I \vdash I,
\]

where \(\to (1)\) is introduced the last is not equivalent to the derivation \(d'\) where \(\to (2)\) is introduced the last.

**Example 3.** Let \(a^{(n)}\) denote the formula \(((a \to I) \to \cdots) \to I\) (\(n\) times \(I\)). The sequent \(a^{(3)} \vdash a^{(3)}\) has two non-equivalent derivations. As it was noticed by Szabo [15], the number of non-equivalent derivations of \(a^{(n)} \vdash a^{(n)}\) \((n \to \infty)\) grows exponentially.

These inequalities can be verified in various SMC categories \(K\) (via the translation of \(L\)-derivations into \(F\) and subsequent interpretation of \(F\) in \(K\)), such as the category of vector spaces or the category of finite pointed sets.

The rules \(\text{perm}\) and \(\text{wkn}\). These rules correspond to composition with so called “central isomorphisms” (representing natural commutativity and associativity of \(\otimes\) and properties of tensor unit \(I\)). Coherence of central isomorphisms [7] implies that a series

\[^2\text{First detailed description of a system similar to } F\text{ was given in classical Kelly-Mac Lane paper [7]. All necessary details concerning } F, L\text{ and their connection may be found in [14]. Due to this definition of } \equiv, \text{ the technicalities in the formulations of rules of } L\text{ (such as two-premise } \text{wkn}\text{) are not really important. One may note also that the rule } \otimes\text{-left has nothing to do with } \text{mix (it corresponds to composition with central isomorphism in } F).}\]
of several applications of \textit{perm} can be replaced by one application. All “degenerate” applications of \textit{wkn} (with $\vdash I$ as a premise) can be omitted. This does not change the equivalence class of a derivation.

Below we suppose that there is no “degenerate” applications of \textit{wkn} and no \textit{perm} is applied immediately after another. (Usually we shall omit applications of \textit{perm} when the derivations are displayed.)

\textit{Cut elimination:} $L$-derivations have cut-elimination property w.r.t. $\equiv$.

If the derivation $d'$ is obtained by standard reductions of \textit{cut} from $d$ then $d' \equiv d$. In $L$ \textit{cut} can be eliminated and hence every derivation $d$ is equivalent to a cut-free one. (See [6, 7].)

One may check, that cut-elimination in $L$ does not augment the number of the rules in a derivation. (More precise complexity bounds are given in the end of this paper.)

The number of cut-free derivations of a given sequent (without repeated \textit{perm} and degenerate \textit{wkn}) is finite.

\textit{Permutation of rules:} There are Kleene-style permutations of inferences that preserve categorical equivalence.

Let two inferences $R_1, R_2$ of main rules of $L$ belong to the same branch ($R_2$ being below $R_1$). They are called adjacent if there is no inferences of main rules between them (only \textit{perm} is possible).

We shall consider some sufficient conditions when the permutation is possible. First, there is the following natural restriction:

\textit{the main formula of $R_1$ is not one of the side formulas of $R_2$.}

(The cut-formula is considered as the side formula of the rule \textit{cut}.)

If the natural restrictions are satisfied the following permutations are possible without any further restrictions.

\[
\begin{align*}
\vdash \neg \rightarrow, \textit{cut, wkn}, \neg \rightarrow ;
\vdash \neg \rightarrow, \textit{cut, wkn}, \neg \rightarrow \otimes ;
\vdash \neg \rightarrow, \textit{cut, wkn}, \neg \rightarrow \otimes \rightarrow ;
\vdash \neg \rightarrow, \textit{cut, wkn}, \otimes \rightarrow ;
\vdash \neg \rightarrow, \textit{cut, wkn}, \otimes \rightarrow \rightarrow .
\end{align*}
\]

The following permutations require further restrictions:

\[
\begin{align*}
\otimes \rightarrow, \textit{cut, wkn}, \neg \rightarrow ;
\otimes \rightarrow, \textit{cut, wkn} \neg \rightarrow .
\end{align*}
\]

The restrictions are that the side formulas of the inference below must not belong to different premises of the inference above.

Natural restrictions are not satisfied in cases $\vdash \neg \rightarrow, \neg \rightarrow \otimes / \neg \rightarrow, \neg \otimes$ and when the inferences of $\neg \rightarrow$ and $\neg \otimes$ are situated above left premises of $\neg \rightarrow, \textit{cut}$.

The derivation after permutation of inferences is equivalent to the derivation before. This fact may be checked (for each permutation) by translation into $F$ and direct calculation.

If the endsequent of a derivation $d$ has the succedent of the form $A \neg \rightarrow B$ then the corresponding inference of $\vdash \neg \rightarrow$ can be “pushed down” and $d \equiv d'$ where $d'$ has $\vdash \neg \rightarrow$ as its last rule. Similarly, if the antecedent of the endsequent of $d$ contains the member of the form $A \otimes B$ then the corresponding $\otimes \rightarrow$ can be “pushed down” and $d \equiv d'$ ending by the $\otimes \rightarrow$ with $A \otimes B$ as its main formula.
Let $d$ contain an inference of the form
\[
\frac{\Gamma, A \rightarrow B, \Sigma \vdash C}{A \rightarrow B, \Sigma \vdash C}\tag{-0-}
\]
and its final sequent be $\Gamma, A \rightarrow B, \Sigma \vdash D$. I.e., the antecedent of the left premise of the $\rightarrow \vdash$ and its main formula occur unchanged into the endsequent. Then this $\rightarrow \vdash$ can be “pushed down” and $d \equiv d'$ where $d'$ ends by $\rightarrow \vdash$ with the left premise $\Gamma \vdash A$ and the right premise $B, \Sigma \vdash D$.

Slightly more complex transformations (also based on permutations of inferences) are considered in the following paragraph.

Sequents and derivations that “split”: Suppose that some sequent $S$ has the form $\Gamma_1, \Gamma_2 \vdash A \otimes B$ where $\Gamma_1 \vdash A$ and $\Gamma_2 \vdash B$ have no common variables or the form $\Gamma_1 \vdash A$ where $\Gamma_1$ has no common variables with the rest of the sequent (up to permutation of the antecedent members).

We shall say that this sequent splits.

If the sequent $S$ does split then every derivation $d$ of $S$ is equivalent to a derivation which ends by $\vdash \otimes$ or (in the second case) by $wkn$ with $\Gamma_1 \vdash I$ as one of the premises (see [12], Lemma 19, [14], Lemma 5.22). (It can be transformed into derivation ending by the corresponding rule by permutations of inferences described above.)

Since the inverse is obviously true too, a derivation $d$ is equivalent to a derivation ending by $wkn$ or $\vdash \otimes$ iff its final sequent splits.

Let $R$ be a rule of $L$. Let us call the derivation $d$ an $R$-derivation if $d$ is equivalent to some derivation ending by $R$.

According to the above, whether $d$ is equivalent to a derivation ending by $wkn$, $\otimes \vdash$, $\vdash \otimes$, $\vdash \rightarrow$ depends only on the structure of its final sequent. If it is not the case it is either an axiom or $\rightarrow \vdash$-derivation.

Atomic derivations: We call a derivation in $L$ atomic if it contains only the axioms of the forms $a \vdash a$, $I \vdash I$ ($a$ is a variable). In arbitrary derivation $d$ every axiom $A \vdash A$ may be replaced by its atomic derivation. (Both derivations represent the categorical identity map.) The result is an atomic derivation which is equivalent to $d$.

Balancedness: A sequent is called balanced if every variable occurs in it twice and with opposite signs (variances).

Cut-free derivation of a balanced sequent in $L$ contains only balanced sequents.

For every derivation $d$ of a sequent $S$ there exists a balanced sequent $S_0$ and a derivation $d_0$ of $S_0$ such that $S$ and $d$ are obtained from $d_0$ and $S_0$ by identification of variables.

If $d$ is already cut-free and atomic the axioms of the form $a \vdash a$ are in one-to-one correspondence with the (disjoint) pairs of occurrences of $a$ in the final sequent (“atomic links”). The variables of different pairs should be given different names (and their ancestors should be renamed in the same way throughout the derivation). The sequent $S_0$ is uniquely determined by $d$ up to the choice of new variables.

Let two derivations $d, d'$ of the same sequent $S$ be given. It is known that if the corresponding atomic links are not the same then $d$ is not equivalent to $d'$ [7]. Thus, non-balanced case is not really a problem.
If they are the same, then without loss of generality it may be assumed that $d$ and $d'$ are obtained by identification of variables from the derivations $d_0, d'_0$ of the same balanced sequent $S_0$. In this case $d \equiv d' \iff d_0 \equiv d'_0$.

As Example 2 shows the derivations of a balanced sequent are not necessarily equivalent.

The main part of our algorithm works with the derivations of the same balanced sequent.

**Reduction to 2-sequents**

**Definition 4.** The sequent $\Gamma \vdash A$ will be called a 2-sequent if $A$ contains no more than one connective, and each member of $\Gamma$ no more than two connectives.

As follows from this definition, $A$ has one of the forms $a, a \otimes b, a \circ b$ and the members of the list $\Gamma$ have one of the forms $a, a \otimes b, a \otimes (a \otimes c), (a \otimes b) \otimes c, a \circ b, a \circ (b \otimes c), (a \otimes (b \otimes c)) \circ c, (a \circ (b \circ c)) \circ c$, where $a, b, c$ denote atoms and possibly the constant $I$. Some further reductions are possible, as the study in [12] shows (for example, one of $(a \otimes b) \circ c, a \circ (b \circ c)$ can be eliminated, since they are isomorphic).

This motivates the following

**Definition 5.** The sequent $\Gamma \vdash A$ will be called pure 2-sequent if $A$ has one of the following forms ($a, b, c$ denote atoms):

$I; a; a \otimes b; a \circ (I; a)$

and the members of $\Gamma$ have one of the forms

$(b \circ I) \circ I, (b \circ a) \circ I, (b \circ I) \circ c, (b \circ a) \circ c$.

**Proposition 6** (Soloviev [12], Soloviev [14]). Let $S = \Gamma \vdash B$ be any balanced sequent. There exist a balanced pure 2-sequent $S_0 = \Gamma_0 \vdash B$, such that for every derivations $\psi, \psi'$ of $S$ there exist some derivations $\psi_0, \psi'_0$ of $S_0$ and $\psi \equiv \psi' \iff \psi_0 \equiv \psi'_0$.

The easiest way to prove it is based on some standard cuts and cut-elimination (it was used in [12,14]). V.P. Orevkov proposed an algorithm that construct $\psi_0, \psi'_0$ which works with proof-schemes of cut-free derivations and has better complexity bounds.

**Substitutions and their action:** Important role in our algorithm will be played by substitutions of $I$. We may assume that the sequent is already a pure 2-sequent. If we apply a substitution $\alpha$ to a derivation $d$ of a pure 2-sequent $S$ the resulting sequent is not necessarily pure (it is still 2-sequent). Some members may become constant, some other may now contain subformulas of the form $I \circ A, I \otimes A, A \otimes I$. To make it pure again the cuts with certain derivations representing isomorphisms may be done (and then eliminated). There exists another algorithm that does not use cuts (V.P. Orevkov). The derivation obtained from $d$ by substitution $\alpha$ and “purification” algorithm is denoted by $\alpha * d$. We have $d \equiv d' \Rightarrow \alpha d \equiv \alpha d'$ and $\alpha d \equiv \alpha d' \iff \alpha * d \equiv \alpha * d'$. 
2.3. Critical pairs and equivalence

Since the work by Voreadou [17] it is understood that there is close connection between non-equivalent derivations and so called “twisted” applications of \( \vdash \) (i.e., the pairs of derivations ending by \( \vdash \) where the main formula of one application belongs to the left premise of another, cf. Example 2). The use of substitutions permits to connect the non-equivalence of derivations with a very special case of twisted \( \vdash \).

**Definition 7** (Soloviev [14, Definition 7.1]). The pair of derivations \( \xi_1, \xi_2 \) of the same balanced pure 2-sequent \( S = A, A_1 \vdash I, A_2 \vdash I \) is called critical if

\[
\begin{align*}
(1) & \quad \xi_1 = \frac{A, A_1 \vdash I, A_2 \vdash I}{A, A_1 \vdash I, A_2 \vdash I} \quad \xi_2 = \frac{A, A_2 \vdash I, A_1 \vdash I}{A, A_1 \vdash I, A_2 \vdash I}, \\
(2) & \quad \text{cut-free derivation of } S \text{ can end only by (some) application of } \vdash, \text{ but} \\
(3) & \quad \text{the derivations } \xi_1, \xi_2 \text{ are not equivalent to derivations ending by } \vdash.
\end{align*}
\]

The pair is minimal critical (MC) if \( A \) does not contain the members of the form \( a, a \otimes b \).

The formulas \( A_1 \vdash I, A_2 \vdash I \) in this definition will be called the key-formulas of the MC pair.

Let us consider two derivations \( d_1, d_2 \) of the same 2-sequent \( \Gamma \vdash C \) in \( L \).

**Proposition 8** (Soloviev [14, Corollary 14.6]). \( d_1 \equiv d_2 \) iff there is no substitution \( \alpha \) of \( I \) for variables such that \( \alpha \ast d_1, \alpha \ast d_2 \) form a minimal critical pair.

3. Construction of an algorithm

3.1. Searching for MC pairs

Using Proposition 8 in a straightforward way one has to consider all possible substitutions. To obtain a reasonable algorithm, it should be taken into account that only some substitutions can produce an MC pair. Also, the recursive check of the equivalence required by (3) of the definition of MC pairs may be simplified.

The analysis of the conditions of Definition 7 will help to find necessary simplifications.

The pair \( d_1, d_2 \) satisfying only the condition (1) of Definition 7 will be called an MC-candidate, the pair that satisfies (1) and (2) a strong MC-candidate. We shall

---

3 The paper [14] as well as our present paper is closely connected with [17] on the level of ideas. At the same time our work is technically independent. The approach based on substitutions is itself due to the necessity to correct certain technical error in [17] (see [14]).
suppose (if not stated otherwise) that all derivations are cut-free and atomic and all sequents are balanced.

**Notation.** In a cut-free L-derivation to each occurrence of a formula $A \otimes B, A \rightarrow B$ corresponds unique inference of the rule introducing its principal connective. The expression $\vdash A \rightarrow B, \vdash A \otimes B$ etc. will denote this inference when there is no ambiguity concerning the occurrence of the formula.

**Condition (1).** Every derivation $d$ of $\Gamma \vdash C$ defines a partial order $<_d$ on the set of implicative formulas of the antecedent $\Gamma$. $A \rightarrow B <_d A' \rightarrow B'$ if $A' \rightarrow B'$ belongs to the antecedent of the left premise of the rule $\vdash A \rightarrow B$.

Substitution defines a (partial) order-preserving map in the following sense:

**Lemma 9.** Let $d$ be a derivation of $\Gamma \vdash C$, $A_1 \rightarrow B_1, A_2 \rightarrow B_2$ be formulas in $\Gamma$, $\sigma$ be a list of variables and $\sigma = \{1/\sigma_1\}$ be a substitution. Consider the derivation $\sigma \ast d$ and the sequent $\sigma \ast (\Gamma \vdash C)$. If the images of $A_1 \rightarrow B_1$ in $\sigma \ast (\Gamma \vdash C)$ are implicative formulas $A'_1 \rightarrow B'_1, A'_2 \rightarrow B'_2$ then $A_1 \rightarrow B_1 <_d A_2 \rightarrow B_2$ iff $A'_1 \rightarrow B'_1 <_{\sigma \ast d} A'_2 \rightarrow B'_2$.

**Proof.** In the derivation $\sigma \ast d$ some of the rules may disappear but the order of remaining rules is the same as in $d$.

When we have two derivations $d_1, d_2$, each defines the partial order $<_{d_i}$.

**Lemma 10.** Suppose there is a substitution $\sigma$ such that the pair

$$\sigma \ast d_1 = \frac{A_1, A'_1 \rightarrow I \vdash A'_2 I \vdash I}{A_1, A'_1 \rightarrow I, A'_2 \rightarrow I \vdash I}, \quad \sigma \ast d_2 = \frac{A_1, A'_1 \rightarrow I \vdash A'_2 I \vdash I}{A_1, A'_1 \rightarrow I, A'_2 \rightarrow I \vdash I}$$

is an MC-candidate. Let the formulas $A_1 \rightarrow B_1, A_2 \rightarrow B_2$ be the ancestors of $A'_1 \rightarrow I$, $A'_2 \rightarrow I$, then $A_1 \rightarrow B_1 <_{d_1} A_2 \rightarrow B_2$ and $A_2 \rightarrow B_2 <_{d_2} A_1 \rightarrow B_1$.

**Proof.** By Lemma 9, if two formulas are in relation $<_{\sigma \ast d_i}$ their ancestors in $\Gamma \vdash C$ are in relation $<_{d_i}$.

**Definition 11.** Given the pair $(d_1, d_2)$, we shall call a pair of formulas $A_1 \rightarrow B_1, A_2 \rightarrow B_2$ such that $A_1 \rightarrow B_1 <_{d_1} A_2 \rightarrow B_2, A_2 \rightarrow B_2 <_{d_2} A_1 \rightarrow B_1$ KF-candidate.

The KF-candidates are the potential ancestors w.r.t. substitutions of the main formulas of the MC-pairs. Obviously, only the substitutions that give the form required in Definition 7 to one of the pair of the KF-candidates should be considered.

Suppose $(\sigma \ast d_1, \sigma \ast d_2)$ is an MC-pair. Let $A_1 \rightarrow B_1, A_2 \rightarrow B_2$ be the ancestors of corresponding key formulas. Suppose that $\vdash A_1 \rightarrow B_1 \vdash <_{d_1} \vdash A_2 \rightarrow B_2 \vdash$ and $\vdash A_2 \rightarrow B_2 \vdash <_{d_2} \vdash A_1 \rightarrow B_1 \vdash$. Consider the parts of $d_1, d_2$ ending by $\vdash A_1 \rightarrow B_1$ (by $\vdash A_2 \rightarrow B_2$).

$$\Gamma_1, A_2 \rightarrow B_2 \vdash A_1, B_1, \Gamma'_1 \vdash C_1 \quad \Gamma_2, A_1 \rightarrow B_1 \vdash A_2, B_2, \Gamma'_2 \vdash C_2 \quad \Gamma_1, \Gamma'_1, A_1 \rightarrow B_1, A_2 \rightarrow B_2 \vdash C_1 \quad \Gamma_2, \Gamma'_2, A_1 \rightarrow B_1, A_2 \rightarrow B_2 \vdash C_2$$
Because of the form of the premises of an MC-pair, \( z \) should substitute \( I \) at least for all the variables of \( I'_1, I'_2, B_1, C_1, B_2, C_2 \). Let us substitute \( I \) for these variables only and "purify" the result. It may contain antecedent members of the form \( a, a \otimes b \); let us substitute \( I \) for their variables. If the new members of such form appear the procedure may be repeated. It is clear that we shall arrive to some "fixpoint" substitution \( z_1 \) and if \( z \) exists then \( x_1 \subseteq x \). The pair \( x_1 \ast d_1, x_1 \ast d_2 \) will either satisfy (1) or the final sequent of these derivations will be \( I \vdash I \). In the second case there is no \( z \) creating an MC pair (with key formulas obtained from \( A_1 \vdash B_1, A_2 \vdash B_2 \).

**Condition (2).** Suppose we have obtained an MC-candidate using \( z_1 \). The derivations \( x_1 \ast d_i \) cannot end by \( \vdash \circ \), \( \delta \vdash \delta \) because the right side of the final sequent of \( x_1 \ast d_1, x_1 \ast d_2 \) is \( I \) and the left side of a pure 2-sequent does not contain formulas of the form \( C \otimes D \).

The derivations \( x_1 \ast d_i \) are equivalent to some derivations that end by \( WKN \) iff its endsequent splits. It is the only possible reason why the pair \( x_1 \ast d_1, x_1 \ast d_2 \) may not satisfy (2).

If the MC-candidate does not satisfy (2), the final sequent splits into components

4 two members are linked if they contain the same variable (with opposite signs).
does not satisfy the condition (3) then there is a $\rightarrow_0$-separable part in $\Lambda,\Lambda_1' \rightarrow I \vdash I$ or in $\Lambda,\Lambda_2' \rightarrow I \vdash I$.

The following is an obvious (and useful) reformulation:

**Lemma 12.** If the pair above is a strong MC-candidate, $\Lambda,\Lambda_1' \rightarrow I \vdash I$ and $\Lambda,\Lambda_2' \rightarrow I \vdash I$ do not contain the $\rightarrow_0$-separable parts, then it is an MC-pair.

The identification of the $\rightarrow_0$-separable parts can be done quickly. The difficulty is that not every $\rightarrow_0$-separable part may be the left premise of some $\rightarrow\vdash$-rule in a derivation that is equivalent to $\xi_1$ or $\xi_2$ (cf. Example 2). If it were true, it would be enough to check whether such parts are present.

### 3.1.1. Partial order of $\rightarrow_0$-separable parts

**Definition 13.** We define $\Sigma \vdash A \triangleleft \Sigma, A \rightarrow B, \Sigma' \vdash C$ where $\Sigma \vdash A$ and $\Sigma, A \rightarrow B, \Sigma' \vdash C$ are $\rightarrow_0$-separable parts of the same sequent.

Let us consider a sequent $\Gamma, A \rightarrow B, \Gamma' \vdash C$ and let $\Gamma \vdash A$ be a $\rightarrow_0$-separable part.

The substitution of $I$ for all the variables of $B, \Gamma', C$ will be called $\rightarrow$-substitution.

We shall call the iterated $\rightarrow$-substitution any substitution which may be regarded as a union (or the result of successive applications) of several $\rightarrow$-substitutions. An iterated $\rightarrow$-substitution is not necessarily a $\rightarrow$-substitution.

**Example 14.** Assume that $\Gamma, A \rightarrow B, \Gamma' \vdash C$ has $\Gamma \vdash A$ as a $\rightarrow_0$-separable part and that in $\Gamma, A \rightarrow I \vdash I$ there is a $\rightarrow_0$-separable part of the form $\Gamma_1, A \rightarrow I \vdash D$, i.e., $\Gamma = \Gamma_1, D \rightarrow E, \Gamma_2$ and $A$ has variables in common with $\Gamma_1, D$ but not with $\Gamma_2, E$.

Then the union of the substitution $\beta$ of $I$ for $B, \Gamma', C$ and the substitution $\beta'$ of $I$ for $E, \Gamma'$ is an iterated $\rightarrow$-substitution but not a $\rightarrow$-substitution.

**Lemma 15.** If $\beta$ is an iterated $\rightarrow$-substitution and $d$ is not a wkn$_-\otimes\vdash$-derivation then $\beta \ast d$ is not a wkn$_-\otimes\vdash$-derivation.

**Proof.** It is enough to show that the lemma is true for single $\rightarrow$-substitution.

Suppose that $\Gamma, A \rightarrow I \vdash I$ is obtained from $\Gamma, A \rightarrow B, \Gamma' \vdash C$ by substitution of $I$ for all variables of $B, \Gamma', C$. If $\Gamma$ contains some member of the form $C \otimes D$ then $d$ is a $\otimes\vdash$-derivation.

If $\Gamma, A \rightarrow I \vdash I$ splits (and $\beta \ast d$ is a wkn$-$-derivation) then one of the components of $\Gamma, A \rightarrow I$ does not contain $A \rightarrow I$. The same component is present in $\Gamma, A \rightarrow B, \Gamma' \vdash C$. Then this sequent splits and $d$ is a wkn-derivation. $\square$

**Lemma 16.** Let the derivation $\Gamma \vdash I$ be obtained by an iterated $\rightarrow$-substitution from some derivation $d$ (which is not wkn, $\otimes$ derivation). If the last rule in $\beta \ast d$ is $\rightarrow\vdash$-
with the left premise $I_0 \vdash_0 F$ that was not affected by the substitution $\beta$ then

$$d \equiv \frac{\Gamma_0 \vdash_0 F \ G, \Gamma' \vdash C}{\Gamma_0, F \rightarrow_0 G, \Gamma'' \vdash C}.$$  

**Proof.** Let us consider the inference $\rightarrow_0 F \rightarrow_0 G'$ in $d$ ($G$ but not $F$ could be affected by $\beta$, so we note its ancestor by $G'$).

In addition to the members of $I_0$ the antecedent of its left premise may contain only some parts that disappear under $\beta$.

These parts may form only a balanced list $\Delta$ that has no variables in common with $\vdash_0 F$.

Thus we may assume that the subderivation $d'_0$ of $I_0, \Delta \vdash F$ in $d$ is equivalent to a derivation that ends by $wkn$. More precisely,

$$d'_0 \equiv \frac{\Delta \vdash I \ I_0 \vdash F}{\Delta, \Gamma \vdash F}.$$  

In this case

$$d''_0 \equiv \frac{\Delta \vdash I \ I_0 \vdash F \ G', \Gamma'' \vdash H}{\Delta, \Gamma_0 \vdash F} \equiv \frac{\Delta, \Gamma_0 \vdash F \rightarrow_0 G', \Gamma'' \vdash H}{\Delta, \Sigma, F \rightarrow_0 G', \Gamma'' \vdash H}$$

and the $\rightarrow_0 F \rightarrow_0 G'$ can be successfully pushed down. □

**Lemma 17.** Let $\beta * d : \Gamma, A \rightarrow_1 I \rightarrow I$ be obtained by $+_{-}$-substitution $\beta$ from $d : \Gamma, A \rightarrow B$, $A \vdash C$ where $\Gamma \vdash A$ is a $\rightarrow_0$-separable part, $\beta$ substitutes $I$ for all variables of $B, A, C$ and $d$ is not a wkn-$\rightarrow_0 \circ \vdash -$-derivation. If $d$ is not equivalent to the $\rightarrow_0 \vdash -$-derivations with the left premise lesser than $\Gamma \vdash A$ then

$$\beta * d \equiv \frac{d'}{\Delta, A \rightarrow_1 I \rightarrow I} \Rightarrow d \equiv \frac{d'}{\Delta, A \rightarrow_1 B, A \vdash C}.$$  

**Proof.** Induction on the number of the $\rightarrow_0$-separable parts in $\Gamma$. We need the following proposition.

**Proposition 18.** I.H. of the lemma implies the following: Let $\beta'$ be an iterated $+_{-}$-substitution containing $\beta$ such that $\beta'*d : \Gamma', A_1 \rightarrow I, A_2 \rightarrow I \rightarrow I$ where $\Gamma'$ was not affected by $\beta'$ (all its members are the same as in the antecedent of the endsequent of $d$). Assume that

$$\beta'*d \equiv \frac{\Gamma', A_1 \rightarrow_1 I \rightarrow_1 A_2 \rightarrow_1 I \rightarrow I}{\Gamma', A_1 \rightarrow_1 I, A_2 \rightarrow_1 I \rightarrow I} \equiv \frac{f_1}{\Gamma', A_1 \rightarrow_1 I \rightarrow_1 A_1 \rightarrow_1 I \rightarrow_1 I} \equiv \frac{f_2}{\Gamma', A_1 \rightarrow_1 I, A_2 \rightarrow_1 I \rightarrow_1 I}.$$
In this case there exists a \( \searrow \)-separable part \( \Gamma_0 \vdash F \) in \( \Gamma' \) such that

\[
\begin{align*}
\Gamma_0 \vdash F, \Gamma_0', A \searrow B, A \vdash C \\
\Gamma_0, F \searrow G, \Gamma_0', A \searrow B, A \vdash C
\end{align*}
\]

\((\Gamma_0, F \searrow G, \Gamma_0' = \Gamma)\).

**Proof of the proposition.** Induction on the length of \( \Gamma' \).

**Base.** If \( \Gamma' \) is empty the configuration is impossible.

**Inductive step.** The pair

\[
\begin{array}{ll}
\Gamma', A_1 \searrow I \vdash A_2 I \vdash I & \Gamma', A_2 \searrow I \vdash A_1 I \vdash I \\
\Gamma', A_1 \searrow I, A_2 \searrow I \vdash I & \Gamma', A_1 \searrow I, A_2 \searrow I \vdash I
\end{array}
\]

is not an MC-pair. The conditions (1) and (2) of the definition being satisfied, only the condition (3) might be wrong.

If (3) is wrong then \( f_1 \) and/or \( f_2 \) is equivalent to some \( \searrow \vdash \)-derivation. Assume that \( f_1 \equiv f \) where \( f \) ends by \( \searrow \vdash \). The left premise of this \( \searrow \vdash \) does or does not contain \( A_1 \searrow I \).

If it does, it has the form \( \Gamma_0, A_1 \searrow I \vdash D \). We may substitute \( I \) for all variables that are not in this premise. We obtain an iterated \( + \)-substitution that includes \( \beta' \) and we may apply I.H. of the proposition.

If it does not, the left premise of the last \( \searrow \vdash \) of \( f \) is \( \Gamma_0 \vdash F \). It contains less \( \searrow \)-separable parts than \( \Gamma \vdash A \) and by the I.H. of the main lemma \( d \) is equivalent to a derivation that ends by this \( \searrow \vdash \).

Note that the second case is impossible if the number of \( \searrow \)-separable parts of \( \Gamma \vdash A \) in the main lemma is 0. If it is so, the proposition holds without the assumption about I.H. of the main lemma. \( \square \)

Now we may proceed with the proof of the lemma.

First of all, if the last rule of \( \beta \ast d \) is \( \searrow_{A \rightarrow I} \vdash \), then its left premise is \( \Gamma \vdash A \) and by Lemma 16 \( d \) is equivalent to a derivation with the same left premise.

Thus, it is enough to show that if the derivation \( \beta \ast d \) does not end by \( \searrow_{A \rightarrow I} \vdash \) then (in the conditions of the lemma) it is not equivalent to a derivation ending by \( \searrow_{A \rightarrow I} \vdash \).

The following observation corresponds to base case and to inductive step. If the last rule of \( \beta \ast d \) is not \( \searrow_{A \rightarrow I} \vdash \), then it is another \( \searrow \vdash \), say \( \searrow_{D \rightarrow E} \vdash \) (only \( \searrow \vdash \) can be the last rule, because the sequent is of the form \( \Gamma, A \rightarrow I \vdash I \), and \( wkn, \otimes \vdash \) are excluded by the condition on \( d \)).

**Base of induction.** There is no \( \searrow \)-separable parts in \( \Gamma \vdash A \). If the last rule of \( \beta \ast d \) is \( \searrow_{D \rightarrow E} \vdash \) there could be two possibilities: its left premise contains or does not contain \( A \rightarrow I \).

If it contains \( A \rightarrow I \) we may substitute \( I \) for all variables that are not in this left premise and apply Proposition 18. This gives contradiction.

The case when it does not contain \( A \rightarrow I \) is impossible (contradicts the assumption that there is no smaller \( \searrow \)-separable parts).
Thus, in this case $\beta \ast d$ cannot be equivalent to the derivation ending by $\neg \alpha \ast I$.

**Inductive step.** Assume that the I.H. is true. Again, if the last rule of $\beta \ast d$ is $\neg \alpha \quad \Gamma \vdash d$ there could be two possibilities: its left premise contains or does not contain $A \neg \alpha I$.

If it contains $A \neg \alpha I$ we substitute $I$ for all variables that are not in this left premise and apply Proposition 18. The result gives contradiction with the assumption that $d$ is not equivalent to a $\neg \alpha \vdash$-derivation with smaller $\neg \alpha$-separable part as the left premise of its last $\neg \alpha \vdash$.

If it does not, its left premise is $\neg \alpha \vdash D$. We substitute $I$ for all the variables that do not belong to $\neg \alpha \vdash D$. Let $\beta''$ be this substitution. Note that it is a $+$-substitution. We may apply I.H. to $\beta'' \ast d$, and obtain contradiction with the assumption that $d$ is not equivalent to the $\neg \alpha \vdash$-derivations with smaller $\neg \alpha$-separable parts as left premises.

**Corollary 19.** In the conditions of the lemma $d$ is equivalent to a derivation ending by $\neg \alpha A \neg \alpha B$ iff $\beta \ast d$ ends by $\neg \alpha A \neg \alpha I$.

Thus, we could replace the verification of the condition (3) by the verification what rule is the last in some derivations obtained by $+$-substitutions. We should stress that it is the verification what rule is actually the last (not up to $\equiv$).

The verification should begin from smallest $\neg \alpha$-separable parts. If at some step we show that the derivation is equivalent to a derivation ending by $\neg \alpha \vdash$, $I$ has to be substituted for this left premise. Iterating this procedure we either obtain an MC-pair or show that no MC-pair can be obtained with the KF-candidates considered at the moment. In the first case we have shown that the derivations are not equivalent. In the second the next pair of KF-candidates should be considered.

3.2. The algorithm (main steps)

1. Perform cut-elimination.
2. Find the derivations of balanced sequents such that $d_1, d_2$ are obtained by identifications of variables. If the balanced sequents corresponding to $\Gamma \vdash A$ in case of $d_1$ and $d_2$ are different, $d_1$ is not equivalent to $d_2$.
3. If the (final) balanced sequents are the same, reduce to (pure) 2-sequents.
4. Mark and order in some way the pairs of KF-candidates.
5. Let a pair be fixed. Find the applications of $\neg \alpha \vdash$ in the first and second derivations where the first (the second) KF-candidate is the main formula. Substitute $I$ for all variables that lie in at least one of the right premises of these $\neg \alpha \vdash$. Let $\alpha_1$ be the substitution.
6. If in the final sequent of $\alpha_1 \ast d_1$ and $\alpha_1 \ast d_2$ (it is the same) there are members of the form $a$ or $a \otimes b$ then $I$ should be substituted for the variables of these members (and simplifications in the sense of $\ast$ should be made). The process is iterated until there is no more such members.
7. If the result does not satisfy condition (1) of Definition 7, the pair of formulas (KF-candidates) is discarded and we consider next pair.
8. If it is a MC-candidate, we verify condition (2). That is, we verify if the final sequent splits into components that have no common variables. If it is the
case, we verify if the KF-candidates belong to the same or different components. If they belong to different components, MC-pair cannot be obtained (using these KF-candidates), we take new pair and return to 4. If they belong to the same component, we substitute I for all variables that do not belong to this component, “purify” the sequent. The result is a strong MC-candidate. Then we go to 9.

(9) We find all \( \neg \circ \)-separable parts and order them.

(10) We begin from the smallest \( \neg \circ \)-separable parts and check if one of the derivations of left premises of the last \( \neg \circ \)-rules is equivalent to some derivation that ends by \( \neg \circ \) with this \( \neg \circ \)-separable part as its left premise (as described in the lemma above). If such derivation does exists, with corresponding \( \neg \circ \)-separable part \( \Sigma \vdash D \) as its left premise, we substitute I for all variables of \( \Sigma, D \) (in the sense of the operation \( * \)) and return to 6.

If the check was negative, the pair under consideration is an MC-pair and initial derivations are not equivalent.

(11) If we checked all MC-candidates without obtaining an MC-pair the derivations are equivalent.

3.3. Complexity

The proofs in \( L \) are represented by trees where each node contains a sequent and an analysis consisting of the code of corresponding axiom or rule together with the pointers to the premises, and the numbers of the main and side formulas. The analysis of the rule \( \text{perm} \) contains the permutation of the antecedent. Note that the rules \( \text{cut} \) and \( \text{wkn} \) do have side formulas but not the main formula.

The tree containing only the analyses of the rules (without sequents) is called the proof-scheme.

Let us call the size of a sequent the total number of symbols (connectives, variables and constants) in \( S \). The size will be denoted by \( |S| \).

The size of derivation \( d \) (denoted by \( |d| \)) is the total number of symbols in the tree-form presentation of \( d \).

\( t(d) \) will denote the number of nodes in the proof-tree of \( d \).

Let us call an application of \( \text{wkn} \) regular if its left premise is the axiom \( I \vdash I \).

The derivation \( d \) is called regular if it doesn’t contain \( \text{cut} \) and all applications of \( \text{wkn} \) in \( d \) are regular.

Lemma 20. There exists an algorithm \( \rho \) defined on \( L \)-derivations such that:

1. for every derivation \( d \) of the sequent \( S \), \( \rho(d) \) is regular, the last sequent of \( \rho(d) \) is \( S \) and \( \rho(d) \equiv d \);
2. \( t(\rho(d)) \leq t(d) \);
3. the number of reductions used to transform \( d \) into \( \rho(d) \) is bound by \( (t(d))^2 \) and the number of elementary operations necessary to perform one reduction is proportional to the size of the sequents, thus the number of elementary operations used to transform \( d \) into \( \rho(d) \) is bound by \( C_0 \cdot t(d) \cdot |d| \) for some constant \( C_0 \).
Theorem 21. Let \( d_1, d_2 \) be regular derivations of the same sequent \( S \). The complexity (number of elementary operations) of the algorithm of verification of the equivalence \( d_1 \equiv d_2 \) described above is bound by \( C|K|^2|S|\max(|d_1|, |d_2|) \) where \( S \) is the final sequent of \( d_1 \) and \( d_2 \) and \( K \) is the number of formulas of the form \( (a \rightarrow b) \rightarrow c \) in the 2-sequent obtained from \( S \). This bound can be replaced by the following (weaker) one: \( C|S|^2\max(|d_1|, |d_2|) \).

Note that the bound in terms of \( \max(|d_1|, |d_2|) \) could be much better, especially in case if we begin with non-regular derivations.

4. Equivalence and permutations of inferences

The results described in this part complete the results of Section 3. They show the connection between permutations of rules and categorical equivalence of derivations.

Let us call the derivation \( d \) of the sequent \( S \) 0-regular if \( d \) is an axiom or any proof \( d' \) that can be obtained from \( d \) by permutations of inferences described in Section 2 ends by \( \text{cut} \), \( \vdash \otimes \) or \( \vdash \omega \).

Lemma 22. If the succedent of the endsequent of a 0-regular proof \( d \) without cut is a variable then \( d \) is an axiom.

Let us call the derivation \( d \) 1-regular if the following conditions are satisfied:

1. \( d \) does not contain \( \text{cut} \);
2. left premises of \( \text{wkn} \) in \( d \) are axioms \( I \vdash I \);
3. the derivations of the left premises of \( \rightarrow \vdash \) in \( d \) are 0-regular;
4. the derivations of both premises of \( \vdash \otimes \) in \( d \) are 0-regular;
5. the derivations of the conclusions of all \( \vdash \omega \) and \( \vdash \otimes \) in \( d \) also are 0-regular.

V. Orevkov obtained the following theorems:

Theorem 23. Every cut-free proof \( d \) can be transformed into some 1-regular proof via permutations of rule inferences described in Section 2.

Theorem 24. Let \( d_1, d_2 \) be any cut-free derivations of a balanced pure 2-sequent \( S \). If \( d_1 \equiv d_2 \) then \( d_1 \) and \( d_2 \) can be transformed into the same 1-regular derivation via permutations of inferences described in Section 2.

References