

## UNIQUE PERFECT MATCHINGS, FORBIDDEN TRANSITIONS AND PROOF NETS FOR LINEAR LOGIC WITH MIX

LÊ THÀNH DŨNG NGUYỄN

Université publique, France  
*e-mail address*: [nltd@nguyentito.eu](mailto:nltd@nguyentito.eu)

**ABSTRACT.** This paper establishes a bridge between linear logic and mainstream graph theory, building on previous work by Retoré (2003). We show that the problem of correctness for MLL+Mix proof nets is equivalent to the problem of uniqueness of a perfect matching. By applying matching theory, we obtain new results for MLL+Mix proof nets: a linear-time correctness criterion, a quasi-linear sequentialization algorithm, and a characterization of the sub-polynomial complexity of the correctness problem. We also use graph algorithms to compute the dependency relation of Bagnol et al. (2015) and the kingdom ordering of Bellin (1997), and relate them to the notion of blossom which is central to combinatorial maximum matching algorithms.

In this journal version, we have added an explanation of Retoré’s “RB-graphs” in terms of a general construction on graphs with forbidden transitions. In fact, it is by analyzing RB-graphs that we arrived at this construction, and thus obtained a polynomial-time algorithm for finding trails avoiding forbidden transitions; the latter is among the material covered in another paper by the author focusing on graph theory.

### 1. INTRODUCTION

**1.1. Algorithmics of proofs in linear logic.** One of the major innovations introduced at the birth of linear logic [Gir87] was a representation of proofs as *graphs*, instead of trees as in natural deduction or sequent calculus. A distinctive property of these *proof nets* is that checking that a proof is correct cannot be done merely by a local verification of inference steps: among the graphs which locally look like proof nets, called *proof structures*, some are invalid proofs. Hence the *correctness* problem: given a proof structure, is it a real proof net?

A lot of work has been devoted to this decision problem, and in the case of the multiplicative fragment of linear logic (MLL), whose proof nets are the most satisfactory, it can be considered solved from an algorithmic point of view. Indeed, Guerrini [Gue11] and Murawski and Ong [MO06] have found linear-time tests for MLL correctness; the problem has

---

*Key words and phrases:* correctness criteria, matching algorithms.

\* Extended version of a FSCD 2018 paper.

The manifesto <https://pageperso.lif.univ-mrs.fr/~sylvain.sene/affiliation.html> (in French; archived on 2020-02-12 on the Internet Wayback Machine (<https://archive.org/>)) explains the given affiliation.

also been shown to be NL-complete by Jacobé de Naurois and Mogbil [JdNM11]. Both the linear-time algorithms we mentioned also solve the corresponding search problem: computing a *sequentialization* of a MLL proof net, i.e., a translation into sequent calculus.

However, for MLL extended with the *Mix rule* [FR94] (MLL+Mix), the precise complexity of deciding correctness has remained unknown (though a polynomial-time algorithm was given by Danos [Dan90]). Thus, one of our goals in this paper is to study the following problems:

**Problem 1.1** (MIXCORR). Given a proof structure  $\pi$ , is it an MLL+Mix proof net?

**Problem 1.2** (MIXSEQ). Reconstruct a sequent calculus proof for an MLL+Mix proof net.

**1.2. Proof nets vs graph theory.** It turns out that a *linear-time* algorithm for MIXCORR follows immediately from already known results<sup>1</sup>, see Theorem 4.1. The key is to use a construction by Retoré [Ret99, Ret03] to reduce it to the problem of *uniqueness of a given perfect matching*, which can be solved in linear time [GKT01]:

**Problem 1.3** (UNIQUENESSPM). Given a graph  $G$ , together with a *perfect matching*  $M$  of  $G$ , is  $M$  the only perfect matching of  $G$ ? Equivalently, is there no *alternating cycle* for  $M$ ?

This brings us to the central idea of this paper: *from the point of view of algorithmics, MLL+Mix proof nets and unique perfect matchings are essentially the same thing*. This allows us to apply matching theory to the study of proof nets, leading to several new results. Indeed, one would expect graph algorithms to be of use in solving problems on proof structures, since they are graphs! But for this purpose, a bridge between the theory of proof nets and mainstream graph theory is needed, whereas previous work on the former mostly made use of “homemade” objects such as *paired graphs* (an exception being Murawski and Ong’s use of *dominator trees*). By building on Retoré’s discovery of a connection with perfect matchings, this paper proposes such a bridge.

Thus, proof structures are revealed to be part of a family of graph-theoretic objects which admit equivalent (as shown by Szeider [Sze04]) “structure from acyclicity” properties. In linear logic, the corresponding acyclicity property has been known for a long time: it is the *Danos–Regnier correctness criterion* [DR89], a necessary and sufficient condition for a proof structure to be a proof net. These connections have also inspired new results concerning other members of this family, not only perfect matchings but also, *e.g.*, “edge-colored graphs”; that is the subject of another paper by the author [Ngu19].

Another occurrence of an equivalent “structure from acyclicity” result, of historical interest for us, is Retoré’s “aggregates” [Ret93, Chapter 2]<sup>2</sup>, an early attempt to define a purely graph-theoretic counterpart to the theory of MLL+Mix correctness. It turns out that these aggregates occur naturally in graph theory as a tractable case of the “rainbow path problem” as we show in [Ngu19].

<sup>1</sup>A similar historical remark can be made about correctness for MLL without Mix, see Remark 4.2.

<sup>2</sup>To be more accurate, in the reference given, which is a PhD thesis written in French, they are called “agrégats”. However, the word “aggregate” is indeed the official translation, and appeared in the title of the never published note *Graph theory from linear logic: Aggregates* (Preprint 47, Équipe de Logique, Université Paris 7). That title is also a good summary for what we try to achieve in the present paper and in [Ngu19].

**1.3. Contributions.** First, we establish our equivalence by giving a translation from graphs equipped with perfect matchings to proof structures (Section 3) — Retoré’s pre-existing construction takes care of the converse direction<sup>3</sup>. We also propose later an alternative to Retoré’s translation (Section 5.1), having better properties with respect to sequentialization; this yields a new graph-theoretic proof of the *sequentialization theorem*, i.e., the equivalence between MLL+Mix proof nets and Danos–Regnier acyclic proof structures.

**1.3.1. Complexity of problems on proof nets.** As already mentioned, we give the first linear-time algorithm for MIXCORR (Section 4.1). As for its sub-polynomial complexity (Section 4.2), we show that MIXCORR is in randomized NC and in quasiNC (informally, NC is the class of problems with efficient *parallel* algorithms). On the other hand, we have a sort of hardness result: if MIXCORR were in NC — in particular, if it were in NL, as for MLL without Mix — this would imply a solution to a long-standing conjecture by Lovász (Conjecture 4.7) concerning the related *unique perfect matching* problem:

**Problem 1.4** (UNIQUEPM [KVV85, GKT01, HMT06]). Given a graph  $G$ , determine whether it admits exactly one perfect matching and, if so, find this matching.

We then turn to the sequentialization problem, for which we provide a graph-theoretic reformulation — thanks to our new translation in Section 5.1 — and an algorithm relying on this reformulation. This gives us a *quasi-linear* time<sup>4</sup> solution to MIXSEQ (Section 5.2); to our knowledge, this beats previous algorithms for MIXSEQ.

As a demonstration of our matching-theoretic toolbox, we also show how to compute some information on the set of *all* sequentializations, namely Bellin’s *kingdom ordering* [Bel97] of the links of a MLL+Mix proof net (rediscovered by Bagnol et al. [BDS15] under the name of *order of introduction*). We give a polynomial time and a quasiNC algorithm (Section 6), both relying on an effective characterization of this ordering.

**1.3.2. Further connections to graph theory.** We also show that this notion of kingdom ordering admits a direct counterpart in unique perfect matchings. The above-mentioned characterization, when rephrased in the language of graph theory (Section 6.2), turns out to involve objects which play a major role in matching algorithms, namely *blossoms* [Edm65]. In this way, we obtain a new result of independent interest in combinatorics. The appendix of the conference version of this paper contained a direct proof of this result; instead of reproducing it here, we have moved it to the companion paper [Ngu19], and limit ourselves here to the equivalence with the already known [Bel97] proof net version.

Finally, in Section 7 — a new section added for this journal version<sup>5</sup> — we analyse Retoré’s “RB-graphs” reduction [Ret03], and show that it can be understood in terms of graphs with *forbidden transitions* [Sze03] which can be seen as the generalized paired graphs. This reveals a minor subtlety about what kind of cycles RB-graphs actually detect in paired graphs.

<sup>3</sup>This is a first difference with the conference version, which did not include Retoré’s translation.

<sup>4</sup>More precisely,  $O(n(\log n)^2(\log \log n)^2)$  time. Both this and our quasiNC algorithms rely on very recent advances, respectively on dynamic bridge-finding data structures [HRT18] and on the perfect matching existence problem [ST17]. Any further progress on these problems would lead to an improvement of our complexity bounds.

<sup>5</sup>This results of that new section were previously claimed without proof in a contributed talk at the 1st International Workshop on Trends in Linear Logic and Applications (TLLA 2017).

## CONTENTS

|   |    |
|---|----|
| 1. Introduction   | 1  |
| 1.1. Algorithmics of proofs in linear logic                         | 1  |
| 1.2. Proof nets vs graph theory                                     | 2  |
| 1.3. Contributions  | 3  |
| 2. Preliminaries  | 4  |
| 2.1. Terminology  | 4  |
| 2.2. Perfect matchings, alternating cycles and sequentialization    | 5  |
| 2.3. Proof structures, proof nets and the correctness criterion     | 6  |
| 3. An equivalence through mutual reductions                         | 9  |
| 3.1. From proof structures to perfect matchings: Retoré’s RB-graphs | 9  |
| 3.2. From perfect matchings to proof structures                     | 11 |
| 4. On the complexity of MLL+Mix correctness                         | 13 |
| 4.1. An immediate linear-time algorithm                             | 13 |
| 4.2. Characterizing the sub-polynomial complexity                   | 14 |
| 5. Tackling sequentialization via an appropriate translation        | 15 |
| 5.1. A new encoding: graphification                                 | 15 |
| 5.2. A sequentialization algorithm for MLL+Mix proof nets           | 17 |
| 6. On the kingdom ordering of links                                 | 19 |
| 6.1. Computing the kingdom ordering                                 | 20 |
| 6.2. Dependencies and blossoms in unique perfect matchings          | 21 |
| 7. A reconstruction of RB-graphs via forbidden transitions          | 24 |
| 8. Conclusion   | 26 |
| 8.1. Further hardness results: pomset logic and visible acyclicity  | 26 |
| 8.2. Open questions   | 27 |
| 8.3. Other variants of proof nets through the lens of graph theory  | 27 |
| Acknowledgments   | 28 |
| References  | 28 |
| Appendix A. Proof of Lemma 6.5                                      | 30 |

## 2. PRELIMINARIES

## 2.1. Terminology.

2.1.1. *Graph theory.* By default, “graph” refers to an *undirected* graph. Our *paths* and *cycles* are **not allowed to contain repeated vertices**<sup>6</sup>; we will sometimes identify them with their sets of edges (which characterize them) and apply set operations on them. A *bridge* of a graph is an edge whose removal increases the number of connected components.

For directed graphs, the notion of connectedness we consider is *weak connectedness*, i.e., connectedness of the graph obtained by forgetting the edge directions. A *predecessor* (resp. *successor*) of a vertex is the source (resp. target) of some incoming (resp. outgoing) edge.

<sup>6</sup>This choice of terminology is common, see, e.g., [BJG09, §1.4]. The adjective “elementary” is sometimes used to refer to such paths and cycles.

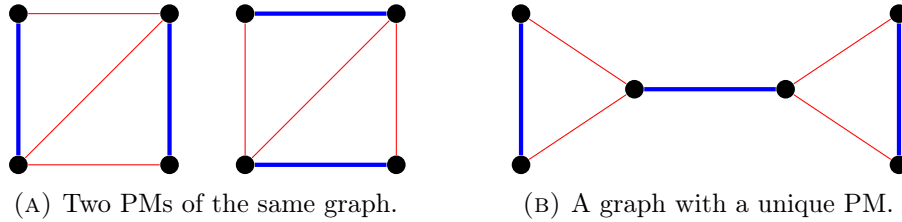


FIGURE 1. Examples of perfect matchings (PMs). The edges in the matchings are thick and blue.

2.1.2. *Complexity classes.* We refer to [JdNM11, §1.4] for the logarithmic space classes L (deterministic) and NL (non-deterministic) and to [CSV84] for the class  $AC^0$  of constant-depth circuits. The class  $NC^k$  (resp.  $quasiNC^k$  [Bar92]) consists of the problems which can be solved by a uniform<sup>7</sup> family of circuits of depth  $O(\log^k n)$  and polynomial (resp. quasi-polynomial, i.e.,  $2^{O(\log^c n)}$ ) size;  $NC = \bigcup_k NC^k$  and  $quasiNC = \bigcup_k quasiNC^k$ .

It is well-known that  $AC^0 \subseteq NC^1 \subseteq L \subseteq NL \subseteq NC^2 \subseteq NC \subseteq P$ .

## 2.2. Perfect matchings, alternating cycles and sequentialization.

**Definition 2.1.** Let  $G = (V, E)$  be a graph. A *matching* (resp. *perfect matching*)  $M$  in  $G$  is a subset of  $E$  such that every vertex in  $V$  is incident to *at most one* (resp. *exactly one*) edge in  $M$ . An *alternating path* (resp. *cycle*) for  $M$  is a path (resp. cycle) where, for every pair of consecutive edges, one of them is in the matching and the other one is not.

Testing the existence of a perfect matching in a graph — or, more generally, finding a maximum cardinality matching — is one of the central computational problems in graph theory. Combinatorial maximum matching algorithms, starting<sup>8</sup> with Edmonds’s *blossom algorithm* [Edm65]<sup>9</sup>, use alternating paths to iteratively increase the size of the matching; similarly, alternating cycles are important for the problems  $UNIQUENESSPM$  and  $UNIQUEPM$  because they witness the *non-uniqueness* of perfect matchings.

**Lemma 2.2** (Berge [Ber57]). *Let  $G$  be a graph and  $M$  be a perfect matching of  $G$ . Then if  $M' \neq M$  is a perfect matching, the symmetric difference  $M \Delta M'$  is a vertex-disjoint union of cycles, which are alternating for both  $M$  and  $M'$ . Conversely, if  $C$  is an alternating cycle for  $M$ , then  $M \Delta C$  is another perfect matching.*

As an example, consider Figure 1a. The matching on the left admits an alternating cycle, the outer square; by taking the symmetric difference between this matching and the set of edges of the cycle, one gets the matching on the right. Conversely, the symmetric difference between both matchings (which, in this case, is their union) is the square. Note also that in Figure 1b, there is no alternating cycle because vertex repetitions are disallowed.

<sup>7</sup>For  $NC^k$  and  $quasiNC^k$ , we may take this to mean that there is a deterministic logarithmic space Turing machine which, given  $n$  in unary, computes the circuit for inputs of size  $n$ . We will not enter into the details of  $AC^0$  uniformity.

<sup>8</sup>Note that the problem was solved long before in the special case of bipartite graphs. In fact, a solution for this case was found in Jacobi’s posthumous papers [Jac65, JO09].

<sup>9</sup>This paper is one of the first to propose defining efficient algorithms as polynomial-time algorithms; it also contributed to the birth of the field of polyhedral combinatorics.

Another approach to finding perfect matchings, using linear algebra, was initiated by Lovász [Lov79] and leads to a *randomized* NC algorithm by Mulmuley et al. [MUV87]. Recently, Svensson and Tarnawski have shown that this algorithm can be derandomized to run in deterministic *quasi*NC [ST17].

There is also a considerable body of purely mathematical work on matchings, starting from the 19th century. Let us mention for our purposes a result dating from 1959.

**Theorem 2.3** (Kotzig [Kot59]). *Let  $G$  be a graph. Suppose that  $G$  admits a unique perfect matching  $M$ . Then  $M$  contains a bridge of  $G$ .*

As shown by Retoré [Ret03], Kotzig’s theorem leads to an inductive characterization of the set of graphs equipped with a unique perfect matching.

**Theorem 2.4** (Sequentialization for unique perfect matchings [Ret03]). *The class  $\mathcal{UPM}$  of graphs equipped with an unique perfect matching is inductively generated as follows:*

- *The empty graph (with the empty matching) is in  $\mathcal{UPM}$ .*
- *The disjoint union of two non-empty members of  $\mathcal{UPM}$  is in  $\mathcal{UPM}$ .*
- *Let  $(G = (V, E), M \subseteq E) \in \mathcal{UPM}$  and  $(G' = (V', E'), M' \subseteq E') \in \mathcal{UPM}$ , with  $V$  and  $V'$  disjoint. Let  $U \subseteq V$ ,  $U' \subseteq V'$  such that  $U \neq \emptyset$  (resp.  $U' \neq \emptyset$ ) unless  $G$  (resp.  $G'$ ) is the empty graph, and let  $x, x'$  be two fresh vertices not in  $V$  nor  $V'$ . Then  $(G'' = (V'', E''), M'' \subseteq E'') \in \mathcal{UPM}$ , where*
  - $V'' = V \cup V' \cup \{x, x'\}$
  - $E'' = E \cup E' \cup \{(x, x')\} \cup (U \times \{x\}) \cup (U' \times \{x'\})$
  - $M'' = M \cup M' \cup \{(x, x')\}$

**Remark 2.5.** By relaxing the non-emptiness condition on  $U$  and  $U'$ , the disjoint union operation becomes unnecessary; this is actually the original statement [Ret03, Theorem 1]. Our motivation for this change is to get a good fit with Theorem 5.6: we want the disjoint union of graphs to correspond to the Mix rule on proof nets.

The inspiration for the above theorem comes from linear logic: it is a graph-theoretic version of the sequentialization theorems for proof nets, with Kotzig’s theorem being analogous to the “splitting lemmas” which appear in various proofs of sequentialization. Section 5 is dedicated to investigating this connection further.

**2.3. Proof structures, proof nets and the correctness criterion.** A proof structure is some kind of graph-like object with the precise definition varying in the literature (we will come back to this point in Remark 3.4). Since our aim is to apply results from graph theory, it will be helpful to commit to a representation of proof structures as graphs.

We write  $\deg^-$  for the indegree and  $\deg^+$  for the outdegree of a vertex.

**Definition 2.6.** A *proof structure* is a non-empty directed acyclic multigraph  $(V, A)$  with a labeling of the vertices  $l : V \rightarrow \{\mathbf{ax}, \otimes, \wp\}$  such that, for  $v \in V$ :

- if  $l(v) = \mathbf{ax}$ , then  $\deg^-(v) = 0$  and  $\deg^+(v) \leq 2$ ,
- if  $l(v) \in \{\otimes, \wp\}$ , then  $\deg^-(v) = 2$  and  $\deg^+(v) \leq 1$ .

Vertices of a proof structure will also be called *links*. A *terminal link* is a link with outdegree 0. A *sub-proof structure* is a vertex-induced subgraph which is a proof structure.

**Remark 2.7.** It is customary to add “dangling outgoing edges” from the terminal links and to consider them to be the *conclusions* of the proof net. See Definition 3.2 and Remark 3.4.

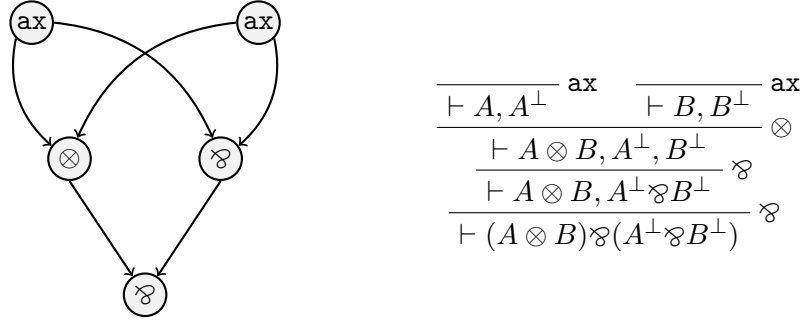


FIGURE 2. A proof net (left) and its sequentialization (right), written as a sequent calculus proof. Edges are usually labeled by the MLL formulae appearing in the sequentialization; since we focus on the combinatorics of proof structures and not on their logical meaning, we omit them here.

$$\frac{}{\vdash A, A^\perp} (\text{ax-rule}) \quad \frac{\vdash \Gamma, A \quad \vdash B, \Delta}{\vdash \Gamma, A \otimes B, \Delta} (\otimes\text{-rule}) \quad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \wp B} (\wp\text{-rule}) \quad \frac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta} (\text{Mix rule})$$

FIGURE 3. Rules for the MLL+Mix sequent calculus; note the correspondence with Definition 2.8.

**Definition 2.8.** The set of *MLL proof nets* is the subset of proof structures inductively generated by the following rules:

- **ax-rule:** a proof structure with a single **ax**-link is a proof net.
- **⊗-rule:** if  $N$  and  $N'$  are proof nets,  $u$  is a link of  $N$  and  $v$  is a link of  $N'$ , then taking the disjoint union of  $N$  and  $N'$ , adding a new  $\otimes$ -link  $w$ , an edge from  $u$  to  $w$  and an edge from  $v$  to  $w$  gives a proof net, as long as the resulting graph is a proof structure (i.e., the degree constraints are satisfied).
- **⊗-rule:** if  $N$  is a proof net and  $u, v$  are links of  $N$ , then adding a new  $\wp$ -link  $w$ , an edge from  $u$  to  $w$  and an edge from  $v$  to  $w$  gives a proof net, with the same proviso as above.

The set of *MLL+Mix proof nets* is inductively generated by the above rules together with the **Mix rule:** if  $N$  and  $N'$  are proof nets, their disjoint union is a proof net.

A proof structure is said to be *correct* if it is a MLL+Mix proof net.

**Remark 2.9.** As with any inductively defined set, membership proofs for the set of MLL (resp. MLL+Mix) proof nets may be presented as inductive derivation trees, which are isomorphic to the usual *sequent calculus proofs* of MLL (resp. MLL+Mix): see Figure 2 for an example, and Figure 3 for the inference rules of the sequent calculus. An example of inductive construction presented directly on proof nets is given in Figure 4.

**Remark 2.10.** The proof structures and proof nets defined here are *cut-free*. This restriction is without loss of generality, since a cut link has exactly the same behavior as a terminal  $\otimes$ -link with respect to correctness and sequentialization.

To tackle the problem of correctness, it is useful to have non-inductive characterizations of proof nets, called *correctness criteria*, at our disposal. Many of them are formulated using the notion of *paired graphs*. We will state a criterion first discovered by Danos and Regnier for MLL [DR89] and extended to MLL+Mix by Fleury and Retoré [FR94].

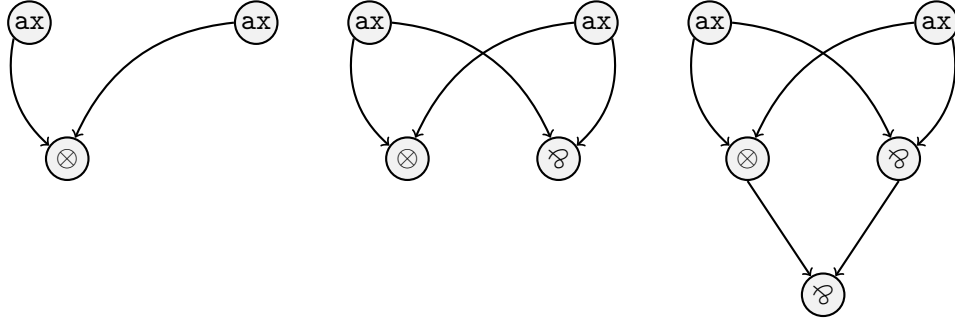


FIGURE 4. Two successive applications of the  $\otimes$ -rule to obtain the proof net of Figure 2 at the end; compare with the two bottom inferences of the sequent calculus proof of Figure 2. The leftmost proof net can be obtained by invoking the **ax**-rule to create two proof nets, then combining them with a  $\otimes$ -rule.

**Definition 2.11.** A *paired graph* consists of an undirected graph  $G = (V, E)$  and a set  $\mathcal{P}$  of unordered pairs of edges such that:

- if  $\{e, f\} \in \mathcal{P}$ , then  $e$  and  $f$  have a vertex in common;
- the pairs are disjoint: if  $p, p' \in \mathcal{P}$  and  $p \neq p'$ , then  $p \cap p' = \emptyset$ .

When  $\{e, f\} \in \mathcal{P}$ , the edges  $e$  and  $f$  are said to be *paired*.

A *switching*  $S$  is a set of edges containing exactly one from every pair in  $\mathcal{P}$ . The *switching graph* for  $S$  is the spanning subgraph  $(V, E \setminus (\bigcup \mathcal{P} \setminus S))$  of  $G$ , where  $\bigcup \mathcal{P}$  is the union of all pairs in  $\mathcal{P}$ . A *switching path* (resp. *cycle*) is a path (resp. cycle) which intersects each pair of  $\mathcal{P}$  at most once.

**Remark 2.12.** Equivalently, switching cycles are cycles which exist in some switching graph.

**Definition 2.13.** Let  $\pi$  be a proof structure. Its *correctness graph*  $C(\pi)$  is the paired graph obtained by forgetting the directions of the edges and the labels of the vertices in  $\pi$ , and pairing together two edges when their targets<sup>10</sup> are the same  $\otimes$ -link.

A *switching path* (resp. *cycle*) in  $\pi$  is a sequence of edges of  $\pi$  whose image in  $C(\pi)$  is a switching path (resp. cycle).

Examples of switchings graphs of a correctness graph are given in Figure 5.

**Theorem 2.14** (Danos–Regnier correctness criterion). *A proof structure  $\pi$  is a MLL (resp. MLL+Mix) proof net if and only if all the switching graphs of  $C(\pi)$  are trees (resp. forests).*

**Remark 2.15.** Equivalently,  $\pi$  is a MLL+Mix proof net if and only if it contains no switching cycle.

The above is usually called a *sequentialization theorem*: it means that a proof structure which satisfies the correctness criterion admits a sequent calculus derivation.

The analogy with Theorem 2.4 is that proof nets are to proof structures what *unique* perfect matchings are to perfect matchings. The next section is dedicated to formalizing this analogy into an equivalence.

<sup>10</sup>That is, the targets of the directed edges in  $\pi$  they come from.



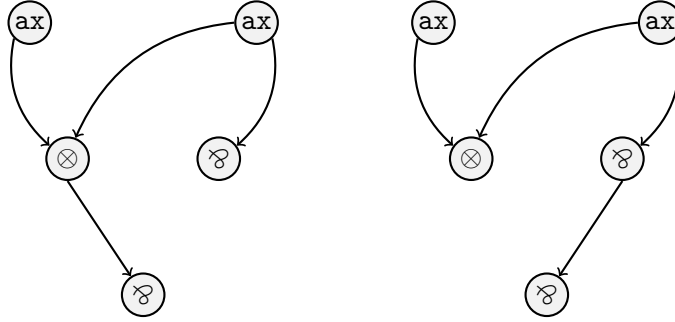


FIGURE 5. Two switching graphs out of four possibilities for the proof structure of Figure 2.

### 3. AN EQUIVALENCE THROUGH MUTUAL REDUCTIONS

We will now see how to turn a proof structure into a graph equipped with a perfect matching, in such a way that switching cycles become alternating cycles, and vice versa. Such a translation from proof structures to perfect matchings was first proposed by Retoré [Ret03], under the name of *RB-graphs*. After recalling the definition of RB-graphs and their properties in Section 3.1, we propose our own translation in the converse direction — which we call the *proofification* construction — in Section 3.2.

Thus, this section sets up the reductions (in the sense of complexity theory) that will be exploited in Section 4. But further developments in Section 5 and Section 6 will require the introduction of a new translation (*graphification*) from proofs to graphs.

**Remark 3.1.** The nature of the object corresponding to a matching edge in a proof structure will vary depending on the translation considered: for RB-graphs, they correspond to edges or terminal links, whereas in the case of proofifications, they are translated into  $\otimes$ -links. (And in the graphifications of Section 5.1, they correspond to links.)

Thus, by taking the proofification of a RB-graph of a proof structure, one gets a different proof structure, with the edges of the former being sent to  $\otimes$ -links of the latter. It is unclear whether this transformation has any meaning in terms of linear logic; in particular it does not preserve correctness for MLL without Mix.

**3.1. From proof structures to perfect matchings: Retoré’s RB-graphs.** To define RB-graphs, it is more convenient to start from a slightly altered definition of proof structures.

**Definition 3.2.** A *proof structure with conclusions* is a non-empty directed acyclic multigraph  $(V, A)$  with a *partial* labeling of the vertices  $l : V \rightarrow \{\mathbf{ax}, \otimes, \wp\}$  such that, for  $v \in V$ :

- if  $l(v) = \mathbf{ax}$ , then  $\deg^-(v) = 0$  and  $\deg^+(v) = 2$ ;
- if  $l(v) \in \{\otimes, \wp\}$ , then  $\deg^-(v) = 2$  and  $\deg^+(v) = 1$ ;
- else,  $v$  is unlabeled, and then  $\deg^-(v) = 1$  and  $\deg^+(v) = 0$ .

In the latter case,  $v$  is called a *conclusion vertex* and its unique incoming edge is called a *conclusion edge*.

Compared with Definition 2.6, the bounds on the outdegree have become equalities, while a new kind of vertex has been added. The idea is that, when the inequality on the outdegree is strict, there are “missing” outgoing edges, which are materialized here as conclusion edges.

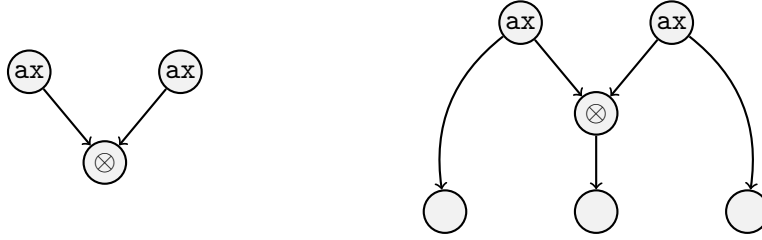


FIGURE 6. An instance of the bijection of Proposition 3.3: the proof structure (according to Definition 2.6) on the left corresponds to the proof structure with conclusions (Definition 3.2) on the right.

Yet the object being manipulated is still fundamentally the same; indeed, the following is immediate (see Figure 6 for an example):

**Proposition 3.3.** *Given a proof structure with conclusions, the subgraph induced by the labeled vertices is a proof structure according to Definition 2.6. This correspondence is bijective: conversely, there is a unique way to add unlabeled conclusions to a proof structure.*

**Remark 3.4.** Here we are confronted with the fact that there is no single canonical definition of MLL proof structures (although two given definitions are always canonically isomorphic). Depending on the task at hand, different combinatorial formalizations of the same object may be more or less convenient. To define proof nets inductively, it was easier to use proof structures without conclusions and rely on the notion of terminal link. This will also prove useful for the sequentialization algorithm of Section 5.2. But the conclusion edges are logically significant<sup>11</sup>: they correspond to the formulas in the sequent being proven.

Starting from this, we can now introduce RB-graphs. The definition we use is taken from Straßburger’s lecture notes at ESSLLI’06 [Str06], and differs slightly from Retoré’s original one (edges are handled more uniformly in Straßburger’s version).

**Definition 3.5** [Ret03, Str06]. Let  $(V, A, l)$  be a proof structure with conclusions. The corresponding *RB-graph* is a graph  $G$  equipped with a perfect matching  $M$  such that:

- $M$  is in bijection with the directed edges  $A$ ;
- the non-matching edges of  $G$  are derived from the labeling  $l : V \rightarrow \{\text{ax}, \otimes, \wp\}$  of the links, following the rules of Figure 7 (conclusion vertices do not induce non-matching edges).

An example of RB-graph is given in Figure 8. The interest of this translation lies in:

**Proposition 3.6** (implicit in [Ret03]). *The switching cycles in a proof structure are in bijection with the alternating cycles in its RB-graph.*

**Corollary 3.7** (Retoré’s correctness criterion [Ret03]). *A proof structure satisfies the Danos–Regnier criterion for MLL+Mix if and only if the perfect matching of its RB-graph is unique.*

<sup>11</sup>An annoying point, however, is that the conclusion *vertices* have no significance, so sometimes proof structures are defined with “dangling edges” with no target. However, dangling edges drag us out of the world of graphs, and into hypergraphs — indeed, they are hyperedges of arity 1. Proof structures are also often defined as the dual hypergraph: links are hyperedges, and formulas are vertices. For our purposes, we have chosen to keep proof structures as actual graphs, to make the connections with graph theory clearer.

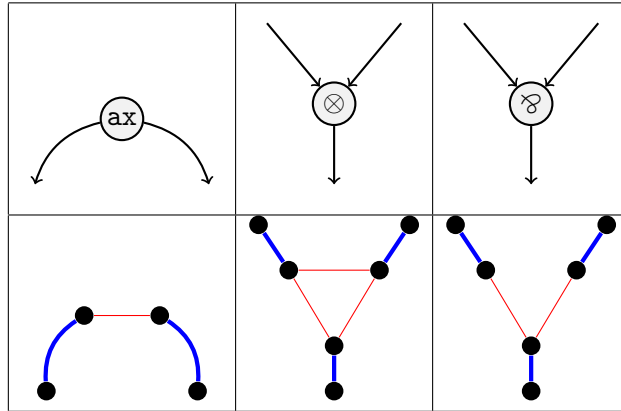


FIGURE 7. Translation of proof structures links (top) to RB-graphs (bottom).

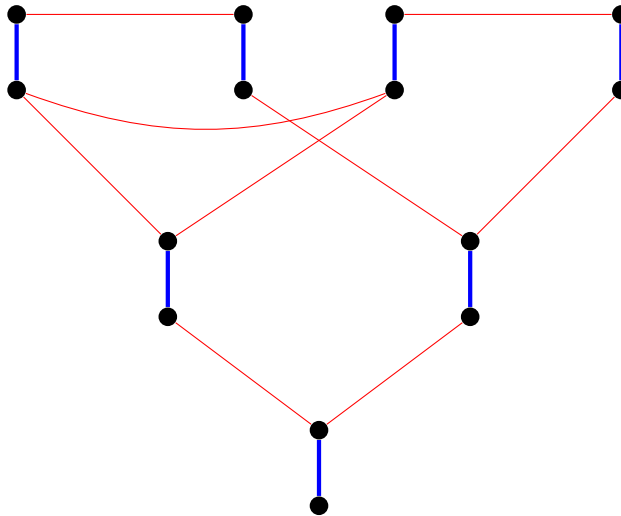


FIGURE 8. RB-graph corresponding to the proof net of Figure 2.

**3.2. From perfect matchings to proof structures.** The translation we present below involves “ $k$ -ary  $\wp$ -links”. When  $k > 1$ , these are just binary trees of  $k - 1$   $\wp$ -links (correctness is independent of the choice of binary tree: semantically, this is associativity of  $\wp$ ) with  $k$  leaves (incoming edges) and a single root (outgoing edge); the  $k = 1$  case corresponds to a single edge and no link.

**Definition 3.8.** Let  $G = (V, E)$  be a graph and  $M$  be a perfect matching of  $G$ . We define the *proofification* of  $(G, M)$  as the proof structure  $\pi$  built as follows:

- For each non-matching edge  $e = (u, v) \in E \setminus M$ , we create an  $\text{ax}$ -link  $\text{ax}_e$  whose two outgoing edges we will call  $A_{u,v}$  and  $A_{v,u}$ .
- For each vertex  $u \in V$ , if  $\text{deg}(u) > 1$ , we add a  $k$ -ary  $\wp$ -link with  $k = \text{deg}(u) - 1$ , whose incoming edges are the  $A_{u,v}$  for all neighbors  $v$  of  $u$  such that  $(u, v) \notin M$ , and we call its outgoing edge  $B_u$ . If  $\text{deg}(u) = 1$ , we add an  $\text{ax}$ -link calling one of its outgoing edges  $B_u$ .
- For each matching edge  $(u, v) \in M$ , we add an  $\otimes$ -link whose incoming edges are  $B_u$  and  $B_v$ . These  $\otimes$ -links are the terminal links of  $\pi$ .

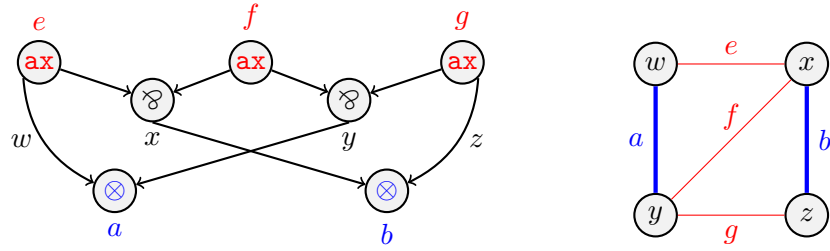


FIGURE 9. The proofification of the graph of Figure 1a.

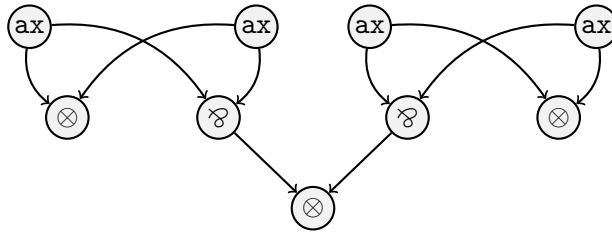


FIGURE 10. The proofification of the graph in Figure 1b. Since the perfect matching in Figure 1b was unique, we get a MLL+Mix proof net. One can check that in this case, it is even correct for MLL.

This proof net will also be used as an example in Section 6.

Examples of proofification are provided in Figure 9 (annotated figure) and Figure 10.

**Proposition 3.9.** *Let  $G$  be a graph and  $M$  be a perfect matching of  $G$ . The alternating cycles for  $M$  in  $G$  are in bijection with the switching cycles in the proofification of  $(G, M)$ .*

*Proof.* Let  $\pi$  be the proofification of  $(G, M)$ . Any switching cycle in  $\pi$  changes direction only at  $\mathbf{ax}$ -links and  $\otimes$ -links, and therefore can be partitioned into an alternation of  $\otimes$ -links, corresponding to matching edges, and of paths starting with some  $B_u$ , ending with some  $B_v$  and crossing some  $\mathbf{ax}_e$ , corresponding to non-matching edges  $e = (u, v)$ . Therefore, it corresponds to an alternating cycle for  $M$ , and the mapping defined this way is bijective.  $\square$

We end this section on a property of the *sequentializations* of  $\pi$ .

**Proposition 3.10.** *Let  $G$  be a graph with a unique perfect matching  $M$  and let  $\pi$  be the proofification of  $(G, M)$ . A matching edge  $e \in M$  is a bridge of  $G$  if and only if its corresponding  $\otimes$ -link is introduced by the last rule of some sequentialization of  $\pi$ .*

*Proof.* This follows from the fact that a  $\otimes$ -link may be introduced by the last rule of a sequentialization if and only if it is splitting, i.e., its removal disconnects its two predecessors.  $\square$

This is consistent with the discussion at the end of Section 2.2: a bridge in a unique perfect matching may be taken as a “last rule” in its “sequentialization” in the sense of Theorem 2.4. However, RB-graphs do not satisfy a property analogous to the above proposition. This is one of the motivations for the introduction of our new translation (Section 5.1), cf. Theorem 5.6.

## 4. ON THE COMPLEXITY OF MLL+MIX CORRECTNESS

Through the translations of the previous section, MLL+Mix proof *nets* become *unique* perfect matchings and conversely: these translations provide *reductions* between the problems MIXCORR and UNIQUENESSPM, allowing us to draw complexity-theoretic conclusions on proof nets from known results in graph theory. We first look at the time complexity of MIXCORR, then turn to its complexity under constant-depth ( $AC^0$ ) reductions.

**4.1. An immediate linear-time algorithm.** Computing Retoré’s RB-graphs (Section 3.1) and deciding UNIQUENESSPM [GKT01, §3] can both be done in linear time, so:

**Theorem 4.1.** MIXCORR *can be decided in linear time.*

**Remark 4.2.** By using the “Euler–Poincaré lemma” (an old part of the linear logic folklore, written down in, *e.g.*, [BDS15]) to count the uses of the Mix rule in a proof net, this also allows us to decide the correctness of a proof structure for MLL without Mix in linear time.

Historically, all the necessary ingredients for Theorem 4.1 and for its corollary for MLL already existed before the announcement (at LICS’99, in July 1999) of Guerrini’s linear-time correctness criterion for MLL [Gue11]. Indeed, Retoré first presented his RB-graphs at the 1996 Linear Logic Tokyo Meeting [Ret96], and Gabow et al.’s algorithm [GKT01] was published at the STOC’99 conference in May 1999.

Yet this does not make Guerrini’s work obsolete: the latter also gives a way to compute a *sequentialization* in linear time for MLL proof nets. The other previously known linear-time algorithm for MLL correctness [MO06] also provides a linear-time sequentialization procedure. For MLL+Mix, we do not quite manage to match this complexity, though we obtain a *quasi-linear* algorithm, cf. Section 5.2.

This is because the methods used in [Gue11, MO06] are quite different from ours: instead of using the Danos–Regnier switching acyclicity criterion, their starting points are respectively contractibility (cf. Remark 4.4) and translation to essential nets (cf. Section 8.3.2), which does not work with the Mix rule. Therefore, linear time correctness for MLL+Mix is absolutely not a trivial generalization of the previous literature on MLL without Mix. The discussion at the start of Section 6 makes a similar point with respect to sequentialization.

**Remark 4.3.** Our decision procedure has the advantage of being simpler to describe than the aforementioned algorithms for MLL correctness. That said, this apparent simplicity is due to our use of the algorithm of Gabow et al. [GKT01] as a black box. Looking inside the black box reveals, for instance, that it uses the *incremental tree set union* data structure of Gabow and Tarjan [GT85], which, intriguingly, is also a crucial ingredient of both [Gue11, MO06].

Finding an alternating cycle is indeed more tricky than it appears at first sight. Naively, one would perform a graph traversal which visits alternatively matching edges and non-matching edges. The issue is that this would not ensure that the alternating cycle found is *elementary*, i.e., that there are no vertex repetitions, which is an essential condition (that we have included in our definition of “cycle” in Section 2.1). The difficulty of the problem indeed lies in the interaction of this global constraint with the local alternation condition. The analogous issue, seen directly on proof structures, is that the traversal does not remember whether a premise of a  $\wp$ -link has already been traversed before (in fact the standard path-finding algorithms rely on a kind of history independence: it does not matter how you reached some intermediate vertex, as long as your path was of minimum length).

**Remark 4.4.** Gabow et al.’s algorithm for UNIQUENESSPM relies on the technique of *blossom shrinking* pioneered by Edmonds [Edm65], a kind of graph contraction which may remind us of Danos’s *contractibility* correctness criterion [Dan90] for MLL without Mix. Indeed, there exists a formal connection: a rewrite step of *big-step contractibility* [BDS15] corresponds, when translated to either Retoré’s RB-graphs or our graphifications (Section 5.1), to contracting a blossom. However, not all blossoms are redexes for big-step contractibility. See Section 6.2 for further discussion of blossoms.

**4.2. Characterizing the sub-polynomial complexity.** For MLL proof nets without Mix, correctness is known to be NL-complete under  $AC^0$  reductions thanks to the Mogbil–Naurois criterion [JdNM11]. What about MLL+Mix? Since the reductions of Section 3 can be computed in constant depth, we have:

**Theorem 4.5.** *MIXCORR and UNIQUENESSPM are equivalent under  $AC^0$  reductions.*

Thus, it will suffice to study the complexity of UNIQUENESSPM. Let us start with a positive result, using the parallel algorithms for perfect matchings mentioned in Section 2.2.

**Proposition 4.6.** *UNIQUENESSPM is in randomized NC and in deterministic quasiNC.*

*Proof.* Let  $G = (V, E)$  be a graph and  $M$  be a perfect matching of  $G$ .  $M$  is *not* unique if and only if, for some  $e \in M$ , the graph  $G_e = (V, E \setminus \{e\})$  has a perfect matching. To test the uniqueness of  $M$ , run the  $|M|$  parallel instances, one for each  $G_e$ , of a randomized NC [MVV87] or deterministic quasiNC [ST17] algorithm for deciding the existence of a perfect matching, and compute the disjunction of their answers in  $AC^0$ .  $\square$

Being in quasiNC is a much weaker<sup>12</sup> result than being in NL. But as we shall now see, even showing that UNIQUENESSPM is in NC (recall that  $NL \subset NC$ ) would be a major result. It would answer in the affirmative the following conjecture dating back from the 1980’s:

**Conjecture 4.7** (Lovász<sup>13</sup>). *UNIQUEPM is in NC.*

Indeed, the following shows that  $UNIQUENESSPM \in NC \Rightarrow UNIQUEPM \in NC$  (and the converse follows from the definitions).

**Proposition 4.8.** *There is a  $NC^2$  reduction from UNIQUEPM to UNIQUENESSPM.*

*Proof.* This is a consequence of a  $NC^2$  algorithm by Rabin and Vazirani [RV89, §4] which, given a graph  $G$ , computes a set of edges  $M$  such that if  $G$  admits a unique perfect matching, then  $M$  is this matching. Starting from any graph  $G$ , run this algorithm and test whether its output is a perfect matching. If not, then  $G$  does not admit a unique perfect matching; if it is, then  $G$  is a positive instance of UNIQUEPM if and only if  $(G, M)$  is a positive instance of UNIQUENESSPM.  $\square$

To sum up these results about UNIQUENESSPM, which apply to MIXCORR:

**Theorem 4.9.** *MIXCORR is in randomized NC and in deterministic quasiNC; it is in deterministic NC if and only if Conjecture 4.7 is true.*

<sup>12</sup>In fact, one can show that  $NL \subsetneq NSPACE(O(\log^{3/2} n)) \subseteq \text{quasiNC}^3$ , and the problem of finding a perfect matching lies in the latter, according to Svensson and Tarnawski’s analysis.

<sup>13</sup>The conjecture is attributed to Lovász by a paper by Kozen et al. [KVV85] which claims to solve it. But Hoang et al. [HMT06] note that “this was later retracted in a personal communication by the authors”. Still, the proposed solution works for bipartite graphs.

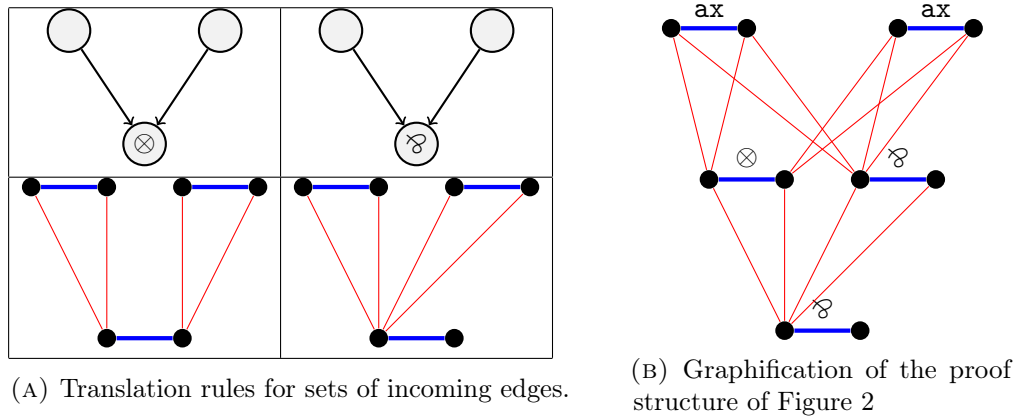


FIGURE 11. The graphification construction.

5. TACKLING SEQUENTIALIZATION VIA AN APPROPRIATE TRANSLATION

We are now interested in using our graph-theoretical tools to deal with problems concerning the *order of logical rules*, typically that of computing a *sequentialization* (problem MIXSEQ from the introduction). However, there is a mismatch between RB-graphs and proof nets: a bridge in a RB-graph does not necessarily correspond to the last rule of some sequentialization of the proof net — in fact, it generally does not even correspond to a terminal link. The key issue is indeed that the successor relation (called  $S(\pi)$  in section 6.1), i.e., “there is a directed edge from  $l$  to  $l'$ ” is forgotten by the translation to RB-graphs.

A toy case to witness the inconvenience caused by this mismatch is the following: we would like to deduce the sequentialization theorem for the Danos–Regnier criterion (Theorem 2.14) as an immediate corollary of Retoré’s sequentialization for unique perfect matchings (Theorem 2.4). But this is not possible with RB-graphs – instead, one must resort to a proof by induction using Kotzig’s theorem (Theorem 2.3), see [Ret99, §2.4].

5.1. **A new encoding: graphification.** To fulfill the desiderata mentioned above, we introduce the following construction, which involves a trick to encode the successor relation.

**Definition 5.1.** Let  $\pi$  be a proof structure and  $L$  be its set of links. The *graphification* of  $\pi$  is the graph  $G = (V, E)$  equipped with a perfect matching  $M \subseteq E$  with

- the matching edges corresponding to the links:  $V = \bigcup_{l \in L} \{a_l, b_l\}$ ,  $M = \{(a_l, b_l) \mid l \in L\}$ ,
- and the remaining edges in  $E \setminus M$  reflect the incoming edges of the  $\otimes$ -links and  $\wp$ -links, as specified by Figure 11a.

Figure 11b shows an example of this construction. As another example, Figure 1b from Section 2.2 is actually the graphification of Figure 6 from Section 3.1.

**Remark 5.2.** There is an ambiguity about the “ $\wp$  of  $ax$ ” configuration (cf. Figure 12) that can occur in correct proof nets: should it result in a multigraph with parallel non-matching edges, or in a simple graph? For simplicity we choose the simple graph option, since that is the setting for most of the literature on matchings, but this detail has very little importance.

**Remark 5.3.** To extend Remark 3.1, there is no clear relationship between graphifications and either of the two translations seen until now (RB-graphs and proofifications).

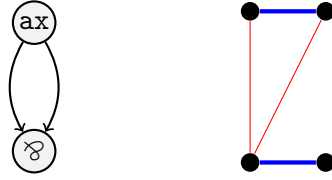


FIGURE 12. The “ $\otimes$  of  $\mathbf{ax}$ ” configuration and its graphification.

Just like RB-graphs, graphifications provide a linear time and  $\text{AC}^0$  reduction from MIXCORR to UNIQUENESSPM: the complexity results of the previous section could have been obtained using graphifications (as was done in the conference version). We focus on the soundness of the reduction, since its complexity is more or less intuitive.

**Proposition 5.4** (Graphification-based correctness criterion). *A proof structure satisfies the Danos–Regnier correctness criterion for  $\text{MLL}+\text{Mix}$  if and only if the perfect matching of its graphification is unique.*

*Proof.* By negating the two sides of the equivalence, the goal becomes proving that a proof structure  $\pi$  contains a switching cycle if and only if its graphification  $(G, M)$  contains an alternating cycle.

Consider any alternating cycle for  $M$  in  $G$  of length  $2n$ , and take the  $\mathbb{Z}/(n)$ -indexed sequence of vertices corresponding to the matching edges in the cycle. By construction of the graphification, if two edges in  $M$  are incident to a common non-matching edge, then the corresponding links in  $\pi$  are adjacent: thus, in our sequence, each vertex is adjacent to the previous and the next one, and thus we have a cycle. If it were not a switching cycle, it would contain three consecutive links  $p, q, r$  with  $q$  a  $\otimes$ -link and  $p, r$  its predecessors<sup>14</sup>; but then the alternating cycle would have to cross two incident non-matching edges (from  $p$  to  $q$  and from  $q$  to  $r$ ), which is impossible. Thus,  $\pi$  contains a switching cycle.

To show the converse we will exhibit a right inverse to the map from alternating cycles to switching cycles defined above. Consider a switching cycle: it can be partitioned into directed paths from  $\mathbf{ax}$ -links to  $\otimes$ -links. Let  $l$  be an intermediate link in such a path, and  $e, p, s$  be matching edges corresponding respectively to  $l$ , its predecessor, and its successor in the directed path.  $s$  has a unique endpoint  $u$  which is incident to both endpoints of  $e$ ;  $e$  has a unique endpoint  $v$  which is *not* incident to both endpoints of  $p$ . To join  $e$  with  $s$ , we use the edge  $(u, v)$ . By taking all these non-matching edges for all maximal directed paths in the cycle, as well as a choice of two edges incident to each matching edge corresponding to an  $\mathbf{ax}$ -link, and the matching edges  $(a_l, b_l)$  corresponding to all the links  $l$  in the cycle, we get an alternating cycle.  $\square$

The situation was a bit nicer for RB-graphs, with an actual bijection between cycles (Proposition 3.6) unlike the case of graphifications. That said, the main technical advantages of the latter that we sought are summarized by the following properties.

**Lemma 5.5.** *Let  $\pi$  be a proof structure with graphification  $(G, M)$  and  $l$  be a link of  $\pi$  such that  $(a_l, b_l) \in M$  is a bridge of  $G$ . Then  $l$  is a terminal link in  $\pi$ , and if  $l$  is a  $\otimes$ -link, then removing  $l$  from  $\pi$  disconnects its predecessors.*

<sup>14</sup>To expand on this point: this is because we have prohibited vertex repetitions in our definition of cycles. This is legitimate since a graph is a forest if and only if it does not contain a non-vertex-repeating cycle.



*Proof.* Suppose for contradiction that  $l$  is not a terminal link, and let  $l'$  be a successor of  $l$ . Then for some endpoint  $v$  of  $(a_{l'}, b_{l'})$ ,  $(a_l, v)$  and  $(b_l, v)$  are both edges in  $G$ , and they make up a path between  $a_l$  and  $b_l$  not going through  $(a_l, b_l)$ . Thus,  $(a_l, b_l)$  cannot be a bridge.

The fact that  $(a_l, b_l)$  is a bridge means that by removing this edge,  $a_l$  and  $b_l$  are in different connected components; if  $l$  is a  $\otimes$ -link, each of these connected components contain the matching edge corresponding to one predecessor of  $l$ .  $\square$

**Theorem 5.6.** *Let  $\pi$  be a proof structure and  $(G, M)$  be its graphification. There is a bijection between the sequent calculus proofs corresponding to  $\pi$  (if any) and the sequentializations (i.e., the derivation trees for the inductive definition of Theorem 2.4) of  $(G, M)$  (if any), through which occurrences of Mix rules correspond to disjoint unions and conversely.*

This entails, in particular, the analogous property to Proposition 3.10 for graphifications.

*Proof.* We convert a sequentialization  $S$  of  $(G, M)$  into a sequentialization  $\Sigma$  of  $\pi$  inductively as follows. Since  $G \neq \emptyset$ , the last rule of  $S$  is either a disjoint union or the introduction of a bridge  $e = (a_l, b_l) \in M$  by joining together  $(G_a, M_a)$  and  $(G_b, M_b)$  with respective sequentializations  $S_a$  and  $S_b$ . In the latter case,  $l$  is a terminal link of  $\pi$ .

- If  $G_a = G_b = \emptyset$ , then  $l$  is an **ax**-link, and  $\Sigma$  consists of a single **ax**-rule.
- If  $G_a \neq \emptyset$  and  $G_b = \emptyset$ , then  $l$  is a  $\wp$ -link, and the removal of  $l$  from  $\pi$  yields a proof structure  $\pi'$  whose graphification is  $(G_a, M_a)$ .  $\Sigma$  then consists of a  $\wp$ -rule introducing  $l$  applied to the sequentialization of  $\pi'$  corresponding to  $S_a$ .
- If  $G_a \neq \emptyset$  and  $G_b \neq \emptyset$ , then  $l$  is a  $\otimes$ -link. Since  $e$  is a bridge, the removal of  $l$  from  $\pi$  yields two proof structures  $\pi_a$  and  $\pi_b$  whose respective graphifications are  $(G_a, M_a)$  and  $(G_b, M_b)$ .  $\Sigma$  then consists of an  $\otimes$ -rule applied to the translations of  $S_a$  and  $S_b$ .

If the last rule of  $S$  is a disjoint union rule, it is translated into a Mix rule in  $\Sigma$ .

The bijectivity can be proven by defining the inverse transformation and by checking that it is indeed its inverse.  $\square$

In particular,  $\pi$  is a MLL+Mix proof net if and only if  $(G, M)$  admits a sequentialization, that is, according to Theorem 2.4, if and only if  $M$  is the only perfect matching of  $G$ . Proposition 5.4 tells us that this is equivalent to  $\pi$  satisfying the Danos–Regnier acyclicity criterion. Therefore, this criterion characterizes MLL+Mix proof nets: as we wanted, we just proved the sequentialization theorem for MLL+Mix (Theorem 2.14).

**5.2. A sequentialization algorithm for MLL+Mix proof nets.** In Section 4.1, we saw how to decide MLL+Mix correctness in linear time, matching the known time complexity for MLL correctness. But the algorithms for MLL correctness still have an advantage: they can compute a sequentialization in linear time, whereas we only have a decision procedure for MIXCORR which returns a yes/no answer<sup>15</sup>. We do not know how to compute MLL+Mix sequentializations in linear time. Nevertheless, by applying our bridge between proof nets and graph theory, we get the first *quasi-linear* time algorithm for MIXSEQ. The beginning of the next section will discuss why the problem seems harder with Mix.

Our algorithm proceeds by first determining the root of the derivation tree and the link it introduces. To obtain the children of the root, it suffices to recurse on the connected components created by removing this link.

<sup>15</sup>It can find a switching cycle, witnessing incorrectness, but cannot produce a certificate of correctness.

Furthermore, through the correspondence of Theorem 5.6, finding a link which is introduced by the last rule of some sequentialization amounts to finding a bridge in the matching of the graphification of the proof net (*cf.* Section 5.1). This is in fact a bit more convenient with graphifications than with general unique perfect matchings, thanks to the following property:

**Lemma 5.7.** *All bridges in the graphification of some proof structure are matching edges.*

*Proof.* Let  $e$  be a non-matching edge. Then there are matching edges  $(u, v)$  and  $(s, t)$  such that the link corresponding to  $(u, v)$  is the predecessor of the one for  $(s, t)$ , and  $e = (u, s)$ . The non-matching edge  $(v, s)$  is then also present in the graph, and so  $e$  cannot be a bridge.  $\square$

The algorithm will alternate between finding and deleting bridges; a deletion may cut cycles and thus create new bridges, which we want to detect without traversing the entire graph each time. To do so, we use a *dynamic bridge-finding data structure* designed for this kind of use case by Holm et al. [HRT18]. It keeps an internal state corresponding to a graph, whose set of  $n$  vertices is immutable but whose set of edges may vary, and supports the following operations in  $O((\log n)^2(\log \log n)^2)$  amortized time:

- updating the graph by inserting or deleting an edge;
- computing the number of vertices of the connected component of a given vertex;
- finding a bridge in the connected component of a given vertex;
- determining whether two vertices are in the same connected component.

**Theorem 5.8.** *MIXSEQ can be solved in  $O(n(\log n)^2(\log \log n)^2)$  time.*

*Proof.* Let  $\pi$  be a MLL+Mix proof net with  $n$  links, and  $(G = (V, E), M)$  be its graphification. Both  $V$  and  $E$  have cardinality  $O(n)$  (in fact,  $|V| = 2n$  and  $|M| = n$ ).

The algorithm starts by initializing the bridge-finding data structure  $D$  with the graph  $G$ , computing the weakly connected components of  $\pi$  in linear time, and selecting a link in each component. On each selected link  $l$ , we call the following recursive procedure; its role is to sequentialize the sub-proof net of  $\pi$  containing  $l$  whose graphification is a current connected component of  $G$  ( $G$  and  $D$  being mutable global variables):

- Let  $u$  be one endpoint of the matching edge corresponding to  $l$ . Using the bridge-finding structure, find a bridge  $e = (v, w)$  in the component of  $u$ ; necessarily,  $e \in M$ . Remove the edge  $e$  from  $G$  (and reflect this change on  $D$  with a deletion operation).
- If both  $v$  and  $w$  are isolated vertices,  $e$  corresponds to an **ax**-link and the entire sub-proof net consisted of this link. In this case, return a sequentialization with a single **ax**-rule.
- If one of  $v$  and  $w$  is isolated, and the other is not — by symmetry, let us assume the latter is  $v$  — then  $e$  corresponds to a  $\wp$ -link  $l'$ . Let  $p$  and  $p'$  be its predecessors.
  - Remove all edges incident to  $v$ .
  - If the matching edges corresponding to  $p$  and  $p'$  are in the same connected component of  $G$ , recurse on  $p$ , add a final  $\wp$ -link and return the resulting sequentialization.
  - If  $p$  and  $p'$  are in different connected components of  $G$ , recurse on  $p$  and  $p'$ , use the results as the two premises of a Mix rule, add a final  $\wp$ -link and return the resulting sequentialization.
- If neither  $v$  nor  $w$  is isolated,  $e$  corresponds to a  $\otimes$ -link. This is handled similarly to the  $\wp$ +Mix case above.

Let us evaluate the time complexity. At each recursive call, one bridge is eliminated from  $G$ , so the number of recursive calls is  $n$ . The cost of each recursive call is  $O(1)$  except for

the updates and queries of the bridge-finding data structure. In total, there are  $|E| = O(n)$  deletions,  $|M| = n$  bridge queries, and at most  $n$  connectedness tests, and each of those takes  $O((\log n)^2(\log \log n)^2)$  amortized time. Hence the  $O(n(\log n)^2(\log \log n)^2)$  bound.  $\square$

**Remark 5.9.** If we want to compute a sequentialization for a unique perfect matching, in general, a complication is the existence of bridges which are not in the matching.

Interestingly, one can determine whether a bridge  $e$  is in  $M$  *without looking at  $M$* : it is the case if and only if both of the connected components created by removing  $e$  have an odd number of vertices. This leads to an algorithm for UNIQUEPM; it is virtually the same as the one proposed by Gabow et al. [GKT01, §2]<sup>16</sup>, from which we took our inspiration.

**Remark 5.10.** One needs to use a sparse representation for derivation trees: the size of a fully written-out sequent calculus proof is, in general, not linear in the size of its proof net.

## 6. ON THE KINGDOM ORDERING OF LINKS

One may wonder if we could not have just tweaked an algorithm for MLL sequentialization into an algorithm for MIXSEQ. In order to argue to the contrary, let us briefly mention a difference between Bellin and van de Wiele’s study of the sub-proof nets of MLL proof nets [BvdW95] and its extension to the MLL+Mix case by Bellin [Bel97]. Any MLL sub-proof net of a MLL proof net may appear in the sequentialization of the latter; however, for MLL+Mix, Figure 13 serves as a counterexample: the sub-proof structure containing all links but the  $\otimes$ -link is correct for MLL+Mix, but it cannot be an intermediate step in a sequentialization of the entire proof net. A *normality* condition is needed to distinguish those sub-proof nets which may appear in a sequentialization, and this is why sequentialization algorithms which are morally based on a greedy parsing strategy, such as Guerrini’s linear-time algorithm [Gue11], do not adapt well to the presence of the Mix rule.

Any link  $l$  in a MLL+Mix proof net  $\pi$  admits a minimum normal sub-proof net of  $\pi$  containing  $l$ , its *kingdom* [Bel97]. Bellin’s *kingdom ordering* is the partial order on links corresponding to the inclusion between kingdoms. We give an algorithm to compute this order for any MLL+Mix proof net: this is yet another application of matching theory. It uses a characterization of the kingdom ordering in terms of a relation called *dependency* by Bagnol et al. [BDS15] (who, in turn, take this name from the closely related *dependency graph* of Mogbil and Naurois [JdNM11]). We will also see how this dependency relation can be reformulated, through our correspondence between proof structures and perfect matchings, in terms of the *blossoms* mentioned in Section 2.2 and Section 4.1.

One may in fact define the kingdom ordering, written  $\ll_{\pi}$ , without reference to the notion of normal sub-proof net (we will not introduce the latter formally here):

**Definition 6.1.** Let  $\pi$  be a MLL+Mix proof net. For any two links  $p, q$  of  $\pi$ ,  $p \ll_{\pi} q$  if and only if, in any sequentialization of  $\pi$ , the rule introducing  $q$  has, among its premises, a proof net containing  $p$ .

From this point of view, the kingdom ordering gives us information about the set of all sequentializations. Let us give some examples. The proof net of Figure 10 admits a unique

<sup>16</sup>Not to be confused with their algorithm for UNIQUENESSPM [GKT01, §3] that we used in Section 4.1. They only claim a bound of  $O(m \log^4 n)$  because the best dynamic 2-edge-connectivity data structure known at the time has operations in  $O(\log^4 n)$  amortized time.

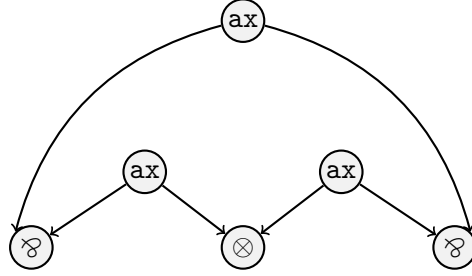


FIGURE 13. A MLL+Mix proof net which highlights a difficulty in solving MIXSEQ.

sequentialization, so this directly gives us the kingdom ordering: for instance the middle  $\otimes$ -link is the greatest element. On the other hand, in the proof net of Figure 13, both  $\otimes$ -links may be introduced by a last rule, so there is no greatest element. In fact, the kingdom ordering coincides with the predecessor relation. So it does not distinguish between the 3 terminal links even though, unlike the 2 others, the  $\otimes$ -link cannot be introduced last.

Before proceeding further, here is another property of MLL proof nets which is contradicted by Figure 13 for MLL+Mix proof nets, providing more evidence that MIXSEQ is trickier algorithmically than MLL sequentialization.

**Proposition 6.2.** *Let  $\pi$  be a MLL proof net and  $l$  be a maximal link for  $\ll_{\pi}$ . Then there exists a sequentialization of  $\pi$  whose last rule introduces  $l$ .*

*Proof.* If  $l$  is a terminal  $\otimes$ -link, no other assumption is needed for the existence of such a sequentialization. Else,  $l$  is a terminal  $\otimes$ -link and it suffices to show that  $l$  is *splitting*, i.e., that the removal of  $l$  splits  $\pi$  into two connected components.

Suppose that it is not the case, and consider some sequentialization of  $\pi$ : it must contain a  $\otimes$ -rule, applied to a sub-proof net  $\pi'$  for which  $l$  is splitting, which turns it into a sub-proof net for which  $l$  is not splitting anymore. Let  $p$  be the  $\otimes$ -link introduced by that rule; its predecessors lie in different connected components of  $\pi' \setminus \{l\}$ . Since  $\pi'$  is a MLL proof net, the predecessors of  $p$  are connected by a switching path in  $\pi'$ , which must cross  $l$ . This shows that  $l$  is a dependency of  $p$  in the sense of Definition 6.3, contradicting the maximality of  $l$ . (This only uses the fact that  $D(\pi) \subseteq \ll_{\pi}$ , which is the “easy” part of Bellin’s theorem.)  $\square$

### 6.1. Computing the kingdom ordering.

**Definition 6.3.** Let  $\pi$  be a proof structure. We write  $D(\pi)$  for the *dependency relation* defined as follows: for any two links  $p \neq q$  of  $\pi$ ,  $p$  is a *dependency of*  $q$  when  $q$  is a  $\otimes$ -link and there exists a switching path between the predecessors of  $q$  going through  $p$ .

For instance, in the proof net of Figure 10 (Section 3.2), the left  $\otimes$ -link depends on the left  $\otimes$ -link, but not on the other  $\otimes$ -links or  $\otimes$ -links; the middle  $\otimes$ -link has no dependency. In the case of Figure 13, the dependency relation is empty.

**Theorem 6.4** (Bellin [Bel97, Lemma 2]<sup>17</sup>). *Let  $\pi$  be a MLL+Mix proof net. The transitive closure of  $D(\pi) \cup S(\pi)$  is  $\ll_{\pi}$ , where  $(p, q) \in S(\pi)$  means that  $p$  is a predecessor of  $q$ .*

<sup>17</sup>This theorem was rediscovered by Bagnol et al. [BDS15, Theorem 11] in the special case of MLL proof nets without Mix (they refer to the kingdom ordering as the “order of introduction”). We borrow the notations  $D(\pi)$  and  $S(\pi)$  from them.

The dependency relation can be computed by reduction to a matching problem *in the case of MLL+Mix proof nets*: even though it is well-defined in arbitrary proof structures, we need MLL+Mix correctness to compute it, because our matching algorithm relies on the absence of alternating cycles. It is mostly a matter of applying a lemma from our paper [Ngu19]; since the latter has not been peer-reviewed as of the time of writing, we reproduce the proof in the appendix.

**Lemma 6.5** ([Ngu19] / Appendix A). *Let  $M$  be a matching of some graph  $G = (V, E)$ . Suppose that:*

- *there are no alternating cycles for  $M$  — equivalently,  $M$  is the unique perfect matching of the subgraph induced by the vertices matched by  $M$ ;*
- *there are exactly two unmatched vertices  $u, v$ .*

*Then the existence of an alternating path for  $M$  with endpoints  $u, v$  and crossing a prescribed matching edge  $e \in M$  can be reduced in  $\text{AC}^0$  to the existence of a perfect matching; furthermore, such a path can be found in linear time.*

**Remark 6.6.** An alternating path between unmatched vertices is often called an *augmenting path*; combinatorial maximum matching algorithms generally work by iteratively searching for augmenting paths, see, *e.g.*, [Tar83, Chapter 9].

**Theorem 6.7.** *Let  $\pi$  be a MLL+Mix proof net with a link  $p$  and a  $\wp$ -link  $q$ . Deciding whether  $(p, q) \in D(\pi)$  can be done in linear time, in randomized NC and in quasiNC.*

*Proof.* A degenerate case is when  $p$  is a predecessor of  $q$ : in this case,  $p$  depending on  $q$  is equivalent to  $\pi$  becoming incorrect if  $q$  is turned into a  $\otimes$ -link, and thus the complexity is the same as that of (the complement of) the correctness problem.

When  $p$  is not a predecessor of  $q$ , the definition of dependency translates into the problem defined in the above lemma by taking the graphification of  $\pi$ , and removing the matching edge corresponding to  $q$ . The endpoints of this edge then become unmatched, and we choose as prescribed intermediate edge the matching edge corresponding to  $p$ . The fact that  $\pi$  is a proof net ensures that the acyclicity assumption of Lemma 6.5 is satisfied.

We directly obtain the linear time complexity, and since the existence of a perfect matching can be decided in randomized NC or quasiNC (*cf.* Section 2.2), so can our problem.  $\square$

A transitive closure can be computed in polynomial time, and reachability in a directed graph can be decided in  $\text{NL} \subset \text{quasiNC}$ , so we get in the end:

**Corollary 6.8.** *There are a polynomial-time algorithm and a quasiNC algorithm to compute the kingdom ordering  $\ll_{\pi}$  of any MLL+Mix proof net  $\pi$ .*

**6.2. Dependencies and blossoms in unique perfect matchings.** We will now see how, through the correspondence of Section 3, Bellin’s theorem can be rephrased as a statement on unique perfect matchings.

**Definition 6.9.** Let  $G$  be a graph and  $M$  be a perfect matching of  $G$ . A *blossom* for  $M$  is a cycle whose vertices are all matched within the cycle, except for one, its *root*. The matching edge incident to the root is called the *stem* of the blossom.

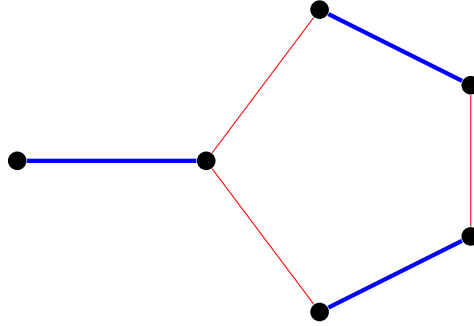


FIGURE 14. A blossom of length 5, with its stem on the left.

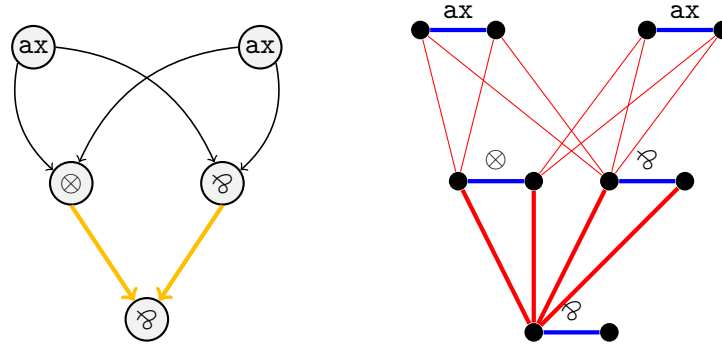


FIGURE 15. The proof net of Figure 2 and its graphification (*cf.* Figure 11b); the directed edges of the proof net correspond to blossoms of length 3 in its graphification.

That is, a blossom consists of an alternating path between two vertices, starting and ending with a matching edge, together with a non-matching edge from the root to each of these two vertices. See Figure 14 for an illustration; as another example, in Figure 1b, the two triangles are blossoms with a common stem. The stem of a blossom is not part of the cycle. Blossoms are central to combinatorial matching algorithms, *e.g.*, [Edm65, GKT01], as we have previously mentioned.

**Definition 6.10.** When  $e \in M$  is in some blossom with stem  $f \in M$ , we write  $e \rightarrow f$ .

This is the graph-theoretical counterpart of the dependency relation, as is shown by the following two propositions.

**Proposition 6.11.** *Let  $\pi$  be a MLL+Mix proof net and  $(G, M)$  be its graphification. Let  $p, q$  be links in  $\pi$  with corresponding matching edges  $e_p, e_q \in M$ . Then  $e_p \rightarrow e_q$  if and only if  $p$  is a dependency of  $q$  or a predecessor of  $q$ , i.e.,  $(p, q) \in D(\pi) \cup S(\pi)$ .*

Both the cases  $(p, q) \in S(\pi)$  and  $(p, q) \in D(\pi)$  occur in the proof net of Figure 2, see respectively Figure 15 and Figure 16.

*Proof.* If  $(p, q) \in S(\pi)$ , then by construction there exists a blossom of length 3 containing  $p$  with stem  $q$ . If  $(p, q) \in D(\pi)$ , then for the same reason as Proposition 5.4, we can get, from the switching path between the predecessors of  $q$  visiting  $p$ , an alternating path for  $M$  starting and ending with the edges corresponding to those predecessors and crossing the

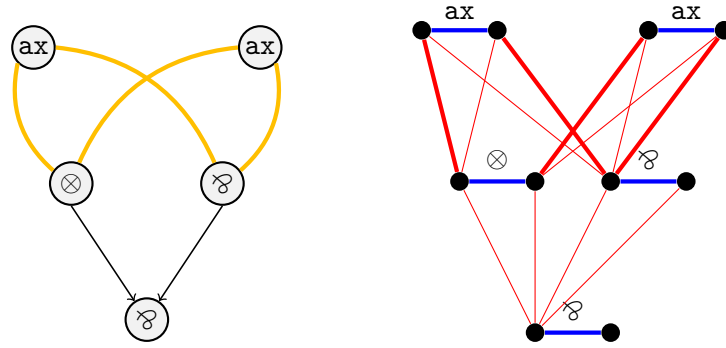


FIGURE 16. A blossom of length 7 corresponding to a dependency. The yellow cycle is not a switching cycle, but should be seen as a switching path between both predecessors of the  $\wp$ -link.

edge corresponding to  $p$ . By adding two non-matching edges to the same endpoint of the matching edge for  $q$ , we get a blossom with stem  $q$ .

Conversely, let  $q$  be a link,  $e$  the corresponding matching edge, and  $B$  be a blossom with stem  $q$ . Let us first note that if  $B$  contains a non-matching edge joining  $e$  with the matching edge corresponding to a successor of  $q$ , then by replacing this non-matching edge with its twin incident to the other endpoint of  $q$ , we get an alternating cycle; this is impossible because we have assumed  $\pi$  to be a MLL+Mix proof net. Therefore, the first and last matching edges in  $B$  are both predecessors of  $q$ . If they are the same — that is, if  $B$  has length 3 and contains a single matching edge — then this edge corresponds to a predecessor  $p$  of  $q$ . Otherwise,  $B$  gives an alternating path between two distinct predecessors of  $q$ ; necessarily  $q$  is a  $\wp$ -link (otherwise, there would be an alternating cycle), and all links corresponding to matching edges in  $B$  are dependencies of  $q$ .  $\square$

**Proposition 6.12.** *Let  $G$  be a graph,  $M$  be a perfect matching of  $G$  and  $\pi$  be the proofification of  $(G, M)$ . Let  $e, f \in M$  with corresponding  $\otimes$ -links  $l_e, l_f \in M$ . Then  $e \rightarrow f$  if and only if  $l_e$  is a dependency of some  $\wp$ -link  $q$  from which  $l_f$  is reachable (by a directed path).*

*Proof.* Let  $B$  be a blossom with stem  $f$ , whose two non-matching edges incident to  $f$  are  $a$  and  $b$ .  $B$  translates into a switching path between  $\mathbf{ax}_a$  and  $\mathbf{ax}_b$  in  $\pi$ . Now,  $\mathbf{ax}_a$  and  $\mathbf{ax}_b$  are also leaves of a binary tree of  $\wp$ -links whose root has the single successor  $l_f$ ; by taking  $q$  to be the lowest common ancestor of  $\mathbf{ax}_a$  and  $\mathbf{ax}_b$  in this tree,  $l_f$  is reachable from  $q$ , and every link in the path between  $\mathbf{ax}_a$  and  $\mathbf{ax}_b$  depends on  $q$ . Conversely, any switching path between the two predecessors of a  $\wp$ -link corresponds to a blossom for  $M$  in  $G$ .  $\square$

**Remark 6.13.** In Proposition 6.11, the “if” direction holds even for incorrect proof structures; in Proposition 6.12, note that no uniqueness property is required of the perfect matching.

Thus, we see that Bellin’s theorem is equivalent to the following theorem where  $\rightarrow^+$  is the transitive closure of  $\rightarrow$ .

**Theorem 6.14.** *Let  $G$  be a graph with a unique perfect matching  $M$ , and  $e, f \in M$ . The edge  $e$  occurs before  $f$  in all sequentializations for  $M$  if and only if  $e \rightarrow^+ f$ .*

For instance, in Figure 1b, the middle edge  $e$  is the only bridge, and it is the stem of the two triangular blossoms which contain the other matching edges.

This graph-theoretic version is somewhat simpler to state than the original theorem: one takes the transitive closure of a single relation, instead of a union of two unrelated relations. And as far as we know, this is a new result in graph theory. We have included it in the companion paper [Ngu19], aimed at a broader audience of graph theorists, where we present a direct combinatorial proof with no mention of proof nets.

## 7. A RECONSTRUCTION OF RB-GRAPHS VIA FORBIDDEN TRANSITIONS

In this section, we come back to Retoré’s RB-graphs (Section 3.1) and factorize Retoré’s correctness criterion (Corollary 3.7) as a composition of:

- the Danos–Regnier correctness graph (Definition 2.13);
- a reduction to the UNIQUENESSPM problem for a general notion of constrained cycles, namely *closed trails avoiding forbidden transitions*.

We introduced the latter in [Ngu19], but here the logical order of exposition is the reverse of the order of discovery: it was by attempting to understand Retoré’s RB-graphs that we found this reduction.

**Definition 7.1** [Sze03]. Let  $G = (V, E)$  be a graph. A *transition graph* for a vertex  $v \in V$  is a graph whose vertices are the edges incident to  $v$ :  $T(v) = (\partial(v), E_v)$ . A *transition system* on  $G$  is a family  $T = (T(v))_{v \in V}$  of transition graphs.

A graph equipped with a transition system is called a *graph with forbidden transitions*.

A path  $v_1, e_1, v_2, \dots, e_{k-1}, v_k$  is said to be *compatible* if for  $i = 1, \dots, k-1$ ,  $e_i$  and  $e_{i+1}$  are adjacent in  $T(v_{i+1})$ . For a *cycle*, we also require  $e_{k-1}$  and  $e_1$  to be adjacent in  $T(v_1) = T(v_k)$ . (So the edges of  $T(v)$  actually specify the *allowed* transitions.)

**Remark 7.2.** By “transition” we mean a pair of consecutive edges in a path/cycle. A transition system could equivalently be specified by literally giving the set of forbidden transitions, i.e., of edge pairs that cannot occur consecutively. This generalizes paired graphs (Definition 2.11) by dropping the disjointness requirement on pairs: switching graphs do not make sense anymore, but switching cycles (generalized to compatible cycles) still do.

Finding a compatible path is proved to be NP-complete in [Sze03]. As in the case of alternating paths in matchings (cf. Remark 4.3), the difficulty is in the interaction of a local constraint — any transition (pair of consecutive edges) must be allowed — and a global one, namely the fact there must be no repeated vertices. Indeed, recall from Section 2.1 that by definition, paths and cycles cannot repeat vertices twice. This is important to ensure that Berge’s lemma for alternating cycles (Lemma 2.2) holds. Following the terminology of [BJG09, §1.4], let us introduce a relaxation of this global condition.

**Definition 7.3.** A *trail* (resp. *closed trail*) is a “path” (resp. “cycle”) in which we allow vertex repetitions, but *edge repetitions are prohibited*. Compatible trails and compatible closed trails in a graph with forbidden transitions are defined analogously to the above definition.

**Remark 7.4.** For perfect matchings, an alternating cycle is the same as an alternating closed trail: repeating a vertex would imply repeating its unique matching edge. However, this is not true for general graphs with forbidden transitions: see Figure 17a for an example with compatible closed trails, but no compatible cycles.

The relevance of this notion is that for compatible *trails*, we showed the problem to be tractable [Ngu19] by using an “edge-colored line graph” construction. This construction



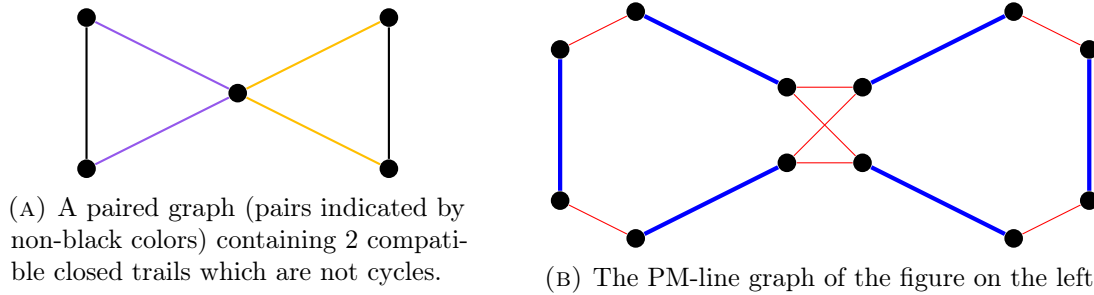


FIGURE 17. A graph with forbidden transitions and its PM-line graph.

has other uses but, in the case of compatible (closed) trails, it can be replaced by a version using perfect matchings that we define below — which in fact is the edge-colored line graph composed with a previously known reduction, see [Ngu19] for details. All this arguably goes to show that the objects which we manipulate are not contrived to fit with RB-graphs: they arise naturally from other considerations.

**Definition 7.5.** Let  $G$  be a graph and  $T$  be a transition system on  $G$ . The *PM-line graph*  $L_{PM}(G, T)$  is defined as the graph:

- with vertex set  $\{u_e \mid e \in E, u \text{ is an endpoint of } e\}$ ;
- with edge set  $M \sqcup E'$ , where

$$M = \{(u_e, v_e) \mid e = (u, v) \in E\} \quad E' = \{(u_e, u_f) \mid u \in V, e, f \in \partial(u) \text{ are adjacent in } T(u)\}$$

- equipped with the perfect matching  $M$ .

**Proposition 7.6** [Ngu19]. *Closed trails of length  $k$  in  $G$  compatible with  $T$  correspond bijectively to alternating cycles of length  $2k$  in  $L_{PM}(G, T)$ .*

An example is given by Figure 17b: it contains two alternating cycles corresponding to the compatible closed trails of Figure 17a.

Finally, we relate the PM-line graph construction to RB-graphs.

**Proposition 7.7.** *Let  $\pi$  be a proof structure with conclusions (Definition 3.2) and  $C(\pi)$  its correctness graph (adapting Definition 2.13 to handle conclusion vertices/edges). Let  $T$  be the transition system corresponding to the paired edges of  $C(\pi)$ .*

*Then  $L_{PM}(C(\pi), T)$  is exactly the RB-graph for  $\pi$ .*

*Proof.* Immediate by comparing Figure 7 with Definition 7.5. □

The moral of the story is that the actual function of RB-graphs is to detect *compatible closed trails*. It turns out that for the correctness graphs of proof structures, this is the same as switching cycles, but as Figure 17a shows this is not true in general. The particularity of correctness graphs that entails this equivalence is that if a vertex is incident to two edges that are paired together, then it is incident to at most one unpaired edge (which corresponds to the outgoing edge of a  $\wp$  link in the proof structure).

## 8. CONCLUSION

We have presented a correspondence between proof nets and perfect matchings, and demonstrated its usefulness through several applications of graph theory to linear logic: our results give the best known complexity for MLL+Mix correctness and sequentialization, by taking advantage of sophisticated graph algorithms. Beyond that, we have also contextualized this correctness problem as a member of a family of equivalent constrained cycle-finding problems in graphs, and used this to shed some light on earlier work on proof nets. These connections also have some benefits for graph theory, as the rephrasing of Bellin’s theorem and our discovery of the “PM-line graph” construction illustrate; this is what we attempt to demonstrate in the companion paper [Ngu19]. In general, we hope to see fruitful interactions arise between those two domains.

**8.1. Further hardness results: pomset logic and visible acyclicity.** To take advantage of this connection, one can peruse the literature on graphs to look for results with potential applications to proof nets. For instance, there is a NP-hardness result for a certain constrained path-finding problem on arc-colored *directed graphs* [GLMM13]. From this, we deduced in [Ngu19] that finding an alternating circuit — for a certain notion of perfect matching in a directed graph — is NP-hard. In other words, the absence of alternating circuits — one possible generalization of the UNIQUENESSPM problem to directed graphs (for which Berge’s lemma doesn’t hold) — is coNP-hard.

It turns out that circuits (i.e., directed cycles) also appear in the study of proof nets:

- Retoré’s *pomset logic* [Ret97] is a conservative extension of MLL+Mix with a self-dual non-commutative connective  $\triangleleft$ . The extension of the Danos–Regnier correctness criterion to pomset logic proof nets allows both premises of a  $\triangleleft$ -link to be traversed consecutively by a “switching cycle”, but *only if the left premise is taken before the right one*: the direction of the cycle therefore becomes relevant. In [Ngu20], we show that *the correctness problem for pomset logic is coNP-complete*<sup>18</sup>, by adapting our proofification construction to take directed graphs as input. A direct proof of the NP-hardness of the directed alternating cycle problem is also provided in [Ngu20].
- The *visible acyclicity* condition was first introduced by Pagani for as a relaxation of the usual correctness criterion for MELL+Mix (by MELL we mean Multiplicative-Exponential Linear Logic) proof structures [Pag06]; it was later extended to differential interaction nets [Pag12]. It is defined as the absence of certain “visible cycles”, which become directed when exponential boxes are present. One can show that visible acyclicity is coNP-hard (a result that we first announced at the DICE 2018 workshop) by imitation of the proof for pomset logic. However, we do not know whether it is in coNP.

Interestingly, both pomset logic correctness and visible acyclicity were motivated by semantic considerations: they are necessary and sufficient conditions for the soundness of the denotation of proof structures in coherence spaces.

---

<sup>18</sup>This contradicts (assuming that  $P \neq NP$ ) the polynomial time claim of [Ret97, Proposition 5], whose purported proof relies on a “standard breadth search algorithm” to find an alternating path for a perfect matching in a digraph. Remark 4.3 explains the subtle issue with this argument.

A similar mistake appears in Hughes’s paper on combinatorial proofs: he claims that a “simple breadth-first search” [Hug06, Footnote 3] can determine, in linear time, some condition that amounts to the correctness of a MLL+Mix proof structure. In that case, the mistake is harmless, thanks to our Theorem 4.1.

**8.2. Open questions.** Now that we have shed a new light on MLL+Mix proof nets, it would be interesting to revisit the well-studied theory of MLL proof nets. Therefore, we would like to find the right graph-theoretical counterpart to the connectedness condition in the Danos–Regnier criterion for MLL. The goal would be to extract the combinatorial essence of the statics of MLL proof structures, *forgetting about logic*; without having to handle the dynamics (cut-elimination), one could hope to distill some simpler combinatorial object, in the same way that perfect matchings are simpler than MLL+Mix proof structures.

But unique perfect matchings do not seem to be the right setting to do so; and one year after the conference version of this paper, despite the connections described here with, *e.g.*, forbidden transitions, we still have not found a natural graph-theoretic decision problem equivalent to correctness for MLL without Mix. (As far as naturality is concerned, perfect matchings set a high bar, given their importance in discrete mathematics!)

Here by “equivalent” we mean, in particular, through low-complexity reductions (hopefully computable both in linear time and in  $\text{AC}^0$ ). Though the NL-completeness of MLL correctness means that it is equivalent to directed reachability, Mogbil and Naurois’s correctness criterion [JdNM11] uses a subroutine for connectivity in undirected forests, a L-complete problem, in its reduction. A related question is to understand why all known linear-time correctness criteria for MLL — including the one presented here — rely on the same sophisticated data structure, as mentioned in Remark 4.3. (Namely, “incremental tree set union”: a restricted union-find data structure with  $O(1)$  amortized operations.)

In the same vein, the present paper does not treat at all — except for the short Remark 4.4 — the *contractibility* criterion introduced by Danos [Dan90], despite its importance in recent developments in proof nets (*e.g.*, [HH16, BH18]). It is also part of the divide between MLL and MLL+Mix proof nets: contractibility, reformulated as graph parsing, underlies a linear-time sequentialization algorithm for MLL [Gue11], while no such algorithm is known for MLL+Mix. Aside from the obvious question of sequentializing MLL+Mix nets in linear time, looking for a mainstream graph-theoretic account of contractibility is also of interest.

Another question<sup>19</sup> would be to give a graph-theoretic account of the notion of *empire* in proof nets, similarly to our treatment of kingdoms in Section 6. Empires were used in Girard’s original proof of the first correctness criterion (the so-called “long trip” criterion) [Gir87]; while the kingdom of a link  $l$  in a MLL+Mix proof net is the minimum normal subnet having  $l$  as a conclusion, the empire of  $l$  is, dually, the maximum such subnet. To achieve this goal, the obvious place to start would be the characterization of empires in proof nets given in [Bel97, Lemma 3] using certain paths (“chains”) in proof nets.

**8.3. Other variants of proof nets through the lens of graph theory.** We gather here miscellaneous ideas on extending the graph-theoretic viewpoint beyond MLL+Mix, that we have not had the time to pursue further. Any assertion that we make below should therefore be seen as purely speculative.

**8.3.1. Jumps and quantifiers.** We have argued that our graphification construction (Section 5.1) faithfully reflects the intrinsic order of logical rules in a proof net. It should therefore be possible to incorporate *jumps*, which are a way to prescribe sequentiality constraints on proof nets. By doing so, one would extend our results to MLL+Mix with (first-order or second-order) quantifiers  $\forall/\exists$ : the technology of jumps was first introduced to handle proof

<sup>19</sup>This was suggested to the author by Gianluigi Bellin.

nets with quantifiers [Gir91]. This treatment should also accommodate more general uses of jumps such as [DGF08].

8.3.2. *Essential nets.* Larmarche’s *essential nets* for *intuitionistic* MLL admit a correctness criterion formulated using a standard notion on graphs, namely the *domination* between vertices in a control flow graph. This is at the heart of Murawski and Ong’s linear time algorithm for MLL correctness [MO06]. So it would be interesting, in view of the aforementioned goal of understanding why the “incremental tree set union” data structure of [GT85] seems necessary to decide MLL correctness in linear time (it occurs in the computation of a “dominator tree” in [MO06]), to compare this domination criterion with the criteria based on unique perfect matchings.

A first remark is that, via a classical correspondence between directed graphs and graphs equipped with *bipartite* perfect matchings, the essential net obtained from a MLL proof structure by the reduction of [MO06] (the so-called “trip translation”) can be identified with a maximal bipartite subgraph of its RB-graph. The missing piece is to understand whether this is an instance of a purely graph-theoretic reduction from the domination condition to the UNIQUENESSPM problem.

#### ACKNOWLEDGMENTS

This work started as a side project during an internship in the Operations Research team at the Laboratoire d’Informatique de Paris 6, supervised by Christoph Dürr, who taught the author the expressive power of perfect matchings; this paper would not exist without him. Thanks also to Kenji Maillard, Michele Pagani, Marc Bagnol, Antoine Amarilli, Alexis Saurin, Stefano Guerrini and Virgile Mogbil for discussions, references and encouragements, and to Thomas Seiller for his writing advice on the initial conference version.

We are also grateful to the anonymous reviewers for their useful and detailed feedback on previous versions of this paper.

#### REFERENCES

- [Bar92] David A. Mix Barrington. Quasipolynomial size circuit classes. In *[1992] Proceedings of the Seventh Annual Structure in Complexity Theory Conference*, pages 86–93, June 1992.
- [BDS15] Marc Bagnol, Amina Doumane, and Alexis Saurin. On the dependencies of logical rules. In *FOSSACS, 18th International Conference on Foundations of Software Science and Computation Structures*, London, United Kingdom, April 2015.
- [Bel97] Gianluigi Bellin. Subnets of proof-nets in multiplicative linear logic with MIX. *Mathematical Structures in Computer Science*, 7(6):663–669, December 1997.
- [Ber57] Claude Berge. Two Theorems in Graph Theory. *Proceedings of the National Academy of Sciences*, 43(9):842–844, September 1957.
- [BH18] Gianluigi Bellin and Willem B. Heijltjes. Proof Nets for Bi-Intuitionistic Linear Logic. In Hélène Kirchner, editor, *3rd International Conference on Formal Structures for Computation and Deduction (FSCD 2018)*, volume 108 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 10:1–10:18, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- [BJG09] Jørgen Bang-Jensen and Gregory Gutin. *Digraphs. Theory, algorithms and applications*. 2nd ed. London: Springer, 2nd ed. edition, 2009.
- [BvdW95] Gianluigi Bellin and Jacques van de Wiele. Subnets of Proof-nets in MLL-. In *Proceedings of the Workshop on Advances in Linear Logic*, pages 249–270, New York, NY, USA, 1995. Cambridge University Press.

- [CSV84] Ashok K. Chandra, Larry Stockmeyer, and Uzi Vishkin. Constant depth reducibility. *SIAM Journal on Computing*, 13(2):423–439, May 1984.
- [Dan90] Vincent Danos. *La Logique Linéaire appliquée à l'étude de divers processus de normalisation (principalement du Lambda-calcul)*. PhD thesis, Université Paris-Diderot – Paris VII, 1990.
- [DGF08] Paolo Di Giamberardino and Claudia Faggian. Proof nets sequentialisation in multiplicative linear logic. *Annals of Pure and Applied Logic*, 155(3):173–182, October 2008.
- [DR89] Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Archive for Mathematical Logic*, 28(3):181–203, 1989.
- [Edm65] Jack Edmonds. Paths, trees, and flowers. *Canadian Journal of Mathematics*, 17(0):449–467, January 1965.
- [FR94] Arnaud Fleury and Christian Retoré. The mix rule. *Mathematical Structures in Computer Science*, 4(2):273–285, 1994.
- [Gir87] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50(1):1–101, January 1987.
- [Gir91] Jean-Yves Girard. Quantifiers in Linear Logic II. In Corsi and Sambin, editors, *Nuovi problemi della logica e della filosofia della scienza*, pages 79–90, Bologna, 1991. CLUEB.
- [GKT01] Harold N. Gabow, Haim Kaplan, and Robert E. Tarjan. Unique maximum matching algorithms. *Journal of Algorithms*, 40(2):159–183, August 2001.
- [GLMM13] Laurent Gourvès, Adria Lyra, Carlos A. Martinhon, and Jérôme Monnot. Complexity of trails, paths and circuits in arc-colored digraphs. *Discrete Applied Mathematics*, 161(6):819–828, April 2013.
- [GT85] Harold N. Gabow and Robert Endre Tarjan. A linear-time algorithm for a special case of disjoint set union. *Journal of Computer and System Sciences*, 30(2):209–221, April 1985.
- [Gue11] Stefano Guerrini. A linear algorithm for MLL proof net correctness and sequentialization. *Theoretical Computer Science*, 412(20):1958–1978, April 2011.
- [HH16] Dominic Hughes and Willem Heijltjes. Conflict nets: Efficient locally canonical MALL proof nets. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), 2016*, pages 437–446, New York, U. S. A., July 2016. ACM.
- [HMT06] Thanh Minh Hoang, Meena Mahajan, and Thomas Thierauf. On the bipartite unique perfect matching problem. In *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part I*, pages 453–464, 2006.
- [HRT18] Jacob Holm, Eva Rotenberg, and Mikkel Thorup. Dynamic bridge-finding in  $\tilde{O}(\log^2 n)$  amortized time. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2018)*, pages 35–52. Society for Industrial and Applied Mathematics, January 2018.
- [Hug06] Dominic J.D. Hughes. Proofs Without Syntax. *Annals of Mathematics*, 143(3):1065–1076, November 2006.
- [Jac65] Carl Gustav Jacob Jacobi. De investigando ordine systematis aequationum differentialium vulgarium cujuscunque. *Journal für die reine und angewandte Mathematik*, (64):297–320, 1865.
- [JdNM11] Paulin Jacobé de Naurois and Virgile Mogbil. Correctness of linear logic proof structures is NL-complete. *Theoretical Computer Science*, 412(20):pp. 1941–1957, April 2011.
- [JO09] Carl Gustav Jacob Jacobi and François Ollivier. Looking for the order of a system of arbitrary ordinary differential equations. De investigando ordine systematis aequationum differentialium vulgarium cujuscunque. *Applicable Algebra in Engineering, Communication and Computing*, 20(1):7–32, 2009.
- [Kot59] Anton Kotzig. Z teórie konečných grafov s lineárnym faktorom. II. *Matematicko-fyzikálny časopis*, 09(3):136–159, 1959.
- [KVV85] Dexter Kozen, Umesh V. Vazirani, and Vijay V. Vazirani. NC algorithms for comparability graphs, interval graphs, and testing for unique perfect matching. In *Foundations of Software Technology and Theoretical Computer Science, Fifth Conference, New Delhi, India, December 16-18, 1985, Proceedings*, pages 496–503, 1985.
- [Lov79] László Lovász. On determinants, matchings, and random algorithms. In *Fundamentals of Computation Theory*, pages 565–574, 1979.
- [MO06] Andrzej S. Murawski and C.-H. Luke Ong. Fast verification of MLL proof nets via IMLL. *ACM Transactions on Computational Logic*, 7(3):473–498, July 2006.
- [MVV87] Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987.

- [Ngu19] Lê Thành Dũng Nguyễn. Constrained path-finding and structure from acyclicity. *CoRR*, abs/1901.07028, 2019.
- [Ngu20] Lê Thành Dũng Nguyễn. Complexity of correctness for pomset logic proof nets. *CoRR*, abs/1912.10606, 2020.
- [Pag06] Michele Pagani. Acyclicity and coherence in multiplicative and exponential linear logic. In Pierre-Louis Curien, editor, *Proceedings of the Twentieth International Workshop on Computer Science Logic*, volume 4207 of *Lecture Notes in Computer Science*, pages 531–545, Szeged, Hungary, 2006. Springer.
- [Pag12] Michele Pagani. Visible acyclic differential nets, Part I: Semantics. *Annals of Pure and Applied Logic*, 163(3):238–265, 2012.
- [Ret93] Christian Retoré. *Réseaux et séquents ordonnés*. PhD thesis, Université Paris-Diderot - Paris VII, February 1993.
- [Ret96] Christian Retoré. Perfect matchings and series-parallel graphs: multiplicatives proof nets as R&B-graphs: [Extended Abstract]. *Electronic Notes in Theoretical Computer Science*, 3(Supplement C):167–182, January 1996.
- [Ret97] Christian Retoré. Pomset logic: A non-commutative extension of classical linear logic. In Gerhard Goos, Juris Hartmanis, Jan Leeuwen, Philippe Groote, and J. Roger Hindley, editors, *Typed Lambda Calculi and Applications*, volume 1210, pages 300–318. Springer Berlin Heidelberg, Berlin, Heidelberg, 1997.
- [Ret99] Christian Retoré. Handsome proof-nets: R&B-graphs, perfect matchings and series-parallel graphs. Research Report 3652, INRIA, March 1999.
- [Ret03] Christian Retoré. Handsome proof-nets: perfect matchings and cographs. *Theoretical Computer Science*, 294(3):473–488, February 2003.
- [RV89] Michael O. Rabin and Vijay V. Vazirani. Maximum matchings in general graphs through randomization. *Journal of Algorithms*, 10(4):557–567, December 1989.
- [ST17] Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-NC. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 696–707. IEEE Computer Society, 2017.
- [Str06] Lutz Straßburger. Proof Nets and the Identity of Proofs. Research Report 6013, INRIA, October 2006.
- [Sze03] Stefan Szeider. Finding paths in graphs avoiding forbidden transitions. *Discrete Applied Mathematics*, 126(2-3):261–273, 2003.
- [Sze04] Stefan Szeider. On theorems equivalent with Kotzig’s result on graphs with unique 1-factors. *Ars Combinatoria*, 73:53–64, 2004.
- [Tar83] Robert Endre Tarjan. *Data Structures and Network Algorithms*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1983.

## APPENDIX A. PROOF OF LEMMA 6.5

We rely on a version of Berge’s lemma (Lemma 2.2) for paths:

**Lemma A.1** (Berge [Ber57]). *Let  $G$  be a graph and  $M$  be a matching of  $G$ . If  $P$  is an augmenting path for  $M$  — i.e., an alternating path whose endpoints are unmatched — then  $M \Delta P$  is a matching and  $|M \Delta P| = |M| + 1$ . (Thus, adding  $P$  “augments”  $M$ , hence the name.) Conversely, if  $M$  is a matching with  $|M'| > |M|$ , then  $M \Delta M'$  is a vertex-disjoint union of:*

- $|M'| - |M|$  augmenting paths for  $M$ ;
- some (possibly zero) cycles which are alternating for both  $M$  and  $M'$ .

Let  $u, v \in V$  be the unmatched vertices. If there is an augmenting path for  $M$  in  $G$ , its endpoints must be  $u$  and  $v$ , and this is equivalent to the existence of a perfect matching in  $G$ . Let  $e = (a, b)$ ,  $G' = (V, E \setminus \{e\})$  and  $M' = M \setminus \{e\}$ .

Suppose  $G'$  admits a perfect matching  $M''$ . Then the symmetric difference  $M' \Delta M''$  consists of two vertex-disjoint alternating paths for  $M'$  whose endpoints are  $\{u, v, a, b\}$ , by Berge's lemma for paths; indeed, our assumptions prevent the existence of alternating cycles for  $M$ , and therefore for  $M' \subset M$  as well.

We claim that these paths either go from  $u$  to  $a$  and  $b$  to  $v$ , or from  $u$  to  $b$  and  $a$  to  $v$ . Otherwise, there would be an alternating path from  $a$  to  $b$  for  $M'$  in  $G'$ , and together with  $(a, b) = e \in M$ , this would give us an alternating cycle for  $M$  in  $G$ .

In both cases, let us join the two paths together by adding  $e$ . We get a path starting with  $u$ , ending with  $v$ , crossing  $e$  and alternating for  $M$  in  $G$ . Conversely, from such a path, one can get a perfect matching in  $G'$ .

It is clear that the reduction is in  $AC^0$ . For the linear time complexity, we exploit the fact that we already have at our disposal a matching  $M'$  of  $G'$  which leaves only 4 vertices unmatched. A perfect matching can then be found as follows: find a first augmenting path  $P$  for  $M'$  in linear time, and then a second one  $P'$  for  $M' \Delta P$ , both steps being done in linear time (using a similar (but simpler) algorithm than for `UNIQUENESSPM`, see [GT85] and [Tar83, Section 9.4]). If both augmenting paths exist, then  $M \Delta P \Delta P'$  is a perfect matching, and conversely, if  $G'$  admits a perfect matching, then the procedure succeeds in finding some  $P$  and  $P'$ . (This does not mean that  $P$  and  $P'$  are the same as the paths in the previous part of the proof, since they may not be vertex-disjoint.)