

# A Characterisation of Medial as Rewriting Rule

Lutz Straßburger

INRIA Futurs, Projet Parsifal

École Polytechnique — LIX — Rue de Saclay — 91128 Palaiseau Cedex — France  
<http://www.lix.polytechnique.fr/~lutz>

**Abstract.** Medial is an inference rule scheme that appears in various deductive systems based on deep inference. In this paper we investigate the properties of medial as rewriting rule independently from logic. We present a graph theoretical criterion for checking whether there exists a medial rewriting path between two formulas. Finally, we return to logic and apply our criterion for giving a combinatorial proof for a decomposition theorem, i.e., proof theoretical statement about syntax.

## 1 Introduction

An interesting question to ask about a given rewriting system is not only whether it is terminating or confluent, but also whether there is a rewriting path between two given terms. This question occurs, for example, in proof search, where one is interested in finding a proof for a formula  $P$ , i.e., a rewriting path from “truth” to  $P$  using the inference rules of the deductive system. Alternatively, one can ask for a refutation of  $P$ , which is nothing but a rewriting path from  $P$  to “falsum”, where the meanings of “truth” and “falsum” depend on the logic in question.

The next natural question to ask is whether we can characterize the existence of a rewriting path between two given terms independently from the rewriting system. For example in [BdGR97], a rewriting system was presented which could be characterized by the inclusion relation of series-parallel orders. Other well-known examples of such characterizations are the various correctness criteria for proof nets for multiplicative linear logic (e.g., [DR89,Ret96,DHPP99,Str03a]).

The work presented in this paper is in line with these results. The rewriting system that we analyze consists only of the medial rule [BT01], which plays an increasing role in the proof theory for classical propositional logic, in particular, in the investigation of the identity of proofs [Str05] and for giving semantics to proofs [Lam06]. Our characterization will be carried out in terms of *relation webs* [Gug07], and is in spirit very close to the work in [BdGR97].

This paper is organized as follows: In the next section we will first explain informally what the medial rule is. Then, in Sections 3 and 4, we will set the stage by formally defining our rewrite system and by introducing the notion of relation web. The main part of the paper is Section 5, in which we prove our main result. The remaining sections compare the result to related work and show an application in proof theory.

## 2 What is medial ?

Let  $\bullet$  and  $\circ$  be two binary operations and consider the equation

$$(x \bullet y) \circ (w \bullet z) = (x \circ w) \bullet (y \circ z) \quad , \quad (1)$$

which is known under the name “middle four exchange” [Mac71]. If we consider  $\bullet$  as “horizontal” composition and  $\circ$  as “vertical” composition, we can give (1) the following geometric interpretation:

$$\begin{array}{|c|c|} \hline x & y \\ \hline w & z \\ \hline \end{array} = \begin{array}{|c|c|} \hline x & y \\ \hline w & z \\ \hline \end{array} = \begin{array}{|c|} \hline x \\ \hline w \\ \hline \end{array} \begin{array}{|c|} \hline y \\ \hline z \\ \hline \end{array}$$

Let us now assume that one of  $\bullet$  and  $\circ$  is stronger, in the sense that the equation (1) gets a direction and becomes a rewriting rule

$$(x \bullet y) \circ (w \bullet z) \rightarrow (x \circ w) \bullet (y \circ z) \quad . \quad (2)$$

If we read  $\bullet$  as “and”  $\wedge$  and  $\circ$  as “or”  $\vee$ , then (2) becomes a valid implication of Boolean logic

$$(x \wedge y) \vee (w \wedge z) \rightarrow (x \vee w) \wedge (y \vee z) \quad . \quad (3)$$

while the other direction would not yield a valid implication. The same situation appears in linear logic if we let  $\langle \bullet, \circ \rangle$  be any of the pairs  $\langle \otimes, \oplus \rangle$ ,  $\langle \wp, \oplus \rangle$ ,  $\langle \&, \oplus \rangle$ ,  $\langle \&, \wp \rangle$ , or  $\langle \&, \otimes \rangle$ . In [BT01], the implication (3) is used as an inference rule in a deductive system for classical logic

$$\text{m} \frac{F\{(A \wedge C) \vee (B \wedge D)\}}{F\{(A \vee B) \wedge (C \vee D)\}} \quad , \quad (4)$$

where  $A, B, C, D$  stand for arbitrary formulas and  $F\{ \}$  for an arbitrary (positive) formula context. Note that (3) and (4) are just different ways of writing the same thing. In [BT01], Brünnler and Tiu gave the name *medial* to the rule (4). They observed that under the presence of the medial rule, the general contraction rule can be reduced to an atomic version:

$$\text{c} \frac{F\{A \vee A\}}{F\{A\}} \quad \rightsquigarrow \quad \text{c} \frac{F\{a \vee a\}}{F\{a\}} \quad , \quad (5)$$

where  $A$  is an arbitrary formula and  $a$  is just an atom (or literal). In [Str02], the same has been observed for linear logic.

## 3 Rewriting with medial

We have in our language two binary function symbols and a countable set  $\mathcal{A} = \{a, b, c, \dots\}$  of constant symbols. The set  $\mathcal{T}$  of terms is defined by the grammar

$$\mathcal{T} ::= \mathcal{A} \mid (\mathcal{T} \bullet \mathcal{T}) \mid [\mathcal{T} \circ \mathcal{T}]$$

For the two binary function symbols we use infix notation. To ease the readability, we use different types of parentheses:  $(\dots)$  for the  $\bullet$  and  $[\dots]$  for the  $\circ$ .<sup>1</sup>

<sup>1</sup> Note that this goes in line with the usual notation used in the literature on deep inference, e.g., [BT01,GS01,DG04].

We will use capital Latin letters to denote terms. To ease readability, we will sometimes write  $(x \bullet y \bullet z)$  for  $((x \bullet y) \bullet z)$  and  $[x \circ y \circ z]$  for  $[[x \circ y] \circ z]$ .

Let AC be the following set of equations on terms, saying that  $\bullet$  and  $\circ$  are both associative and commutative:

$$\begin{aligned} (x \bullet y) &\approx (y \bullet x) & ((x \bullet y) \bullet z) &\approx (x \bullet (y \bullet z)) \\ [x \circ y] &\approx [y \circ x] & [[x \circ y] \circ z] &\approx [x \circ [y \circ z]] \end{aligned} \quad (6)$$

where  $x$ ,  $y$ , and  $z$  are variables. Let  $\approx_{\text{AC}}$  be the equational theory induced by AC, i.e., the smallest congruence relation containing AC.

Now let M be the rewriting system consisting only of the medial rule

$$[(x \bullet y) \circ (w \bullet z)] \rightarrow ([x \circ w] \bullet [y \circ z]) \quad , \quad (7)$$

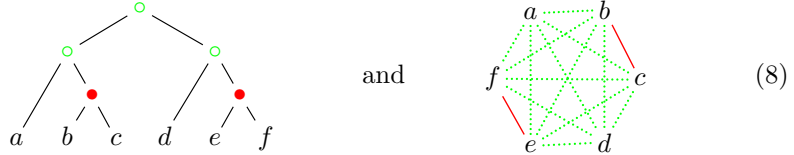
where  $x$ ,  $y$ ,  $z$ , and  $w$  are variables. The object of interest in this paper is the rewrite relation  $\rightarrow_{\text{M/AC}}$ , i.e., rewriting via the medial rule modulo associativity and commutativity of the two binary operations. More formally: Let  $P$  and  $Q$  be terms. Then  $P \rightarrow_{\text{M/AC}} Q$ , if and only if there are terms  $P'$  and  $Q'$  such that  $P \approx_{\text{AC}} P'$  and  $P' \rightarrow_{\text{M}} Q'$  and  $Q' \approx_{\text{AC}} Q$ , where  $P' \rightarrow_{\text{M}} Q'$  means there is a single rewriting step from  $P'$  to  $Q'$  using the rule in (7). For more details on the formal definitions see, e.g, [BN98]. Since no ambiguity is possible here, we omit the index AC and simply write  $P \approx Q$  instead of  $P \approx_{\text{AC}} Q$ . Further, we write  $P \xrightarrow{\text{M}} Q$  instead of  $P \rightarrow_{\text{M/AC}} Q$ , and we define  $\xrightarrow{\text{M}}^*$  to be the transitive closure of  $\xrightarrow{\text{M}}$ . We are interested in the question: *Under which conditions do we have  $P \xrightarrow{\text{M}}^* Q$  ?*

## 4 Relation webs

For simplifying the definitions, we will in the following assume that every constant symbol appears at most once in a term. This allows us to ignore the distinction between constants and constant occurrences. What matters in this and the next section are the positions occupied by the constants in the terms.

For a given term  $P$ , let  $\mathcal{V}_P$  denote the set of constants occurring in  $P$ . Let us now treat a term as a binary tree whose inner nodes are labeled by either  $\bullet$  or  $\circ$ , and whose leaves are the elements of  $\mathcal{V}_P$ . For  $a, b \in \mathcal{V}_P$  we write  $a \overset{\bullet}{\widehat{P}} b$  if their first common ancestor in  $P$  is a  $\bullet$  and we write  $a \overset{\circ}{\widehat{P}} b$  if it is a  $\circ$ . Furthermore, we define  $\mathcal{E}_P^\bullet = \{(a, b) \in \mathcal{V}_P \times \mathcal{V}_P \mid a \overset{\bullet}{\widehat{P}} b\}$  and  $\mathcal{E}_P^\circ = \{(a, b) \in \mathcal{V}_P \times \mathcal{V}_P \mid a \overset{\circ}{\widehat{P}} b\}$ . Note that  $\mathcal{E}_P^\bullet$  and  $\mathcal{E}_P^\circ$  are symmetric, i.e.,  $(a, b) \in \mathcal{E}_P^\bullet$  iff  $(b, a) \in \mathcal{E}_P^\bullet$ . We also have  $\mathcal{E}_P^\bullet \cap \mathcal{E}_P^\circ = \emptyset$  and  $\mathcal{E}_P^\bullet \cup \mathcal{E}_P^\circ = (\mathcal{V}_P \times \mathcal{V}_P) \setminus \{(a, a) \mid a \in \mathcal{V}_P\}$ . The triple  $\otimes P = \langle \mathcal{V}_P; \mathcal{E}_P^\bullet, \mathcal{E}_P^\circ \rangle$  is called the *relation web of  $P$* . We can think of it as a complete undirected graph with vertices  $\mathcal{V}_P$  and edges  $\mathcal{E}_P^\bullet \cup \mathcal{E}_P^\circ$  where we color the edges in  $\mathcal{E}_P^\bullet$  red and the edges in  $\mathcal{E}_P^\circ$  green.

Consider for example the term  $P = [[a \circ (b \bullet c)] \circ [d \circ (e \bullet f)]]$ . Its syntax tree and its relation web are, respectively,



where the red lines are solid and green lines are drawn as dotted lines.

It is now easy to see that we have the following:

**4.1 Proposition** *Let  $P$  and  $Q$  be terms. Then  $\otimes P = \otimes Q$  iff  $P \approx Q$ .*

More interesting, however, is the question, under which circumstances a triple  $\langle \mathcal{V}; \mathcal{E}^\bullet, \mathcal{E}^\circ \rangle$  is indeed the relation web of a term. Let us define a *preweb* to be a triple  $\langle \mathcal{V}; \mathcal{E}^\bullet, \mathcal{E}^\circ \rangle$  where  $\mathcal{E}^\bullet$  and  $\mathcal{E}^\circ$  are symmetric subsets of  $\mathcal{V} \times \mathcal{V}$  such that

$$\mathcal{E}^\bullet \cap \mathcal{E}^\circ = \emptyset \quad \text{and} \quad \mathcal{E}^\bullet \cup \mathcal{E}^\circ = (\mathcal{V} \times \mathcal{V}) \setminus \{(a, a) \mid a \in \mathcal{V}\} \quad . \quad (9)$$

**4.2 Proposition** *Let  $\mathcal{G} = \langle \mathcal{V}; \mathcal{E}^\bullet, \mathcal{E}^\circ \rangle$  be a preweb. Then  $\mathcal{G} = \otimes P$  for some term  $P$  if and only if we do not have any  $a, b, c, d \in \mathcal{V}$  with*

$$\begin{array}{ccc} a & \cdots & b \\ | & \diagdown & | \\ | & & | \\ | & \diagup & | \\ c & \cdots & d \end{array} \quad (10)$$

**Proof:** See, e.g., [Ret93,BdGR97,Gug07]. □

Let  $P$  be a term and let  $\mathcal{W} \subseteq \mathcal{V}_P$ . Then we can obtain from  $\otimes P$  a new relation web  $(\otimes P)|_{\mathcal{W}} = \langle \mathcal{W}; \mathcal{F}^\bullet, \mathcal{F}^\circ \rangle$  by simply removing all vertices not belonging to  $\mathcal{W}$  and all edges adjacent to them. Similarly we can obtain from  $P$  a term  $P|_{\mathcal{W}}$  by removing in the term tree all leaves not in  $\mathcal{W}$  and then systematically removing all  $\circ$ - and  $\bullet$ -nodes that became unary by this. More formally, we define  $a|_{\mathcal{W}} = a$  if  $a \in \mathcal{W}$  and

$$[A \circ B]|_{\mathcal{W}} = \begin{cases} [A|_{\mathcal{W}} \circ B|_{\mathcal{W}}] & \text{if } \mathcal{V}_A \cap \mathcal{W} \neq \emptyset \text{ and } \mathcal{V}_B \cap \mathcal{W} \neq \emptyset \\ A|_{\mathcal{W}} & \text{if } \mathcal{V}_A \cap \mathcal{W} \neq \emptyset \text{ and } \mathcal{V}_B \cap \mathcal{W} = \emptyset \\ B|_{\mathcal{W}} & \text{if } \mathcal{V}_A \cap \mathcal{W} = \emptyset \text{ and } \mathcal{V}_B \cap \mathcal{W} \neq \emptyset \\ \text{undefined} & \text{otherwise} \end{cases}$$

and similarly we define  $(A \bullet B)|_{\mathcal{W}}$ . Clearly we then have  $\otimes(P|_{\mathcal{W}}) = (\otimes P)|_{\mathcal{W}}$ , but note that  $P|_{\mathcal{W}}$  is not necessarily a subterm of  $P$ . For example, let  $P = [(a \bullet b) \circ (c \bullet [(d \bullet e) \circ f])]$  and  $\mathcal{W} = \{a, c, f\}$ . Then  $P|_{\mathcal{W}} = [a \circ (c \bullet f)]$ . If we have another term  $Q$  with  $\mathcal{V}_P \cap \mathcal{V}_Q \neq \emptyset$  then we write  $P|_Q$  to abbreviate  $P|_{\mathcal{V}_P \cap \mathcal{V}_Q}$ .

The term “relation web” first appears in [Gug07]. The basic idea, however, is much older. In graph theory, a graph  $\langle \mathcal{V}; \mathcal{E}^\bullet \rangle$  not containing configuration (10) is called  *$P_4$ -free*. It is also called a *cograph* because its complement  $\langle \mathcal{V}; \mathcal{E}^\circ \rangle$  has the same property. Cographs are used in [Ret96] to provide a correctness criterion for linear logic proof nets, where  $\langle \bullet, \circ \rangle$  is  $\langle \otimes, \wp \rangle$ . One can also find the terms  *$N$ -free* or  *$Z$ -free* if configuration (10) is forbidden, depending on how the picture is drawn. A comprehensive survey is for example [Möh89]. If  $\bullet$  is not commutative, but only associative, then  $\mathcal{E}^\bullet$  becomes a partial order, more precisely, a *series-parallel order* (by Proposition 4.2 it can be obtained from the singletons via series- and parallel composition of orders). The inclusion relation for these orders has been characterized by a rewriting system in [BdGR97].

**4.3 Remark** Proposition 4.2 also scales to the case with more than two binary operations. For example in [Ret93,BdGR97,Gug07] it is proved for the case of two commutative operations and one non-commutative operation.

## 5 The Characterisation of Medial

For two terms  $P$  and  $Q$ , we write  $P \blacktriangleleft Q$  if their relation webs obey the following three properties:

- (i)  $\mathcal{V}_P = \mathcal{V}_Q$ ,
- (ii)  $\mathcal{E}_P^\bullet \subseteq \mathcal{E}_Q^\bullet$  (or, equivalently,  $\mathcal{E}_Q^\circ \subseteq \mathcal{E}_P^\circ$ ), and
- (iii) for all  $a, d \in \mathcal{V}_P (= \mathcal{V}_Q)$  with  $a \overset{\circ}{\underset{P}{\rhd}} d$  and  $a \overset{\bullet}{\underset{Q}{\rhd}} d$ , there are  $b, c \in \mathcal{V}_P$  such that we have the following configurations

$$\text{in } \otimes P: \begin{array}{ccc} a & \text{---} & b \\ & \diagdown & \diagup \\ & c & \\ & \diagup & \diagdown \\ c & \text{---} & d \end{array} \quad \text{in } \otimes Q: \begin{array}{ccc} a & \text{---} & b \\ & \diagup & \diagdown \\ & c & \\ & \diagdown & \diagup \\ c & \text{---} & d \end{array} \quad (11)$$

The motivation for this definition is the following theorem.

**5.1 Theorem** *For two terms  $P$  and  $Q$  we have  $P \xrightarrow{*}_M Q$  iff  $P \blacktriangleleft Q$ .*

When proving this theorem, we make crucial use of two lemmas.

**5.2 Lemma** *Let  $P$  and  $Q$  be terms with  $P \xrightarrow{*}_M Q$ . If  $P'$  is a subterm of  $P$ , then  $P' \xrightarrow{*}_M Q|_{P'}$ . And if  $Q_1$  is a subterm of  $Q$ , then  $P|_{Q_1} \xrightarrow{*}_M Q_1$ .*

**Proof:** Since  $P \xrightarrow{*}_M Q$ , we have an  $n \geq 0$  and terms  $R_0, \dots, R_n$ , such that  $P \approx R_0 \xrightarrow{M} R_1 \xrightarrow{M} \dots \xrightarrow{M} R_n \approx Q$ . We will say an  $R_i$  (for  $0 \leq i \leq n$ ) is *nested* if there is a term  $R \approx R_i$  which has a subterm  $[(A_1 \bullet B_1) \circ (A_2 \bullet B_2)]$  such that  $\mathcal{V}_{A_1} \cap \mathcal{V}_{P'} \neq \emptyset$  and  $\mathcal{V}_{A_2} \cap \mathcal{V}_{P'} \neq \emptyset$  and  $\mathcal{V}_{B_1} \cap \mathcal{V}_{P'} = \emptyset$ . We first show that none of the  $R_i$  can be nested. Clearly  $R_0 (\approx P)$  is not nested. Now we proceed by way of contradiction and pick the smallest  $i$  such that  $R_i$  is nested. Since  $R_i$  is obtained from  $R_{i-1}$  via a medial rewriting step, we can, without loss of generality, assume that  $A_1 = [A \circ C]$  and  $B_1 = [B \circ D]$  such that  $\mathcal{V}_A \cap \mathcal{V}_{P'} \neq \emptyset$  and  $\mathcal{V}_{[B \circ D]} \cap \mathcal{V}_{P'} = \emptyset$ , and that  $R_{i-1}$  has  $[(A \bullet B) \circ (C \bullet D) \circ (A_2 \bullet B_2)]$  as subterm. But then  $R_{i-1}$  is also nested. Contradiction. Now we define  $R'_i = R_i|_{P'}$  for all  $0 \leq i \leq n$ . We are going to show that  $R'_i \approx R'_{i+1}$  or  $R'_i \xrightarrow{M} R'_{i+1}$  for all  $0 \leq i \leq n$ . We have  $R_i \xrightarrow{M} R_{i+1}$ . Hence,  $R_i$  has a subterm  $[(A \bullet B) \circ (C \bullet D)]$  which is replaced by  $([A \circ C] \bullet [B \circ D])$  in  $R_{i+1}$ . Now we proceed by way of contradiction: since  $R'_i \not\approx R'_{i+1}$  we have (without loss of generality) that  $\mathcal{V}_A \cap \mathcal{V}_{P'} \neq \emptyset$  and  $\mathcal{V}_D \cap \mathcal{V}_{P'} \neq \emptyset$ . Since additionally  $R'_i \xrightarrow{M} R'_{i+1}$ , we must have  $\mathcal{V}_A \cap \mathcal{V}_{P'} = \emptyset$  or  $\mathcal{V}_C \cap \mathcal{V}_{P'} = \emptyset$ . Hence  $R_i$  is nested, which is a contradiction. Now the first statement of the lemma follows by an induction on  $n$ . The second statement is shown analogously.  $\square$

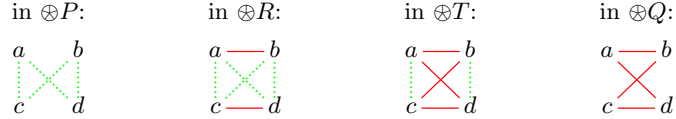
**5.3 Lemma** *Let  $P$  and  $Q$  be terms with  $P \blacktriangleleft Q$ . If  $P'$  is a subterm of  $P$ , then  $P' \blacktriangleleft Q|_{P'}$ . And if  $Q_1$  is a subterm of  $Q$ , then  $P|_{Q_1} \blacktriangleleft Q_1$ .*

**Proof:** For proving the first statement, let  $Q' = Q|_{P'}$ . We have  $\mathcal{V}_{P'} = \mathcal{V}_{Q'}$  and  $\mathcal{E}_{P'}^\bullet \subseteq \mathcal{E}_{Q'}^\bullet$ . Now let  $a, d \in \mathcal{V}_{P'}$  with  $a \overset{\circ}{\underset{P'}{\rhd}} d$  and  $a \overset{\bullet}{\underset{Q'}{\rhd}} d$ . Then we also have  $a \overset{\circ}{\underset{P}{\rhd}} d$

and  $a \overset{\bullet}{\underset{Q}{\curvearrowright}} d$ , and therefore we have  $b, c \in \mathcal{V}_P$  such that (11). In order to complete the proof of the lemma, we need to show that  $b, c \in \mathcal{V}_{P'}$ . By way of contradiction, assume that  $b$  occurs in the context of  $P'$ . Then  $b$  has the same first common ancestor with  $a$  and  $d$  in  $P$ . Hence, the edges  $(a, b)$  and  $(d, b)$  have the same color in  $\otimes P$ . Contradiction. The second statement is shown analogously.  $\square$

**5.4 Remark** It is important to observe that it is crucial for both lemmas that  $P'$  is a subterm of  $P$  (or that  $Q_1$  is a subterm of  $Q$ ). If we just have  $P \blacktriangleleft Q$  (resp.  $P \xrightarrow[M]{*} Q$ ) and a subset  $\mathcal{W} \subseteq \mathcal{V}_P$ , then in general we do *not* have that  $P|_{\mathcal{W}} \blacktriangleleft Q|_{\mathcal{W}}$  (resp.  $P|_{\mathcal{W}} \xrightarrow[M]{*} Q|_{\mathcal{W}}$ ). A simple example is given by  $P = [(a \bullet b) \circ (c \bullet d)]$  and  $Q = ([a \circ c] \bullet [b \circ d])$  and  $\mathcal{W} = \{a, b, d\}$ . Then  $P|_{\mathcal{W}} = [(a \bullet b) \circ d]$  and  $Q|_{\mathcal{W}} = (a \bullet [b \circ d])$ . We clearly have  $P \blacktriangleleft Q$  (resp.  $P \xrightarrow[M]{*} Q$ ) but not  $P|_{\mathcal{W}} \blacktriangleleft Q|_{\mathcal{W}}$  (resp.  $P|_{\mathcal{W}} \xrightarrow[M]{*} Q|_{\mathcal{W}}$ ).

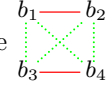
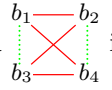
**Proof of Theorem 5.1:** First, assume we have  $P \xrightarrow[M]{*} Q$ . Then there is an  $n \geq 0$  with  $P \xrightarrow[M]{n} Q$ . Obviously, we have  $\mathcal{V}_P = \mathcal{V}_Q$  and  $\mathcal{E}_P^\bullet \subseteq \mathcal{E}_Q^\bullet$ . Hence Conditions (i) and (ii) are satisfied. For proving Condition (iii), we proceed by induction on  $n$ . For  $n = 0$  this is trivial. Now let  $n \geq 1$ , and assume we have  $a$  and  $d$  with  $a \overset{\circ}{\underset{P}{\curvearrowright}} d$  and  $a \overset{\bullet}{\underset{Q}{\curvearrowright}} d$ . Then there are terms  $R$  and  $T$  such that  $P \xrightarrow[M]{*} R \xrightarrow[M]{*} T \xrightarrow[M]{*} Q$  and  $a \overset{\circ}{\underset{R}{\curvearrowright}} d$  and  $a \overset{\bullet}{\underset{T}{\curvearrowright}} d$ . Because of Proposition 4.1, we can assume without loss of generality that  $R$  has a subterm  $[(A \bullet B) \circ (C \bullet D)]$ , which is in  $T$  replaced by  $([A \circ C] \bullet [B \circ D])$ . We can without loss of generality assume that  $a \in \mathcal{V}_A$  and  $d \in \mathcal{V}_D$ . Then we have for all  $b \in \mathcal{V}_B$  and  $c \in \mathcal{V}_C$  the following configurations:

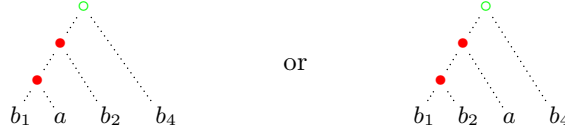


We will now show that there is a  $b \in \mathcal{V}_B$  with  $a \overset{\bullet}{\underset{P}{\curvearrowright}} b$  and  $b \overset{\circ}{\underset{Q}{\curvearrowright}} d$ . For this, we need an auxiliary definition. For a term  $S$  and a constant  $a \in \mathcal{V}_S$  we define a partial order  $\overset{a}{\underset{S}{\curvearrowright}}$  on the set  $\mathcal{V}_S$  as follows:  $b_1 \overset{a}{\underset{S}{\curvearrowright}} b_2$  iff the first common ancestor of  $a$  and  $b_2$  in the term tree of  $S$  is also an ancestor of  $b_1$ . For example, in (8) we have  $b \overset{c}{\underset{P}{\curvearrowright}} e$ , and  $d, e$  are incomparable wrt.  $\overset{c}{\underset{P}{\curvearrowright}}$ . Now pick  $b_1 \in \mathcal{V}_B$  which is minimal wrt.  $\overset{a}{\underset{P}{\curvearrowright}}$ . We claim that  $a \overset{\bullet}{\underset{P}{\curvearrowright}} b_1$ . By way of contradiction, assume  $a \overset{\circ}{\underset{P}{\curvearrowright}} b_1$ . Then we apply the induction hypothesis to  $P \xrightarrow[M]{*} R$ , which gives us  $a'$  and  $b'$  with

configurations in  $\otimes P$  and in  $\otimes R$ . It follows (cf. the proof of

Lemma 5.3) that  $b' \in \mathcal{V}_B$  and that  $b' \overset{a}{\underset{P}{\curvearrowright}} b_1$ , contradicting the minimality of  $b_1$ . If  $b_1 \overset{\circ}{\underset{Q}{\curvearrowright}} d$ , then we have found our desired  $b$ . So, assume  $b_1 \overset{\bullet}{\underset{Q}{\curvearrowright}} d$ , and pick a  $b_4 \in \mathcal{V}_B$  which is minimal wrt.  $\overset{d}{\underset{Q}{\curvearrowright}}$ . With a similar argument as above, we can show that

$b_4 \overset{\circ}{Q} d$ . If  $a \overset{\bullet}{P} b_4$ , then, as before, we have our  $b$ . So, let us assume that  $a \overset{\circ}{P} b_4$ . Since we also have that  $b_1 \overset{a}{P} b_4$  and  $b_4 \overset{d}{Q} b_1$ , it follows that  $b_1 \overset{\circ}{P} b_4$  and  $b_1 \overset{\bullet}{Q} b_4$ . By Lemma 5.2 we have  $P|_B \xrightarrow{*} B \xrightarrow{*} Q|_B$ . Now we can apply the induction hypothesis to  $P|_B \xrightarrow{*} Q|_B$  and get  $b_2, b_3 \in \mathcal{V}_B$  such that we have  in  $\otimes P|_B$  and  in  $\otimes Q|_B$ . Note that  $b_2, b_3 \in \mathcal{V}_B$  and that  $b_2 \overset{b_1}{P} b_4$ . Hence, in the term tree for  $P$ , we have one of the following situations:



In both cases  $a \overset{\bullet}{P} b_2$ . Similarly, it follows that  $b_2 \overset{\circ}{Q} d$ . With a similar argumentation, we can find  $c_2 \in \mathcal{V}_C$  with  $c_2 \overset{\bullet}{P} d$  and  $a \overset{\circ}{Q} c_2$ . Hence, Condition (iii) is fulfilled, and we have  $P \blacktriangleleft Q$ .

Conversely, assume we have  $P \blacktriangleleft Q$ . We proceed by induction on the cardinality of  $\mathcal{V}_P$ , to show that  $P \xrightarrow{*} Q$ . The base case, where  $\mathcal{V}_P$  is a singleton, is trivial. Now we make a case analysis on the term structure of  $P$  and  $Q$ .

1.  $P = [P' \circ P'']$  and  $Q = [Q_1 \circ Q_2]$ . We define the following four sets:

$$\mathcal{V}'_1 = \mathcal{V}_{P'} \cap \mathcal{V}_{Q_1}, \quad \mathcal{V}'_2 = \mathcal{V}_{P'} \cap \mathcal{V}_{Q_2}, \quad \mathcal{V}''_1 = \mathcal{V}_{P''} \cap \mathcal{V}_{Q_1}, \quad \mathcal{V}''_2 = \mathcal{V}_{P''} \cap \mathcal{V}_{Q_2}.$$

First, note that we cannot have that one of  $\mathcal{V}'_1$  and  $\mathcal{V}'_2$  is empty, and at the same time that one of  $\mathcal{V}''_1$  and  $\mathcal{V}''_2$  is empty because then one of  $\mathcal{V}_{P'}, \mathcal{V}_{P''}, \mathcal{V}_{Q_1}, \mathcal{V}_{Q_2}$  would be empty, which is impossible. The remaining two possibilities of two empty sets are:

- If  $\mathcal{V}'_2 = \emptyset$  and  $\mathcal{V}''_1 = \emptyset$ , then  $\mathcal{V}_{P'} = \mathcal{V}_{Q_1}$  and  $\mathcal{V}_{P''} = \mathcal{V}_{Q_2}$ . Hence, by Lemma 5.3 we have  $P' \blacktriangleleft Q_1$  and  $P'' \blacktriangleleft Q_2$ . By induction hypothesis we have therefore

$$P = [P' \circ P''] \xrightarrow{*} [Q_1 \circ P''] \xrightarrow{*} [Q_1 \circ Q_2] = Q$$

- If  $\mathcal{V}'_1 = \emptyset$  and  $\mathcal{V}''_2 = \emptyset$ , then  $\mathcal{V}_{P'} = \mathcal{V}_{Q_2}$  and  $\mathcal{V}_{P''} = \mathcal{V}_{Q_1}$ , and we proceed similarly.

Let us now assume that one of the four sets is empty, say  $\mathcal{V}'_1 = \emptyset$ . We let

$$P'_2 = P'|_{Q_2}, \quad P''_1 = P''|_{Q_1}, \quad P''_2 = P''|_{Q_2}.$$

Then  $P'_2 = P'$  and  $P'' \approx [P''_1 \circ P''_2]$  because  $\mathcal{E}_Q^\circ \subseteq \mathcal{E}_P^\circ$ . By Lemma 5.3 we have  $P''_1 \blacktriangleleft Q_1$  and  $[P'_2 \circ P''_2] \blacktriangleleft Q_2$ . Hence, by induction hypothesis we have

$$P \approx [P'_2 \circ [P''_1 \circ P''_2]] \approx [P''_1 \circ [P'_2 \circ P''_2]] \xrightarrow{*} [Q_1 \circ [P'_2 \circ P''_2]] \xrightarrow{*} [Q_1 \circ Q_2] = Q$$

If one of  $\mathcal{V}'_2, \mathcal{V}''_1, \mathcal{V}''_2$  is empty, we can proceed analogously. Let us now consider the case where none of  $\mathcal{V}'_1, \mathcal{V}'_2, \mathcal{V}''_1, \mathcal{V}''_2$  is empty. Then we can define

$$P'_1 = P'|_{Q_1}, \quad P'_2 = P'|_{Q_2}, \quad P''_1 = P''|_{Q_1}, \quad P''_2 = P''|_{Q_2}.$$

We have  $P' \approx [P'_1 \circ P'_2]$  and  $P'' \approx [P''_1 \circ P''_2]$ . By Lemma 5.3 we have  $[P'_1 \circ P'_1] \blacktriangleleft Q_1$  and  $[P'_2 \circ P'_2] \blacktriangleleft Q_2$ . Hence, by induction hypothesis:

$$P \approx [[P'_1 \circ P'_2] \circ [P''_1 \circ P''_2]] \approx [[P'_1 \circ P'_1] \circ [P'_2 \circ P'_2]] \xrightarrow{*}_M [Q_1 \circ Q_2] = Q$$

2.  $P = (P' \bullet P'')$  and  $Q = (Q_1 \bullet Q_2)$ . This is analogous to the previous case.
3.  $P = (P' \bullet P'')$  and  $Q = [Q_1 \circ Q_2]$ . As before, we let

$$\mathcal{V}'_1 = \mathcal{V}_{P'} \cap \mathcal{V}_{Q_1}, \mathcal{V}'_2 = \mathcal{V}_{P'} \cap \mathcal{V}_{Q_2}, \mathcal{V}''_1 = \mathcal{V}_{P''} \cap \mathcal{V}_{Q_1}, \mathcal{V}''_2 = \mathcal{V}_{P''} \cap \mathcal{V}_{Q_2}.$$

Note that if  $\mathcal{V}'_1 \neq \emptyset$  and  $\mathcal{V}'_2 \neq \emptyset$  then we have immediately a contradiction to Condition (ii), and similarly if  $\mathcal{V}''_2 \neq \emptyset$  and  $\mathcal{V}''_1 \neq \emptyset$ . Hence, one of  $\mathcal{V}'_1$  and  $\mathcal{V}'_2$  must be empty, and one of  $\mathcal{V}''_2$  and  $\mathcal{V}''_1$  must be empty. But this is impossible as observed in Case 1 above.

4.  $P = [P' \circ P'']$  and  $Q = (Q_1 \bullet Q_2)$ . This is the most interesting case. As before, we let

$$\mathcal{V}'_1 = \mathcal{V}_{P'} \cap \mathcal{V}_{Q_1}, \mathcal{V}'_2 = \mathcal{V}_{P'} \cap \mathcal{V}_{Q_2}, \mathcal{V}''_1 = \mathcal{V}_{P''} \cap \mathcal{V}_{Q_1}, \mathcal{V}''_2 = \mathcal{V}_{P''} \cap \mathcal{V}_{Q_2}.$$

We first show that none of the sets  $\mathcal{V}'_1, \mathcal{V}''_1, \mathcal{V}'_2, \mathcal{V}''_2$  is empty. So, assume by way of contradiction, that  $\mathcal{V}''_1 = \emptyset$ . By a similar argumentation as before it follows that  $\mathcal{V}'_1 \neq \emptyset$  and  $\mathcal{V}''_2 \neq \emptyset$ . So, pick  $a \in \mathcal{V}'_1$  and  $d \in \mathcal{V}''_2$ . We have  $a \overset{\circ}{\underset{P}{\blacktriangleleft}} d$  and  $a \overset{\bullet}{\underset{Q}{\blacktriangleleft}} d$ . Since  $P \blacktriangleleft Q$ , we have  $b, c \in \mathcal{V}_P$  such that (11). Because  $c \overset{\bullet}{\underset{P}{\blacktriangleleft}} d$  we must have that  $c \in \mathcal{V}_{P''}$ , and because of  $a \overset{\circ}{\underset{Q}{\blacktriangleleft}} c$ , we must have that  $c \in \mathcal{V}_{Q_1}$ . Hence  $c \in \mathcal{V}''_1$ . Contradiction. We can therefore define:

$$P'_1 = P'|_{Q_1}, \quad P'_2 = P'|_{Q_2}, \quad P''_1 = P''|_{Q_1}, \quad P''_2 = P''|_{Q_2},$$

and

$$Q'_1 = Q_1|_{P'}, \quad Q'_2 = Q_2|_{P'}, \quad Q''_1 = Q_1|_{P''}, \quad Q''_2 = Q_2|_{P''}.$$

We now want to show that  $P'_1 \blacktriangleleft Q'_1$ . But by Remark 5.4 we cannot apply Lemma 5.3. However, we have  $\mathcal{V}_{P'_1} = \mathcal{V}_{Q'_1}$  and  $\mathcal{E}_{P'_1} \subseteq \mathcal{E}_{Q'_1}$ . Now let  $a, d \in \mathcal{V}_{P'_1}$  with  $a \overset{\circ}{\underset{P'_1}{\blacktriangleleft}} d$  and  $a \overset{\bullet}{\underset{Q'_1}{\blacktriangleleft}} d$ . Hence, we have  $a \overset{\circ}{\underset{P}{\blacktriangleleft}} d$  and  $a \overset{\bullet}{\underset{Q}{\blacktriangleleft}} d$ . Since  $P \blacktriangleleft Q$ , we have  $b, c \in \mathcal{V}_P$  such that (11). Note that because  $a, d \in \mathcal{V}_{P'}$ , we also have  $b \in \mathcal{V}_{P'}$  (otherwise we would have  $a \overset{\circ}{\underset{P}{\blacktriangleleft}} b$ ) and  $c \in \mathcal{V}_{P'}$  (otherwise we would have  $c \overset{\circ}{\underset{P}{\blacktriangleleft}} d$ ). Similarly, because  $a, d \in \mathcal{V}_{Q_1}$ , we also have  $b, c \in \mathcal{V}_{Q_1}$  (otherwise we would have  $a \overset{\bullet}{\underset{Q}{\blacktriangleleft}} c$  and  $b \overset{\bullet}{\underset{Q}{\blacktriangleleft}} d$ , respectively). Hence  $b, c \in \mathcal{V}_{P'_1}$ , and therefore  $P'_1 \blacktriangleleft Q'_1$ . Similarly, we get  $P''_1 \blacktriangleleft Q''_1$  and  $P'_2 \blacktriangleleft Q'_2$  and  $P''_2 \blacktriangleleft Q''_2$ . Hence, we have by induction hypothesis

$$P'_1 \xrightarrow{*}_M Q'_1, \quad P''_1 \xrightarrow{*}_M Q''_1, \quad P'_2 \xrightarrow{*}_M Q'_2, \quad P''_2 \xrightarrow{*}_M Q''_2. \quad (12)$$

Now let  $P'_{12} = (P'_1 \bullet P'_2)$ . We clearly have  $\mathcal{V}_{P'} = \mathcal{V}_{P'_{12}}$  and  $\mathcal{E}_{P'} \subseteq \mathcal{E}_{P'_{12}}$ . Now let us assume we have  $a, d \in \mathcal{V}_{P'}$  with  $a \overset{\circ}{\underset{P'}{\blacktriangleleft}} d$  and  $a \overset{\bullet}{\underset{P'_{12}}{\blacktriangleleft}} d$ . Then we must have  $a \in \mathcal{V}_{P'_1}$  and  $d \in \mathcal{V}_{P'_2}$ , or vice versa (otherwise the two edges would have the same color in  $P'$  and  $P'_{12}$ ). Hence, we have  $a \overset{\circ}{\underset{P}{\blacktriangleleft}} d$  and  $a \overset{\bullet}{\underset{Q}{\blacktriangleleft}} d$ . Since  $P \blacktriangleleft Q$ , we have  $b, c \in \mathcal{V}_Q$  such that (11). Note that because  $a, d \in \mathcal{V}_{P'}$ , we also have  $b, c \in \mathcal{V}_{P'}$  (otherwise we would have  $a \overset{\circ}{\underset{P}{\blacktriangleleft}} b$  and  $d \overset{\circ}{\underset{P}{\blacktriangleleft}} c$ ). This means we have in



$\otimes P'$  the configuration  $\begin{array}{c} a \text{---} b \\ \diagup \quad \diagdown \\ c \text{---} d \end{array}$ . Since we have  $a \overset{\circ}{Q} c$  and  $b \overset{\circ}{Q} d$ , we must also have  $a \overset{\circ}{P_{12}} c$  and  $b \overset{\circ}{P_{12}} d$ . And since we have  $a \overset{\bullet}{P} b$  and  $c \overset{\bullet}{P} d$ , we also have  $a \overset{\bullet}{P_{12}} b$  and  $c \overset{\bullet}{P_{12}} d$ . Furthermore, we have  $a \overset{\bullet}{P_{12}} d$  (because  $a \in \mathcal{V}_{P_1}$  and  $d \in \mathcal{V}_{P_2}$ ).

Hence, we have in  $\otimes P'_{12}$  the configuration  $\begin{array}{c} a \text{---} b \\ \diagup \quad \diagdown \\ c \text{---} d \end{array}$ . By Proposition 4.2, we must have  $\begin{array}{c} a \text{---} b \\ \diagdown \quad \diagup \\ c \text{---} d \end{array}$ . Hence,  $P' \blacktriangleleft (P_1 \bullet P_2)$ . By the same argumentation, we get  $P'' \blacktriangleleft (P_1' \bullet P_2')$  and  $[Q_1' \circ Q_1''] \blacktriangleleft Q_1$  and  $[Q_2' \circ Q_2''] \blacktriangleleft Q_2$ . By induction hypothesis we have therefore

$$\begin{array}{ccc} P' \xrightarrow[M]{*} (P_1 \bullet P_2) & [Q_1' \circ Q_1''] \xrightarrow[M]{*} Q_1 & \\ P'' \xrightarrow[M]{*} (P_1' \bullet P_2') & [Q_2' \circ Q_2''] \xrightarrow[M]{*} Q_2 & \end{array} \quad (13)$$

Now we can combine (12) and (13) to get

$$\begin{aligned} [P' \circ P''] \xrightarrow[M]{*} [(P_1 \bullet P_2) \circ (P_1' \bullet P_2')] & \xrightarrow[M]{*} [(P_1 \circ P_1') \bullet (P_2 \circ P_2')] \\ & \xrightarrow[M]{*} ([Q_1' \circ Q_1''] \bullet [Q_2' \circ Q_2'']) \xrightarrow[M]{*} (Q_1 \bullet Q_2) \end{aligned}$$

In other words:  $P \xrightarrow[M]{*} Q$ .  $\square$

**5.5 Corollary** *The relation  $\blacktriangleleft \subseteq \mathcal{T} \times \mathcal{T}$  is transitive.*

## 6 Related results

Let us compare our result to the one in [BdGR97], where one of the two binary operations was not commutative but only associative. Although this has some consequences for the characterization of relation webs (Proposition 4.2), the consequences for the main result (Theorem 5.1) are only cosmetic. For this reason let us recall here the commutative version of the results in [BdGR97]. Let  $P$  be the rewriting system

$$\begin{aligned} ([x \circ y] \bullet [w \circ z]) & \rightarrow [(x \bullet w) \circ (y \bullet z)] \\ (x \bullet [y \circ z]) & \rightarrow [(x \bullet y) \circ z] \\ (x \bullet y) & \rightarrow [x \circ y] \end{aligned} \quad (14)$$

Note that it is *not* a typo that the first rewrite rule is the inversion of medial. Analogous to  $\xrightarrow[M]{*}$ , we define  $\xrightarrow[P]{*}$  to be the transitive closure of the rewriting relation via (14) modulo AC. The result of [BdGR97] can be stated as follows:

**6.1 Theorem** *For terms  $P, Q$  we have  $P \xrightarrow[P]{*} Q$  iff  $\mathcal{V}_P = \mathcal{V}_Q$  and  $\mathcal{E}_P^\circ \subseteq \mathcal{E}_Q^\circ$ .*

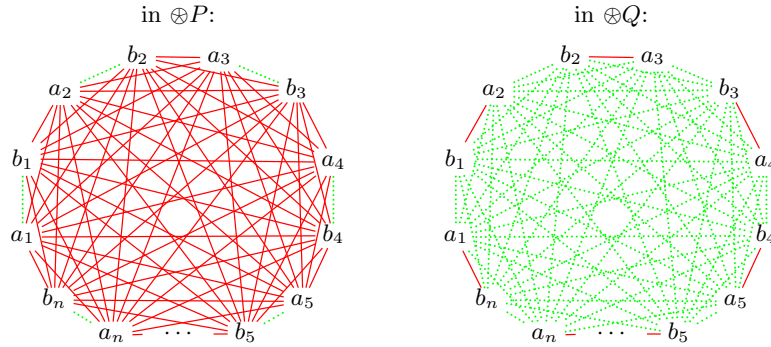
In other words, the main difference to Theorem 5.1 is that the Condition (iii) is absent in [BdGR97]. Let us now look at the case where we remove the first rule from  $P$ . Let  $S$  be the rewrite system

$$\begin{aligned} (x \bullet [y \circ z]) & \rightarrow [(x \bullet y) \circ z] \\ (x \bullet y) & \rightarrow [x \circ y] \end{aligned} \quad (15)$$

We define  $P \xrightarrow{*}_5 Q$  as above. The characterization of this relation is the following:

**6.2 Theorem** *We have  $P \xrightarrow{*}_5 Q$  if and only if  $\mathcal{V}_P = \mathcal{V}_Q$ , and for all  $n \geq 1$  and all subsets  $\mathcal{W} = \{a_1, b_1, \dots, a_n, b_n\} \subseteq \mathcal{V}_P$  we do not have that*  
 $P|_{\mathcal{W}} \approx ([a_1 \circ b_1] \bullet \dots \bullet [a_n \circ b_n])$  and  $Q|_{\mathcal{W}} \approx [(b_1 \bullet a_2) \circ (b_2 \bullet a_3) \circ \dots \circ (b_n \bullet a_1)]$

In other words, we are not allowed to have the following configurations in the relation webs of  $P$  and  $Q$ :



Note that  $\mathcal{E}_P^\circ \subseteq \mathcal{E}_Q^\circ$  follows by letting  $n = 1$ .

**6.3 Remark** This characterization is simply an alternative formulation of the correctness criterion for proof nets for multiplicative linear logic [Ret96]. For this, we have to read the  $\bullet$  as *tensor*  $\otimes$ , and the  $\circ$  as *par*  $\wp$ . Then, the rule

$$(x \otimes [y \wp z]) \rightarrow [(x \otimes y) \wp z]$$

is also called *switch* [Gug07], *weak distributivity* [BCST96], or *dissociativity* [DP04]. The rule

$$(x \otimes y) \rightarrow [x \wp y]$$

is called *mix*. The condition in Theorem 6.2 is equivalent to the acyclicity condition in proof nets [DR89].<sup>2</sup>

It is interesting to note the different nature of the three characterizations of the rewrite systems M, P, and S. This is the reason for the difficulty to give a characterization of the rewrite system MS, which combines M and S:

$$\begin{aligned} [(x \bullet y) \circ (w \bullet z)] &\rightarrow [(x \circ w) \bullet [y \circ z]] \\ (x \bullet [y \circ z]) &\rightarrow [(x \bullet y) \circ z] \\ (x \bullet y) &\rightarrow [x \circ y] \end{aligned} \tag{16}$$

<sup>2</sup> If mix is absent, then an additional condition (connectedness) would be needed. For more details on the relation between S and linear logic, see, e.g., [DHPP99, Ret93, Gug07, Str03a], and for relating the condition in Theorem 6.2 to multiplicative proof nets, see, e.g., [Ret03]. For more information on mix, see [FR94], and for a direct proof of Theorem 6.2, see, e.g., [Str03b, Str03a].

**6.4 Open Problem:** Find a characterization of the rewrite relation  $\xrightarrow[\text{MS}]{*}$  in terms of relation webs.

## 7 Application in Proof Theory

The motivation for stating the open problem concluding the previous section is the increasing importance of the relation  $\xrightarrow[\text{MS}]{*}$  for the proof theory of classical propositional logic [BT01,Lam06,Str05]. To see this, we have to read the  $\bullet$  as *conjunction*  $\wedge$  and the  $\circ$  as *disjunction*  $\vee$ .

A central ingredient to logic is the notion of duality. For dealing with this, we let the set of constant symbols come in pairs: for every  $a$  there is its dual  $\bar{a}$ . Then the terms are the formulas in negation normal form and the constants are the literals. If a formula  $I$  is of the shape

$$([a_1 \circ \bar{a}_1] \bullet [a_2 \circ \bar{a}_2] \bullet \cdots \bullet [a_n \circ \bar{a}_n])$$

for some  $n \geq 1$  and constants  $a_1, a_2, \dots, a_n$ , then we say  $I$  is an *initial formula*.

It is well-known that classical logic is multiplicative linear logic plus contraction and weakening. Let us therefore introduce two more rewrite systems. Let  $W$  be the rewrite system containing only the rule

$$x \rightarrow [x \circ y] \tag{17}$$

and let  $C$  be the system containing only the rule

$$[x \circ x] \rightarrow x \tag{18}$$

Now let  $K1 = S \cup W \cup C$ . Then we have the following theorem, which says that a proof in classical logic is a rewrite path in  $K1$ .

**7.1 Theorem** *A formula  $Q$  is a Boolean tautology if and only if there is an initial formula  $I$  with  $I \xrightarrow[\text{K1}]{*} Q$ . [BT01]*

As already mentioned in Section 2, we can with medial reduce contraction to literals. Let  $C'$  be the rewrite system consisting of a rule

$$[a \circ a] \rightarrow a \tag{19}$$

for every constant symbol (including their duals). If we let  $K2 = MS \cup W \cup C'$ , then we have

**7.2 Theorem** *Let  $P$  and  $Q$  be formulas. Then  $P \xrightarrow[\text{K1}]{*} Q$  iff  $P \xrightarrow[\text{K2}]{*} Q$ . [BT01]*

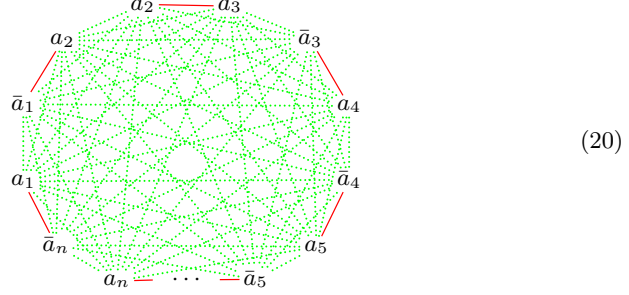
While [BT01] and related work (e.g., [GS01,Gug07,Brü03,Str03a]) are mainly concerned with the syntactic manipulation of terms/formulas, Hughes proposes in [Hug06] the notion of *combinatorial proof*, which is based on a variant of Theorem 6.2 and the notion of *skew fibration*: Given two prewebs  $\mathcal{G}_1 = \langle \mathcal{V}_1; \mathcal{E}_1^\bullet, \mathcal{E}_1^\circ \rangle$  and  $\mathcal{G}_2 = \langle \mathcal{V}_2; \mathcal{E}_2^\bullet, \mathcal{E}_2^\circ \rangle$ , then a skew fibration  $h: \mathcal{G}_1 \rightarrow \mathcal{G}_2$  is a mapping  $\mathcal{V}_1 \rightarrow \mathcal{V}_2$  such that

- (a)  $(a, b) \in \mathcal{E}_1^\bullet$  implies  $(h(a), h(b)) \in \mathcal{E}_2^\bullet$  (i.e.,  $h$  is a graph homomorphism for the red edges), and

- (b) for all  $a \in \mathcal{V}_1$  and  $d \in \mathcal{V}_2$ , if  $(h(a), d) \in \mathcal{E}_2^\bullet$ , then there is a  $b \in \mathcal{V}_1$  with  $(a, b) \in \mathcal{E}_1^\bullet$  and  $(h(b), d) \notin \mathcal{E}_2^\bullet$ .

A *combinatorial proof* of a Boolean formula  $Q$  is a skew fibration  $h: \otimes P \rightarrow \otimes Q$  for a formula  $P$  such that

- (c)  $\otimes P$  does not contain a configuration

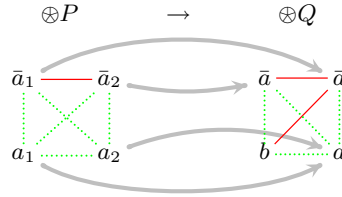


- for any  $n \geq 1$  and constants  $a_1, a_2, \dots, a_n$ , and
- (d)  $h$  maps only non-negated constants to non-negated constants and negated constants to negated ones.

**7.3 Theorem** *A formula  $Q$  is a Boolean tautology, if and only if it has a combinatorial proof.* [Hug06]

**7.4 Remark** Note that for Theorems 7.1 and 7.3 to make sense, we have to allow more than one occurrence of a constant in a formula. This means that in the relation web  $\otimes P$  of a formula  $P$ , the set  $\mathcal{V}_P$  is the set of constant occurrences. Then we can call a map  $h: \mathcal{V}_P \rightarrow \mathcal{V}_Q$  *label preserving* if the name of a constant is not changed by  $h$ .

To give an example, we show here the combinatorial proof of Pierce's law  $Q = [([\bar{a} \vee b] \wedge \bar{a}) \vee a]$ , taken from [Hug06]. We let  $P = [(\bar{a}_1 \wedge \bar{a}_2) \vee a_1 \vee a_2]$ . The skew fibration  $h: \otimes P \rightarrow \otimes Q$  is given as follows:



**7.5 Theorem** *Let  $P$  and  $Q$  be formulas. Then  $P \triangleleft Q$  if and only if  $\mathcal{V}_P = \mathcal{V}_Q$  and the identity function on  $\mathcal{V}_P$  is a skew fibration  $\otimes P \rightarrow \otimes Q$ .*

**Proof:** First, assume  $P \triangleleft Q$ . Since  $\mathcal{E}_P^\bullet \subseteq \mathcal{E}_Q^\bullet$ , Condition (a) above is fulfilled. Now let  $a, d \in \mathcal{V}_P$  with  $a \overset{\bullet}{\triangleleft} d$ . If  $a \overset{\bullet}{\triangleleft} d$ , then we let  $b = d$  and we are done. If  $a \overset{\circ}{\triangleleft} d$ , then we have  $b, c \in \mathcal{V}_P$  with (11). Now  $b$  has the desired properties. Conversely, assume that  $\mathcal{V}_P = \mathcal{V}_Q$  and the identity  $\mathcal{V}_P \rightarrow \mathcal{V}_Q$  is a skew fibration.

By (a) we have  $\mathcal{E}_P^\bullet \subseteq \mathcal{E}_Q^\bullet$ . Now let  $a, d \in \mathcal{V}_P$  with  $a \overset{\circ}{\underset{P}{\frown}} d$  and  $a \overset{\bullet}{\underset{Q}{\frown}} d$ . Then by (b) there is a  $b \in \mathcal{V}_P$  with  $a \overset{\bullet}{\underset{P}{\frown}} b$  and  $b \overset{\circ}{\underset{Q}{\frown}} d$ . Since  $\mathcal{E}_P^\bullet \subseteq \mathcal{E}_Q^\bullet$ , we also have  $a \overset{\bullet}{\underset{Q}{\frown}} b$  and  $b \overset{\circ}{\underset{P}{\frown}} d$ . By exchanging the roles of  $a$  and  $d$  and applying (b) again, we get  $c \in \mathcal{V}_P$  with  $d \overset{\bullet}{\underset{P}{\frown}} c$  and  $c \overset{\circ}{\underset{Q}{\frown}} a$ . Since  $\mathcal{E}_P^\bullet \subseteq \mathcal{E}_Q^\bullet$ , it follows that  $d \overset{\bullet}{\underset{Q}{\frown}} c$  and  $c \overset{\circ}{\underset{P}{\frown}} a$ . Hence  $c \neq b$ . By Proposition 4.2, we conclude that  $b \overset{\circ}{\underset{P}{\frown}} c$  and  $b \overset{\bullet}{\underset{Q}{\frown}} c$ .  $\square$

In the following, we establish a precise relation between the notion of proof as rewriting path (in a deep inference deductive system) and the notion of proof as a combinatorial object using relation webs and skew fibrations. For this, we first have to characterize the rewrite systems  $\mathbb{W}$  and  $\mathbb{C}'$ . Let  $P$  and  $Q$  be formulas. A map  $w: \otimes P \rightarrow \otimes Q$  is called a *weakening*, if

- (e)  $w$  is an injective skew fibration, and
- (f) for all  $a, b \in \mathcal{V}_P$ , we have  $a \overset{\bullet}{\underset{P}{\frown}} b$  iff  $w(a) \overset{\bullet}{\underset{Q}{\frown}} w(b)$ .

A map  $c: \otimes P \rightarrow \otimes Q$  is called an *atomic contraction*, if

- (g)  $c$  is surjective, and
- (h) for all  $a, b \in \mathcal{V}_P$ , we have  $a \overset{\bullet}{\underset{P}{\frown}} b$  iff  $c(a) \overset{\bullet}{\underset{Q}{\frown}} c(b)$ .

Note that it follows that  $c$  is a skew fibration. We have the following:

**7.6 Proposition** *For all formulas  $P$  and  $Q$ ,*

1.  $P \xrightarrow[\mathbb{W}]{*} Q$  iff there is a label preserving weakening  $w: \otimes P \rightarrow \otimes Q$ .
2.  $P \xrightarrow[\mathbb{C}']{*} Q$  iff there is a label preserving atomic contraction  $c: \otimes P \rightarrow \otimes Q$ .

**Proof:** The “only if” direction is trivial for both statements. The “if” direction for the first statement follows by observing that condition (b) implies that for all  $d$  not in the image of  $w$  there is in  $Q$  a subformula  $D$  containing only material (including  $d$ ) not appearing in  $P$ , and a subformula  $B$  containing only material (including  $b$ ) appearing in  $P$ , such that  $[B \circ D]$  is also a subformula of  $Q$ . Injectivity and Condition (f) ensure that  $B$  is also a subformula of  $P$ . Hence, we can rewrite  $B$  into  $[B \circ D]$ . For the second statement it suffices to note that whenever two occurrences of a constant  $a$  in  $P$  are mapped onto the same occurrence in  $Q$ , then they must appear as subformula  $[a \circ a]$  in  $P$ .  $\square$

**7.7 Lemma** *A label preserving skew fibration  $h: \mathcal{V}_P \rightarrow \mathcal{V}_Q$  is surjective if and only if there is a formula  $R$  with  $\mathcal{V}_R = \mathcal{V}_P$  such that  $P \blacktriangleleft R$  and  $h$  is an atomic contraction when seen as map  $\otimes R \rightarrow \otimes Q$ .*

**Proof:** Let  $h$  be surjective. We construct  $R$  from  $Q$  by replacing each constant occurrence  $a$  by  $[a \circ \dots \circ a]$  where the number of  $a$ 's is the cardinality of the preimage  $h^{-1}(a)$  in  $P$ . Then obviously the canonical map  $\mathcal{V}_R \rightarrow \mathcal{V}_Q$  is an atomic contraction, and the identity map  $\mathcal{V}_P \rightarrow \mathcal{V}_R$  inherits from  $h$  the property of being a skew fibration. Finally we apply Theorem 7.5. The converse follows from the fact that the composition of a skew fibration with an atomic contraction is again a skew fibration.<sup>3</sup>  $\square$

<sup>3</sup> An anonymous referee pointed out that it is in general not true that the composition of two skew fibrations is again a skew fibration because they are defined on prewebs.

Now we can put everything together to give a combinatorial proof for the following theorem:

**7.8 Theorem** *A formula  $Q$  is a Boolean tautology if and only if there is an initial formula  $I$ , such that  $I \xrightarrow{S} P \xrightarrow{M} R \xrightarrow{C'} S \xrightarrow{W} Q$  for some formulas  $P$ ,  $R$ , and  $S$ .*

**Proof:** The “if” direction follows immediately from Theorems 7.1 and 7.2. For the “only if” direction we start with the combinatorial proof for  $Q$  given by Theorem 7.3. We have a skew fibration  $h: \otimes P \rightarrow \otimes Q$ . By Theorem 6.2 and Condition (c) we can obtain an initial formula  $I$  with  $I \xrightarrow{S} P$ . Now we let  $\mathcal{V}_S \subseteq \mathcal{V}_Q$  be the image of  $h: \mathcal{V}_P \rightarrow \mathcal{V}_Q$ , and let  $S = Q|_{\mathcal{V}_S}$ . This gives us a surjective skew fibration  $h': \otimes P \rightarrow \otimes S$ . We can rename in  $P$  (and in  $I$ ) all appearing constants such that  $h'$  becomes label preserving. Then we apply Lemma 7.7 to get  $R$ . By Theorem 5.1 we have  $P \xrightarrow{M} R$ , and by Proposition 7.6.2 we have  $R \xrightarrow{C'} S$ . Finally, note that the embedding  $\otimes S \rightarrow \otimes Q$  is a weakening. So, by Proposition 7.6.1 we get  $S \xrightarrow{W} Q$ .  $\square$

**7.9 Remark** The proof of Theorem 7.8, together with the rule permutation results in the calculus of structures [Brü03] can be used to show that skew fibrations are closed under composition when their definition is restricted to relation webs (cf. Footnote 3).

## 8 Conclusions and future work

We have shown a combinatorial criterion for characterizing rewriting via medial modulo associativity and commutativity. This has been used for giving a combinatorial proof to a proof theoretic statement. So far, statements as in Theorem 7.8, also called *decomposition theorems* [Str03b, Brü03], have been proved via tedious permutations of inference rules in the calculus of structures. An interesting question for future research is whether these proofs can be simplified in general via a combinatorial analysis as carried out in this paper.

A second line of research is in the area of coherence problems in category theory. There, the question is not the existence of rewriting paths, but the identity of rewriting paths. Some investigation in this direction for rewriting via  $M$  can be found in [DP07]. For the system  $MS$ , see [Lam06], and for all of  $K1$  and/or  $K2$ , see [Str05].

## References

- [BCST96] Richard Blute, Robin Cockett, Robert Seely, and Todd Trimble. Natural deduction and coherence for weakly distributive categories. *Journal of Pure and Applied Algebra*, 113:229–296, 1996.
- [BN98] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

- [BdGR97] Denis Bechet, Philippe de Groote, and Christian Retoré. A complete axiomatisation of the inclusion of series-parallel partial orders. In *RTA 1997*, volume 1232 of *LNCS*, pages 230–240. Springer-Verlag, 1997.
- [Brü03] Kai Brünnler. *Deep Inference and Symmetry for Classical Proofs*. PhD thesis, Technische Universität Dresden, 2003.
- [BT01] Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In R. Nieuwenhuis and A. Voronkov, editors, *LPAR 2001*, volume 2250 of *LNAI*, pages 347–361. Springer-Verlag, 2001.
- [DG04] Pietro Di Gianantonio. Structures for multiplicative cyclic linear logic: Deepness vs cyclicity. In J. Marcinkowski and A. Tarlecki, editors, *CSL 2004*, volume 3210 of *LNCS*, pages 130–144. Springer-Verlag, 2004.
- [DHPP99] H. Devarajan, Dominic Hughes, Gordon Plotkin, and Vaughan R. Pratt. Full completeness of the multiplicative linear logic of Chu spaces. In *14th IEEE Symposium on Logic in Computer Science (LICS 1999)*, 1999.
- [DP04] Kosta Došen and Zoran Petrić. *Proof-Theoretical Coherence*. KCL Publications, London, 2004.
- [DP07] Kosta Došen and Zoran Petrić. Intermutation. preprint, Mathematical Institute, Belgrade, 2007.
- [DR89] Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Annals of Mathematical Logic*, 28:181–203, 1989.
- [FR94] Arnaud Fleury and Christian Retoré. The mix rule. *Mathematical Structures in Computer Science*, 4(2):273–285, 1994.
- [GS01] Alessio Guglielmi and Lutz Straßburger. Non-commutativity and MELL in the calculus of structures. In Laurent Fribourg, editor, *Computer Science Logic, CSL 2001*, volume 2142 of *LNCS*, pages 54–68. Springer-Verlag, 2001.
- [Gug07] Alessio Guglielmi. A system of interaction and structure. *ACM Transactions on Computational Logic*, 8(1), 2007.
- [Hug06] Dominic J.D. Hughes. Proofs Without Syntax. *Annals of Mathematics*, 164(3):1065–1076, 2006.
- [Lam06] François Lamarche. Exploring the gap between linear and classical logic, 2006. Accepted for publication in *TAC*.
- [Mac71] Saunders Mac Lane. *Categories for the Working Mathematician*. Number 5 in Graduate Texts in Mathematics. Springer-Verlag, 1971.
- [Möh89] Rolf H. Möhring. Computationally tractable classes of ordered sets. In I. Rival, editor, *Algorithms and Order*, pages 105–194. Kluwer Acad. Publ., 1989.
- [Ret93] Christian Retoré. *Réseaux et Séquents Ordonnés*. Thèse de Doctorat, spécialité mathématiques, Université Paris VII, February 1993.
- [Ret96] Christian Retoré. Perfect matchings and series-parallel graphs: multiplicative proof nets as R&B-graphs. *ENTCS*, vol. 3, 1996.
- [Ret03] Christian Retoré. Handsome proof-nets: perfect matchings and cographs. *Theoretical Computer Science*, 294(3):473–488, 2003.
- [Str02] Lutz Straßburger. A local system for linear logic. In M. Baaz and A. Voronkov, editors, *LPAR 2002*, volume 2514 of *LNAI*, pages 388–402. Springer-Verlag, 2002.
- [Str03a] Lutz Straßburger. *Linear Logic and Noncommutativity in the Calculus of Structures*. PhD thesis, Technische Universität Dresden, 2003.
- [Str03b] Lutz Straßburger. MELL in the Calculus of Structures. *Theoretical Computer Science*, 309(1–3):213–285, 2003.
- [Str05] Lutz Straßburger. On the axiomatisation of Boolean categories with and without medial, 2005. Accepted for publication in *TAC*.