Rewriting with Linear Inferences in Propositional Logic

Anupam Das

Department of Computer Science
University of Bath
Bath, UK
a.das@bath.ac.uk

Abstract

Linear inferences are sound implications of propositional logic where each variable appears exactly once in the premiss and conclusion. We consider a specific set of these inferences, MS, first studied by Straßburger, corresponding to the logical rules in deep inference proof theory. Despite previous results characterising the individual rules of MS, we show that there is no polynomial-time characterisation of MS, assuming that integers cannot be factorised in polynomial time.

We also examine the length of rewrite paths in an extended system MSU that also has unit equations, utilising a notion dubbed *trivialisation* to reduce the case with units to the case without, amongst other observations on MS-rewriting and the set of linear inferences in general.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases proof theory, propositional logic, complexity of proofs, deep inference

Digital Object Identifier 10.4230/LIPIcs.RTA.2013.158

1 Introduction

Linear inferences are sound implications of propositional logic where the same variables occur in the premiss and conclusion, and occur exactly once in both. For example,

$$A \wedge B \to A \vee B \quad \text{and} \quad A \wedge (B \vee C) \to (A \wedge B) \vee C$$

The left implication is usually known as *mix*, while the right is logically equivalent to $\wedge, \vee$ introduction rules in Gentzen calculi, and is also known as *switch*. While these two rules have traditionally been at the core of proof theory, the advent of *deep inference* proof theory has triggered the study of an additional rule, *medial*:

$$(A \wedge B) \vee (C \wedge D) \to (A \vee C) \wedge (B \vee D)$$

The motivation to consider such a rule is to obtain *locality* for the contraction rule in proofs, an impossible task in traditional Gentzen systems [2]. In recent years there has been much work on understanding the role of medial in proofs and logic [4] [15] [5] [18]. Most recently, Straßburger commenced a study of it from the point of view of rewriting theory [17].

In proof theory we are interested in derivations from one formula to another, under some set of inference rules. In deep inference these rules operate on formulae as in a rewriting system, i.e. they may be applied anywhere in the formula, not just at the root connective. Two typical questions a proof theorist might ask are the following:

1. Is there a derivation from a formula A to a formula B?
2. What is the complexity of a derivation from A to B?

24th International Conference on Rewriting Techniques and Applications (RTA'13).
Editor: Femke van Raamsdonk; pp. 158–173
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In deep inference systems derivations can be considered as rewrite paths by the inference rules, and in this work we ask these questions particularly for the switch-medial fragment.

In [17] Straßburger considered (1) and gave polynomial-time characterisations of switch and medial individually in terms of *relation webs*, graphs that record certain logical information about a formula. An open problem arising from the work was whether a similar characterisation could be given for the combined switch-medial system. In this work we answer this question negatively, if such a characterisation is to decide (1) in polynomial-time, conditional on the assumption that integer factoring cannot be computed by polynomial-size circuits. Along the way we (essentially) show that proof-search in Frege systems (and so also Gentzen/deep inference systems with cut [5]) can be reduced in polynomial time to the search for switch-medial rewrite paths between formulae, suggesting that a lot of the computational content of deep inference proofs lies in this switch-medial fragment.

With regards to (2), it is well-known that switch-medial derivations have polynomial size, in the absence of units. However this does not remain true when units are added, as is common for deep inference proof systems, even after quotienting the set of formulae by unit-equivalences. We exhibit a specific example of this in Sect. 4.1 where we present a derivation using units that contains exponentially many logically distinct formulae. We show that such derivations can only occur when a variable is *trivialised*, i.e. put in disjunction with $\top$ or conjunction with $\bot$, and give a transformation from any switch-medial derivation with units to one of polynomial-size with same premiss and conclusion.

While this is beyond the scope of the current work, the results given have certain consequences for *atomic flows*, diagrams recording structural changes in a proof [11] [9], essentially a type of trace for rewriting derivations. We do not introduce them here, but will briefly comment on these consequences as remarks in this work.

Finally we consider the set of all linear inferences. From the previous results it can be shown that switch and medial are insufficient to derive every linear inference, assuming $\boldsymbol{coNP} \neq \boldsymbol{NP}$. Straßburger gives an explicit linear inference in [19] on 36 variables that cannot be derived, the smallest known thusfar. We improve this result by constructing a linear inference on 10 variables that cannot be derived by switch and medial, even in the presence of units, and conjecture that this is the minimal such inference.

Since this work is primarily motivated by proof theory, we adopt the notational convention presented in [10] for deep inference proofs or, equivalently, rewriting derivations. The main purpose of this work is to better understand the complexity of the logical fragment of deep inference systems, specifically in answering the two questions above.

Acknowledgements

I would like to thank Lutz Straßburger, Alvin Šipraga and Alessio Guglielmi for all the helpful discussions on this work, and also the anonymous referees for their thorough reviews.

2 Preliminaries

The language of propositional logic consists of countably many atoms a, b, etc. and their duals $\bar{a}, \bar{b}$ etc., units $\top, \bot$ and the connectives $\wedge, \vee$, with their usual interpretations. We also have formula variables, or simply variables, denoted A, B, etc. Terms are defined as follows:

$$t ::= \quad a \quad | \quad A \quad | \quad \top \quad | \quad \bot \quad | \quad (t \wedge t) \quad | \quad [t \vee t]$$

The distinction between brackets $(,)$ and $[,]$ is purely a notational convenience to aid the reader distinguish conjunctions from disjuntions.

Ground terms, i.e. terms free of variables, are called *formulae*, and are denoted α, β etc.

▶ Remark (Negation). Note that we have no symbol for negation in our language. Instead atoms come in pairs with their duals and we can express all of propositional logic using the De Morgan laws to push negation to the atoms.

Consequently all contexts (defined below) are positive, and so the soundness of an inference rule is preserved by applying it anywhere in a term.

▶ **Definition 1** (Contexts). A *context* is a term with a hole, denoted $\{\ \}$, occurring in place of a subterm. We write $\xi\{t\}$ to denote the result of substituting the term t for the hole in $\xi\{\ \}$. Contexts can also have multiple holes, e.g. $\xi\{\ \}\cdots\{\ \}$, defined in the natural way.

We identify inference rules with term rewriting rules, and derivations with rewrite paths. Derivations are considered as objects in proof theory, sometimes themselves subject to rewriting, and so it will be convenient to adopt a notation that allows for this. The notation described below was introduced in [10] as a proof formalism, *open deduction*, but can be thought of as just a convenient notation for term rewriting.

▶ **Definition 2.** Let $\mathcal{R}$ be a term rewriting system for propositional logic, i.e. a set of rewrite rules on terms of propositional logic. We write $\begin{array}{c} s \\ \|\mathcal{R} \\ t \end{array}$ to denote an $\mathcal{R}$-derivation from a term s to a term t, defined as follows:

- $\rho \frac{s}{t}$ is an $\mathcal{R}$-derivation from s to t, if $s \to t$ is an instance of a rule $\rho : l \to r$ in $\mathcal{R}$.[1]
- $\left(\begin{array}{ccc} s & & t \\ \|\mathcal{R} & \star & \|\mathcal{R} \\ s' & & t' \end{array}\right)$ is an $\mathcal{R}$-derivation from $(s \star t)$ to $(s' \star t')$, for $\star \in \{\wedge, \vee\}$.
- $\begin{array}{c} s \\ \|\mathcal{R} \\ t \\ \|\mathcal{R} \\ u \end{array}$ is an $\mathcal{R}$-derivation from s to u.

All rewriting rules operate modulo associativity and commutativity of $\vee, \wedge$ in the usual way. For this reason we often exclude internal brackets of a formula.

Sometimes, if two terms s, t are considered equivalent up to some relation, e.g. associativity and commutativity, we may aid the reader by adding a 'fake' rewrite step: $\begin{array}{c} s \\ \cdots\cdots \\ t \end{array}$.

▶ **Definition 3.** A term is *linear* if no variable occurs more than once. A *(sound) linear inference* is a sound[2] rewrite rule $\rho : l \to r$ where l and r are linear terms on the same variables. We define L as the set of all (sound) linear inferences.

▶ **Definition 4.** We define the system MS to consist of the following rules,

$$\mathsf{M} : \quad (A \wedge B) \vee (C \wedge D) \to [A \vee C] \wedge [B \vee D] \quad , \quad \mathsf{S} : \quad A \wedge [B \vee C] \to (A \wedge B) \vee C$$

The system U consists of rules for both directions of the following equations:

$$A \vee \bot = A \quad , \quad A \wedge \top = A \quad , \quad \bot \wedge \bot = \bot \quad , \quad \top \vee \top = \top$$

The system MSU is defined as $\mathsf{MS} \cup \mathsf{U}$.

---

[1] Note in particular that this is a one-step shallow rewrite step.
[2] A rule is sound if every substitution of formulae for formula variables is sound in propositional logic.

3 Complexity of characterising MS

The motivation behind this section originates from the following result in [17].

▶ **Theorem 5** (Straßburger). *There are polynomial-time criteria deciding whether there is a* S *or* M *rewrite path between two terms.*

In the same work the task of characterising MS was raised as an open problem.

In this section we give a polynomial-time reduction from the problem of finding a Frege proof[3] of a given tautology to the problem of finding a MS-rewrite path between two formulae. Consequently, we deduce that there is no polynomial-time characterisation of MS (and also MSU) under the assumption that integers factoring is outside $P/poly$.

Throughout this section we deal with formulae (i.e. ground terms), which are the natural objects of proof theory, rather than generic terms.

3.1 Reducing proof-search to rewriting in MS

We utilise some results from previous work that is beyond the scope of this paper, and so we state them with references but give no proofs. In particular, we refer to a specific deep inference system KSg, on which more can be found in [3],[5].

▶ Notation. For a formula α let $\alpha^n := \overbrace{\alpha \wedge \cdots \wedge \alpha}^{n}$ and $n \cdot \alpha := \overbrace{\alpha \vee \cdots \vee \alpha}^{n}$.

▶ **Proposition 6** (Jeřábek). *A Frege or Gentzen proof (with cut) of a formula τ can be polynomially transformed to a* KSg*-proof of $\tau \vee (a_1 \wedge \bar{a}_1) \vee \cdots \vee (a_n \wedge \bar{a}_n)$, where a_i are the atoms occurring in τ, and vice-versa.*

Proof. See e.g. [13], [8]. ◀

▶ **Proposition 7.** *A* KSg*-proof of a formula τ can be polynomially transformed to a derivation of the following shape,*

$$\begin{array}{c} \bigwedge_i a_i \vee \bar{a}_i \vee \beta_i \\ \| \, \mathsf{MS} \\ \tau' \end{array}$$

where τ' differs from τ only by replacing some atom occurrences a by a disjunction $n \cdot a$.

Proof. See e.g. [3], [7]. ◀

▶ **Lemma 8.** *Given a formula $\bigwedge_i a_i \vee \bar{a}_i \vee \beta_i$ there is a polynomial-size derivation of the following form,*

$$\begin{array}{c} \alpha \\ \| \, \mathsf{S} \\ \bigwedge_i k_i \cdot a_i \vee k_i \cdot \bar{a}_i \vee \beta_i \end{array}$$

where α is a valid formula in conjunctive normal form, for some k_i.

[3] A Frege proof is a sequence of formulae where each line follows from some previous lines under modus ponens (from α and $\alpha \supset \beta$ infer β) or is drawn from some complete set of axioms.

Proof. Freely apply the inverse of S to each β_i to obtain a formula β_i' of same size in conjunctive normal form, with disjunctions $\beta_{i1}', \dots, \beta_{ik}'$. Construct the following derivations as required:

$$\begin{array}{c} [a_i \vee \bar{a}_i \vee \beta_{i1}'] \wedge \cdots \wedge [a_i \vee \bar{a}_i \vee \beta_{ik}'] \\ \Big\| \mathsf{S} \\ \left[k \cdot a_i \vee k \cdot \bar{a}_i \vee \begin{array}{c} \beta_i' \\ \| \mathsf{S} \\ \beta_i \end{array} \right] \end{array}$$

Validity follows since each disjunction at the top contains a pair of dual atoms. ◀

▶ **Lemma 9.** *Let α be a valid formula in conjunctive normal form, with at least two conjuncts, such that each atom occurs as many times as its dual. Then there is a polynomial-size derivation of the following shape:*

$$\begin{array}{c} \bigwedge_i a_i \vee \bar{a}_i \\ \Big\| \mathsf{MS} \\ \alpha \end{array}$$

Proof. Since α is valid each of its disjunctions must contain a pair of dual atoms. If there are two such pairs in some disjunction then build the following derivation:

$$\begin{array}{c} 2\cdot\mathsf{S} \dfrac{[a \vee \bar{a}] \wedge [\beta \vee \gamma] \wedge \left[b \vee \bar{b} \vee \alpha\right]}{\mathsf{M} \dfrac{([a \vee \bar{a}] \wedge \beta) \vee \left(\gamma \wedge \left[b \vee \bar{b}\right]\right)}{\left[a \vee \bar{a} \vee b \vee \bar{b} \vee \alpha\right] \wedge [\beta \vee \gamma]}} \end{array}$$

Read bottom-up, the number of pairs of dual atoms in the same disjunction has reduced and validity has been preserved, so we can repeatedly apply this construction until there are no disjunctions with two pairs of dual atoms.

Now each disjunction has exactly one pair of dual atoms, so match each other atom in a disjunction with an occurrence of its dual in another disjunction; the matching is bijective by the given condition.

We build the following derivation:

$$\begin{array}{c} 2\cdot\mathsf{S} \dfrac{\alpha \wedge \beta \wedge [a \vee \bar{a}]}{\mathsf{M} \dfrac{(\alpha \wedge \bar{a}) \vee (\beta \wedge a)}{[\alpha \vee a] \wedge (\beta \wedge \bar{a})}} \end{array}$$

Read bottom-up, if a and $\bar{a}$ are a matching pair, the total number of matching pairs in distinct disjunctions has reduced and validity has been preserved, so we can repeatedly apply this construction to obtain a derivation of the required form. ◀

▶ **Theorem 10.** *A Frege proof of a formula τ can be polynomially transformed to a derivation of the following form,*

$$\begin{array}{c} \bigwedge_i [a_i \vee \bar{a}_i]^{n_i} \\ \Big\| \mathsf{MS} \\ \tau' \end{array}$$

where τ' is obtained from $\sigma = \tau \vee (a_1 \wedge \bar{a}_1) \vee \cdots \vee (a_n \wedge \bar{a}_n)$, where a_i are the atoms occurring in τ, by replacing each atom occurrence a_i by $k \cdot m_i \cdot a_i$, where m_i is the number of occurrences of $\bar{a}_i$ in σ, k is some fixed global constant and n_i is determined by m_i and k by linearity of MS*, and similarly for dual atoms.*

Proof sketch. Follows from Props. 6, 7 and Lemmata 8, 9, under suitable substitution of disjunctions $l \cdot a$ for an atom a everywhere in a MS-derivation. ◀

▶ **Corollary 11.** *Verifying the validity of a tautology τ can be reduced to determining the existence of a* MS*-rewrite path between two formulae in time polynomial in the size of the smallest Frege proof of τ.*

Proof. The premiss and conclusion of the derivations in Thm. 10 are governed by a single parameter, k. We simply run any algorithm that determines the existence of a MS-rewrite path between two formulae on the premiss and conclusion determined by each value of k, from 1 upwards, until it returns. ◀

▶ Remark. The above results could have equivalently been obtained for MSU, rather than MS, with similar proofs.

3.2 No polynomial-time characterisation for MS

By the corollary above, any polynomial-time characterisation of MS would yield an algorithm verifying any tautology in time polynomial in the size of its smallest Frege proof. The existence of such an algorithm for a proof system, known as *weak automatisability*, was proved to be impossible for Frege systems in [1], conditional on the assumption that integer factoring is outside $P/poly$.

▶ **Definition 12.** A proof system P is *weakly automatisable* if there is a procedure verifying the validity of any tautology τ in time polynomial in the size of the smallest P-proof of τ.

▶ **Theorem 13** (Bonet et al.)**.** *If integer factoring is outside $P/poly$ then Frege is not weakly automatisable.*

▶ **Corollary 14.** *If integer factoring is outside $P/poly$ then there is no polynomial-time characterisation of* MS*.*

▶ Remark. With slight modifications, it follows from the results in this section that atomic flows do not form a proof system, in the sense that they cannot be verified in polynomial-time, unless integer factoring is in $P/poly$. This (conditionally) refutes a conjecture of Guglielmi that atomic flows form a proof system [9].

4 Length of paths with units

In this section we address the complexity of rewriting paths in MSU. The length of MS-paths is well-known to be polynomial, and we give a simple proof below that the length is at most cubic in the size of an input term. Much tighter bounds can be obtained, and this is the subject of ongoing work by Bruscoli, Guglielmi and Straßburger.[4]

It should be pointed out that the general belief that units do not contribute to the complexity of a proof is commonplace in the deep inference community, with some results

[4] Personal correspondence.

as folklore, for example the theorem below. Nonetheless, the technicalities of proving this belief, or even formalising what this means, seems nontrivial to the author and this sentiment is communicated via numerous examples.

▶ **Theorem 15.** MS *has only polynomial-length paths.*

Proof. Let $n(t)$ denote the number of $\wedge$s occurring in a term t, and let $m(t)$ denote the number of pairs of leaves in the term-tree of t whose least common connective is $\wedge$. Clearly each medial step reduces the n-value of a term and each switch step reduces the m-value of a term, while not changing the n-value.

Let M denote the product measure $n \times m : t \mapsto (n(t), m(t))$, then each step of an MS-derivation strictly reduces M. But n is linear in the size of a term and m is quadratic, so an MS-derivation can only contain a cubic number of steps. ◀

The situation becomes more complicated when units are considered. Since the rules of U are bidirectional, cycles can be trivially constructed, yielding infinite rewrite paths. Moreover non-cyclic infinite 'increasing' paths can be constructed:

$$a \quad \to \quad \top \wedge a \quad \to \quad \top \wedge \top \wedge a \quad \to \quad \top \wedge \top \wedge \top \wedge a \quad \to \quad \cdots$$

One approach here would be to conduct rewriting modulo the equational theory generated by U, i.e. consider formulae equivalent up to U-rewriting.[5]

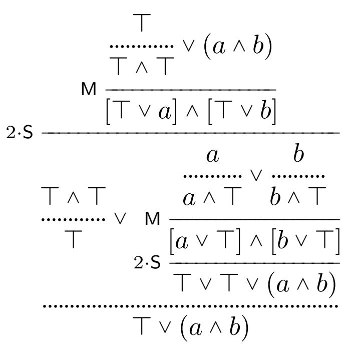
▶ **Definition 16** (Rewriting modulo)**.** Let $\mathcal{R}$ be a rewriting system and $\sim$ an equivalence relation on the terms of $\mathcal{R}$. A derivation in $\mathcal{R}/\sim$ is a sequence,

$$s \sim s_1 \to t_1 \sim s_2 \to t_2 \sim \cdots \to t_k \sim t$$

where each $s_i \to t_i$ is a one-step rewrite in $\mathcal{R}$ and $s_i \not\sim t_i$.

We should note that this is a nonstandard definition of rewriting modulo, since we enforce that each rewriting step is between $\sim$-distinct terms. This condition crucially affects termination of a system, but makes sense in the current setting since the equivalence relations induced by our equations can be checked efficiently.

In any case this approach does not quite work here, since we can still construct cycles when rewriting modulo U. For example the following,



is a derivation for a cycle $\top \vee (a \wedge b) \to \cdots \to \top \vee a \vee b \to \cdots \to \top \vee (a \wedge b)$.

[5] We will not address here complexity issues arising from such an approach. There are ways to present such rewritings such that each step can still be checked efficiently [5].

These situations only occur when a subterm appears in conjunction with $\bot$ or disjunction with $\top$, a concept we later define as *trivialisation*. They can be avoided by adding to U the following 'non-linear' equations:

$$A \vee \top = \top \qquad A \wedge \bot = \bot$$

Let us call the resulting system U′. We state the following results, whose proofs appear elsewhere and are not difficult to reconstruct.

▶ **Proposition 17.** *Every term is* U′*-equivalent to a unique unit-free term or* $\top$ *or* $\bot$*.*

Proof. See e.g. [7]. ◀

▶ **Proposition 18.** *If two unit-free formulae are distinct, modulo associativity and commutativity, with each atom occurring at most once, then they compute distinct boolean functions.*

Proof. See e.g. [12]. ◀

From these we can deduce the strong normalisation property.

▶ **Corollary 19.** *Rewriting in* MS/U′ *is terminating.*

Proof. Assume the input is a formula (i.e. a ground term) without loss of generality, since MS and U′ do not distinguish between atoms and variables. By Props. 17 and 18 it follows that, for each step $\alpha \to \beta$ in a MS/U′ derivation, α and β compute distinct boolean functions.

There are 2^n assignments on n atoms, and each boolean function determines a unique set of these assignments. Since rewriting in MS/U′ preserves logical implication, any rewrite path determines a strictly decreasing sequence of sets of assignments with respect to $\subset$. ◀

Notice that the complexity bound on termination above is exponential, unlike the unit-free case which is polynomial. Perhaps surprisingly, one cannot do better than this, and we prove this by constructing explicit rewrite-paths of exponential length.

4.1 An exponential-length path in MS/U′

We present a new class of rules, collectively known as *supermix*, that are derivable in MSU and show that one can construct exponential-length paths with it, with exponentially many U′-distinct formulae occurring.

▶ **Definition 20** (Supermix). We define the supermix rules, indexed by n, below:

$$\mathsf{smix} \quad : \quad A \vee \bigwedge_{i=1}^{n} B_i \quad \to \quad A \wedge \bigvee_{i=1}^{n} B_i$$

Each supermix rule is clearly a sound linear inference and, for the special case when $n = 1$, it coincides with the usual mix rule.

The following results aim to prove that supermix is derivable in MSU.

▶ **Lemma 21.** *There is a rewrite path from* $\bot$ *to* $\top$ *in both* M/U *and* S/U*.*

Proof.

$$\mathsf{M}\,\dfrac{\dfrac{\bot}{(\bot \wedge \top) \vee (\bot \wedge \top)}}{\dfrac{[\bot \vee \top] \wedge [\bot \vee \top]}{\top}} \quad , \quad \mathsf{S}\,\dfrac{\dfrac{\bot}{\bot \wedge [\bot \vee \top]}}{\dfrac{(\bot \wedge \bot) \vee \top}{\top}}$$

◀

We will simply write $\frac{\bot}{\top}$ if we do not mind which rules are used.

▶ **Lemma 22.** *There is a* MS/U *derivation from* $\bigvee_{i=1}^{n} B_i$ *to* $\top \vee \bigwedge_{i=1}^{n} B_i$.

Proof. We proceed by induction on n.

Base Case: by Lemma 21 we have $\frac{\bot}{\top} \vee B$.

Inductive Step: Suppose there are such derivations Φ_r for $r < n$. Define:

$$\Phi_n \quad := \quad \text{2·S}\ \dfrac{\text{M}\ \dfrac{\dfrac{B_n}{\top \wedge B_n} \vee \dfrac{\begin{array}{c}\bigvee_{i=1}^{n-1} B_i \\ \Phi_{n-1} \Big\Vert \text{MSU} \\ \top \vee \bigwedge_{i=1}^{n-1} B_i\end{array}}{\top \wedge \left[\top \vee \bigwedge_{i=1}^{n-1} B_i\right]}}{[\top \vee B_n] \wedge \left[\top \vee \top \vee \bigwedge_{i=1}^{n-1} B_i\right]}}{\dfrac{\top \vee \top \vee \top}{\top} \vee \left(B_n \wedge \bigwedge_{i=1}^{n-1} B_i\right)}$$

◀

▶ **Theorem 23.** *Supermix is derivable in* MS/U.

Proof. Let Φ_n be the derivations constructed in Lemma 22. The derivation is as follows:

$$\text{S}\ \dfrac{A \wedge \begin{array}{c}\bigvee_{i=1}^{n} B_i \\ \Phi_n \Big\Vert \text{MSU} \\ \top \vee \bigwedge_{i=1}^{n} B_i\end{array}}{\dfrac{A \wedge \top}{A} \vee \bigwedge_{i=1}^{n} B_i}$$

◀

Note that the premiss and conclusion of a supermix step are distinct modulo U′, since they are unit-free and compute distinct boolean functions, and so we can construct an exponential-length path in MS/U′ as follows:

$$\Lambda_1 := a_1 \qquad , \qquad \Lambda_{n+1} := \quad \text{smix}\ \dfrac{\begin{array}{c}\bigwedge_{i=1}^{n} a_i \\ a_{n+1} \wedge \Lambda_n \Big\Vert \text{smix} \\ \bigvee_{i=1}^{n} a_i\end{array}}{\begin{array}{c}\bigwedge_{i=1}^{n} a_i \\ a_{n+1} \vee \Lambda_n \Big\Vert \text{smix} \\ \bigvee_{i=1}^{n} a_i\end{array}}$$

4.2 Construction of polynomial-length paths

The cause of problems in (complexity of) termination of MSU seems to be the trivialising of atoms and variables in a derivation, by putting them in disjunction with $\top$ or conjunction with $\bot$. We define this property formally in this section and show that, although there are paths of exponential length, any two terms with a MSU-path between them has one of polynomial length. The general idea is to 'push' trivialised atoms and variables to one side and reduce to the unit-free case, before reintroducing the trivialised symbols.

Throughout this section we use 'dotted' steps $\begin{array}{c} s \\ \cdots \\ t \end{array}$ to denote U-steps in a derivation, to help distinguish MS-steps from U-steps. This is technically an overloading of notation, but does not cause any problem since there is a polynomial-size MSU-derivation from s to t just if there is a polynomial-size MS/U-derivation from s to t.

▶ **Definition 24** (Trivialisation). A term is *trivial* if it is a disjunction containing $\top$ or a conjunction containing $\bot$. In a derivation we say that an atom or variable is *trivialised* if at any point it occurs inside a trivial subterm.

▶ **Proposition 25.** *There are polynomial-size derivations* $\begin{array}{c} \xi\{A\} \\ \| \mathsf{SU} \\ A \vee \xi\{\bot\} \end{array}$, $\begin{array}{c} A \wedge \xi\{\top\} \\ \| \mathsf{SU} \\ \xi\{A\} \end{array}$.

Proof. See e.g. [3], [16], [13]. The proof is similar to that of Lemma 27. ◀

▶ **Lemma 26.** *Let* $\begin{array}{c} \xi\{A\} \\ \| \mathsf{MSU} \\ \zeta\{A\} \end{array}$ *be a derivation where* A *is trivialised. Then there is a derivation* $\begin{array}{c} \xi\{\top \vee A\} \\ \| \mathsf{MSU} \\ \zeta\{\bot \wedge A\} \end{array}$ *whose size is at most polynomial in the size of the former derivation.*

Proof. There are two cases. In the first case we transform the derivation as follows,

$$
\begin{array}{c} \xi\{A\} \\ \Phi \| \mathsf{MSU} \\ \eta\{\top \vee \zeta\{A\}\} \\ \Psi \| \mathsf{MSU} \\ \xi'\{A\} \end{array}
\quad \to \quad
\begin{array}{c} \xi\{\top \vee A\} \\ \Phi' \| \mathsf{MSU} \\
\eta \left\{ \begin{array}{c} \top \vee \zeta \left\{ \begin{array}{c} \top \vee \mathsf{s} \dfrac{\begin{array}{c} A \\ \cdots\cdots \\ [\top \vee \bot] \wedge A \end{array}}{\top \vee (\bot \wedge A)} \\ \cdots\cdots\cdots\cdots \\ \top \vee (\bot \wedge A) \end{array} \right\} \\ \bullet \| \mathsf{S} \\ \top \vee \zeta\{\bot \wedge A\} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \top \vee \zeta\{\bot \wedge A\} \end{array} \right\} \\
\Psi' \| \mathsf{MSU} \\ \xi'\{\bot \wedge A\} \end{array}
$$

where Φ', Ψ' are obtained by substituting $\top \vee A$, $\bot \wedge A$ resp. everywhere for A, and the derivation marked $\bullet$ is obtained by Prop. 25. In the second case we transform the derivation as follows,

$$
\begin{array}{c} \xi\{A\} \\ \Phi \Big\Vert \mathsf{MSU} \\ \eta\{\bot \wedge \zeta\{A\}\} \\ \Psi \Big\Vert \mathsf{MSU} \\ \xi'\{A\} \end{array}
\quad \to \quad
\begin{array}{c}
\xi\{\top \vee A\} \\
\Phi' \Big\Vert \mathsf{MSU} \\
\eta\left\{ \begin{array}{c}
\mathsf{2{\cdot}S}\dfrac{\dfrac{\bot}{\bot \wedge \bot} \wedge \zeta\left\{ \begin{array}{c} \top \vee \mathsf{S}\dfrac{\dfrac{A}{[\top \vee \bot] \wedge A}}{\top \vee (\bot \wedge A)} \\ \hline \top \vee (\bot \wedge A) \end{array} \right\} \\ \bullet \Vert \mathsf{S} \\ \top \vee \zeta\{\bot \wedge A\}}{\dfrac{(\bot \wedge \top) \vee (\bot \wedge \zeta\{A\})}{\bot \wedge \zeta\{\bot \wedge A\}}}
\end{array} \right\} \\
\Psi' \Big\Vert \mathsf{MSU} \\
\zeta\{\bot \wedge A\}
\end{array}
$$

where Φ', Ψ' are obtained by substituting $\top \vee A$, $\bot \wedge A$ resp. everywhere for A, and the derivation marked $\bullet$ is obtained by Prop. 25. ◀

▶ **Lemma 27.** *There are polynomial-size derivations* $\begin{array}{c} (\bot \wedge A) \vee \xi\{\bot\} \\ \Vert \mathsf{MU} \\ \xi\{\bot \wedge A\} \end{array}$, $\begin{array}{c} \xi\{\top \vee A\} \\ \Vert \mathsf{MU} \\ [\top \vee A] \wedge \xi\{\top\} \end{array}$.

Proof. We proceed by induction on the depth of the hole in $\xi\{\ \}$. The base cases are trivial, and we give the inductive steps for the first derivation below,

$$
\begin{array}{c}
\mathsf{M}\dfrac{\left(\dfrac{\bot}{\bot \wedge \bot} \wedge A\right) \vee (\xi\{\bot\} \wedge B)}{\begin{array}{c}(\bot \wedge A) \vee \xi\{\bot\} \\ IH \Big\Vert \mathsf{M} \\ \xi\{\bot \wedge A\}\end{array} \wedge \dfrac{\bot \vee B}{B}}
\end{array}
\quad , \quad
\begin{array}{c}
\dfrac{(\bot \wedge A) \vee [\xi\{\bot\} \vee B]}{(\bot \wedge A) \vee \xi\{\bot\} \vee B} \\
IH \Big\Vert \mathsf{M} \\
\xi\{\bot \wedge A\}
\end{array}
$$

where derivations marked IH are obtained by the inductive hypothesis. The second derivation is obtained by duality of the inference rules. ◀

▶ **Lemma 28.** *Every* MSU*-derivation where no atoms or variables occur trivialised can be transformed into an* MS*-derivation with* U*-equivalent premiss and conclusion.*

Proof. We simply reduce every line in the derivation to a unit-free term by U. Since no atoms or variables are trivialised we do not need any rules of $\mathsf{U}' \setminus \mathsf{U}$. We rewrite derivations using the four possible cases below, any other combination of rules with units results in some term in either the premiss or conclusion being trivialised.

$$
\mathsf{S}\frac{s \wedge [\bot \vee t]}{(s \wedge t) \vee \bot} \quad \to \quad s \wedge t \qquad\qquad \mathsf{S}\frac{\top \wedge [s \vee t]}{(\top \wedge s) \vee t} \quad \to \quad s \vee t
$$

$$
\mathsf{M}\frac{(s \wedge t) \vee (\bot \wedge \bot)}{[s \vee \bot] \wedge [t \vee \bot]} \quad \to \quad s \wedge t \qquad\qquad \mathsf{M}\frac{(s \wedge \top) \vee (t \wedge \top)}{[s \vee t] \wedge [\top \vee \top]} \quad \to \quad s \vee t
$$

In particular these rewrite rules operate *anywhere* in a derivation. ◀

▶ **Theorem 29.** *Every* MSU*-derivation can be transformed to one with same premiss and conclusion and whose size is polynomial in the size of its premiss and conclusion.*

Proof. Let Φ be an MSU-derivation. If there are no trivialisations then transform it into an MS-derivation by Lemma 28 which must be of polynomial size by Thm. 15.

Otherwise assume there is a trivialised variable in Φ, say A_1, and transform Φ as follows:

$$\begin{array}{c} \xi\{A_1\} \\ \Phi \Big\| \mathsf{MSU} \\ \zeta\{A_1\} \end{array} \quad \to \quad \begin{array}{c} \xi\{\top \vee A_1\} \\ \Phi' \Big\| \mathsf{MSU} \\ \zeta\{\bot \wedge A_1\} \end{array} \quad \to \quad \begin{array}{c} \xi\{\top \vee \bot\} \\ \Phi_1 \Big\| \mathsf{MSU} \\ \zeta\{\bot \wedge \bot\} \end{array}$$

where Φ' is obtained from Φ by Lemma 26 and Φ_1 from Φ' by substituting $\bot$ for every instance of A_1.

Now do the same for Φ_1, and repeat this process until either there are no trivialisations in some Φ_k. (Note that it is not sufficient to just do all the trivialised variables at once, since the transformation above may result in new trivialisations.)

Now by Lemma 28 we can transform Φ_k to an MS-derivation Ψ, with same premiss and conclusion modulo U, which we assume to have polynomial size by Thm. 15.

$$\begin{array}{c} \xi\{\top \vee \bot\} \cdots \{\top \vee \bot\} \\ \Phi_k \Big\| \mathsf{MSU} \\ \zeta\{\bot \wedge \bot\} \cdots \{\bot \wedge \bot\} \end{array} \quad \to \quad \begin{array}{c} \xi\{\top \vee \bot\} \cdots \{\top \vee \bot\} \\ \hdashline s \\ \Psi \| \mathsf{MS} \\ t \\ \hdashline \zeta\{\bot \wedge \bot\} \cdots \{\bot \wedge \bot\} \end{array}$$

The complete transformation is as follows,

$$\begin{array}{c} \xi\{A_1\} \cdots \{A_k\} \\ \Phi \Big\| \mathsf{MSU} \\ \zeta\{A_1\} \cdots \{A_k\} \end{array} \quad \to \quad \begin{array}{c} \xi \left\{ \mathsf{s} \dfrac{\dfrac{A_1}{[\top \vee \bot] \wedge A_1}}{\top \vee (\bot \wedge A_1)} \right\} \cdots \left\{ \mathsf{s} \dfrac{\dfrac{A_k}{[\top \vee \bot] \wedge A_k}}{\top \vee (\bot \wedge A_k)} \right\} \\ \circ \Big\| \mathsf{S} \\ \left[\begin{array}{c} \xi\{\top \vee \bot\} \cdots \{\top \vee \bot\} \\ \hdashline s \\ \Psi \| \mathsf{MS} \\ t \\ \hdashline \zeta\{\bot \wedge \bot\} \cdots \{\bot \wedge \bot\} \end{array} \vee (\bot \wedge A_1) \vee \cdots \vee (\bot \wedge A_k) \right] \\ \bullet \Big\| \mathsf{M} \\ \zeta \left\{ \dfrac{\dfrac{\bot}{\top} \wedge A_1}{A_1} \right\} \cdots \left\{ \dfrac{\dfrac{\bot}{\top} \wedge A_k}{A_k} \right\} \end{array}$$

where the derivations marked $\circ, \bullet$ are obtained by repeatedly applying Lemma 27. ◀

▶ Remark. By the above theorem it follows that any derivation can be transformed to one with the same premiss and conclusion, the same atomic flow and whose size is polynomial in the size of its atomic flow. This is tacitly assumed in some papers where the complexity of proofs is controlled by atomic flows, e.g. [6], [8], albeit never in a critical way.

5 The system L of all linear inferences

In the previous sections we considered the specific rules S and M, due to their importance in proof theory, in particular deep inference. However there are infinitely many other inferences one could consider, and there is good reason to analyse the set of all linear inferences, from the point of view of complexity, due to the following result by Straßburger.

▶ **Proposition 30** (Straßburger)**.** L *is* $\boldsymbol{coNP}$*-complete.*

In this section we present two observations, first on a small linear inference not derivable in MSU, and second an extension of the notion of trivialisation that simplifies any search of new linear inferences.

5.1 A linear inference not derivable in MSU

MSU cannot derive every linear inference. This is immediate from Straßburger's result above, and since the length of paths can be assumed to be polynomial, under the assumption that $\boldsymbol{coNP} \neq \boldsymbol{NP}$. Nonetheless Straßburger has given an explicit linear inference on 36 variables that cannot be derived in MS [19]. Here we give an example on 10 variables, and conjecture that it is the minimal inference not derivable in MS. By observing that there are no trivial atoms, the same result follows for MSU.

▶ **Theorem 31.** *The following is a linear inference that is not derivable in* MS*.*

$$\frac{[A \vee (B \wedge B')] \wedge [(C \wedge C') \vee (D \wedge D')] \wedge [(E \wedge E') \vee F]}{([C \vee E] \wedge [A \vee (C' \wedge E')]) \vee ([(B \wedge D) \vee F] \wedge [B' \vee D'])}$$

Proof. The inference is linear by inspection and its soundness can be checked mechanically. However we give an intuitive argument below, to give an idea of its meaning.

The inference is essentially an encoding of the pigeonhole principle with 3 pigeons and 2 holes. Consider the following grid:

A	$B \quad B'$
$C \quad C'$	$D \quad D'$
$E \quad E'$	F

The linear inference roughly[6] encodes the following statement,

if each row contains a box whose variables are true,
then some column has two boxes with a true variable

which is clearly a tautology since there are more rows than columns. The use of multiple variables in some boxes is so that repetition of variables is avoided, ensuring linearity.

Using this interpretation, it is clear that any application of switch or medial leading to the conclusion must be from a formula not logically implied by the premiss. This can also be checked mechanically. ◀

▶ **Corollary 32.** *The above inference cannot be derived in* MSU*.*

Proof. If it could then some variable must be trivialised by Lemma 28, meaning we could substitute $\top$ for it in the premiss and $\bot$ in the conclusion and obtain a valid implication. Inspection shows that no variable has this property (the aforementioned interpretation makes it easier to verify this). ◀

6 Not exactly since not all combinations of variables in boxes are exhausted.

5.2 Towards a basis for L

Can we find a basis for L? I.e. can we find some polynomial-time decidable set of linear inferences from which every linear inference can be derived? This question remains open, but it is worth noting that such a set cannot be finite; the encoding in Thm. 31 can easily be generalised to arbitrary $n \times (n-1)$ grids, and it is not difficult to show that each subsequent linear inference cannot be derived from all the previous ones, along with MSU. It is also worth noting that any basis would have to admit (necessarily) superpolynomial-length paths, unless $\boldsymbol{coNP} = \boldsymbol{NP}$.

Here we present an observation extending the previous notion of trivialisation. We considered previously *syntactic* trivialisation of an atom or variable, when it is explicitly put in disjunction with $\top$ or conjunction with $\bot$. However, when talking about all linear inferences we will want a more general concept that is not reliant on how it is derived in any particular system:

▶ **Definition 33** (Semantic trivialisation)**.** Let $\rho : \xi\{A\} \to \zeta\{A\}$ be a linear inference. We say that ρ is *semantically trivial* at A, or simply trivial, if $\xi\{\top\} \to \zeta\{\bot\}$ is sound.

The condition in the above definition is equivalent to demanding that $\xi\{s\} \to \zeta\{t\}$ is sound for every s, t.

Note that trivialities may depend on each other, and so one should say that an inference is "trivial at A then B" or "trivial at A or B" rather than "trivial at A and B". For example $\mathsf{mix} : A \wedge B \to A \vee B$ is trivial at A or B but not both at once.

▶ **Theorem 34.** *If a linear inference ρ is trivial somewhere then there is a linear inference ρ' on fewer variables that is not trivial anywhere and from which ρ is derivable in* MSU*.*

Proof. Let $\rho : s \to t$ and let $A_1, \dots, A_k$ be the trivial variables (in order). We construct the following derivation in $\rho' \cup \mathsf{MS/U}$,

$$
\dfrac{s}{\xi\left\{A_1 \vee \dfrac{\bot}{\top}\right\} \cdots \left\{A_k \vee \dfrac{\bot}{\top}\right\}}
$$

$$
\bullet \,\Big\Vert\, \mathsf{M}
$$

$$
\left([A_1 \vee \top] \wedge \cdots \wedge [A_k \vee \top] \wedge \dfrac{\dfrac{\xi\{\top\}\cdots\{\top\}}{\rho' \, \dfrac{s'}{t'}}}{\zeta\left\{\dfrac{\bot}{\top \wedge \bot}\right\} \cdots \left\{\dfrac{\bot}{\top \wedge \bot}\right\}} \right)
$$

$$
\circ \,\Big\Vert\, \mathsf{S}
$$

$$
\dfrac{\zeta\left\{ \mathsf{s}\, \dfrac{\dfrac{[A_1 \vee \top] \wedge \bot}{A_1 \vee (\top \wedge \bot)}}{A_1} \right\} \cdots \left\{ \mathsf{s}\, \dfrac{\dfrac{[A_k \vee \top] \wedge \bot}{A_k \vee (\top \wedge \bot)}}{A_k} \right\}}{t}
$$

where the derivation marked • is obtained from Lemma 27, the derivation marked ∘ from Prop. 25 and s', t' are the unique unit-free terms U-equivalent to $\xi\{\top\}\cdots\{\top\}$, $\zeta\{\bot\}\cdots\{\bot\}$ respectively. ◀

6 Conclusions

In this work we considered the linear inferences of propositional logic, in particular from the point of view of complexity and termination of rewriting derivations. This was motivated by the seemingly fundamental role played by linear inferences in deep inference proof theory; as well as being necessary for locality of the inference rules in deep inference, we showed in Sect. 3 that proof search in Frege and Gentzen systems with cut can be reduced in polynomial-time to finding MS-rewrite paths. In contrast, we showed in Sect. 4 that the length of MS(U)-rewrite paths can always be made polynomial, and so the size of a proof is determined by the use of structural rules in a deep inference derivation. Finally we considered the set of all linear inferences and made some general observations.

One particular outcome of this research is the possibility to implement proof search based on strong systems. Typically, proof search algorithms are based on weak proof systems, due to an apparent tradeoff between proof size and proof search. This is most significantly exemplified by the presence of *nonanalytic* rules in stronger systems, e.g.

$$\underset{\textit{modus ponens}}{\frac{A \quad A \supset B}{B}} \qquad \underset{\textit{cut}}{\frac{\Gamma \to \Delta, A \quad A, \Sigma \to \Pi}{\Gamma, \Sigma \to \Delta, \Pi}}$$

When searching for a proof we tend to work 'bottom-up', and in the two rules above there are seemingly infinitely many choices for A, which is terrible for proof-search. The tradeoff is that weak systems, such as cut-free Gentzen and Resolution, have much larger proofs. In many cases there are only exponential-size proofs, as opposed to polynomial-size ones in Frege systems [14], for example the propositional encodings of the pigeonhole principle. This lower bound acts as a barrier to efficient proof search, since the complexity of the search procedure is bounded below by the complexity of the objects it searches for.

However, in Sect. 3 we gave a polynomial-time reduction of the problem of proof-search in Frege and Gentzen systems to finding MS-rewrite paths between formulae. This is arguably a simpler problem, firstly since there is no infinite choice present as variables in a term are preserved by linear inferences, and secondly since we already have some understanding of various subproblems, namely a characterisation of S and M in [17]. It would be interesting to see what progress could be made on proof search algorithms based on MS-rewriting, enabling access to the shorter proofs of stronger systems while still restricting the nondeterminism of proof search.

Even more powerful systems, e.g. Extended Frege, could also be used as a base for proof search in the same way, by adding more linear rules. A proof system P can be simulated by Frege when axioms expressing the soundness of P are added [14], and using a trick from [19] these can be encoded as linear inference rules which could be added to MS, again preserving analyticity.

References

1 ML Bonet, T. Pitassi, and R. Raz. No feasible interpolation for tc0-frege proofs. In *focs*, page 254. Published by the IEEE Computer Society, 1997.

2 Kai Brünnler. Two restrictions on contraction. *Logic Journal of the IGPL*, 11(5):525–529, 2003. `http://www.iam.unibe.ch/~kai/Papers/RestContr.pdf`.

3 Kai Brünnler. *Deep Inference and Symmetry in Classical Proofs*. Logos Verlag, Berlin, 2004. `http://www.iam.unibe.ch/~kai/Papers/phd.pdf`.

4 Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In R. Nieuwenhuis and A. Voronkov, editors, *LPAR 2001*, volume 2250 of *Lecture Notes in Computer Science*, pages 347–361. Springer-Verlag, 2001. `http://www.iam.unibe.ch/~kai/Papers/lcl-lpar.pdf`.

5 Paola Bruscoli and Alessio Guglielmi. On the proof complexity of deep inference. *ACM Transactions on Computational Logic*, 10(2):1–34, 2009. Article 14. `http://cs.bath.ac.uk/ag/p/PrComplDI.pdf`.

6 Paola Bruscoli, Alessio Guglielmi, Tom Gundersen, and Michel Parigot. Quasipolynomial normalisation in deep inference via atomic flows and threshold formulae. Submitted. `http://cs.bath.ac.uk/ag/p/QuasiPolNormDI.pdf`, 2009.

7 Anupam Das. On the proof complexity of cut-free bounded deep inference. 2011. Tableaux'11.

8 Anupam Das. Complexity of deep inference via atomic flows. In S. Barry Cooper, Anuj Dawar, and Benedikt Löwe, editors, *Computability in Europe*, volume 7318 of *Lecture Notes in Computer Science*, pages 139–150. Springer-Verlag, 2012. `http://www.anupamdas.com/items/RelComp/RelComp.pdf`.

9 Alessio Guglielmi and Tom Gundersen. Normalisation control in deep inference via atomic flows. *Logical Methods in Computer Science*, 4(1:9):1–36, 2008. `http://www.lmcs-online.org/ojs/viewarticle.php?id=341`.

10 Alessio Guglielmi, Tom Gundersen, and Michel Parigot. A proof calculus which reduces syntactic bureaucracy. In Christopher Lynch, editor, *RTA 2010*, volume 6 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 135–150. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2010. `http://drops.dagstuhl.de/opus/volltexte/2010/2649`.

11 Alessio Guglielmi, Tom Gundersen, and Lutz Straßburger. Breaking paths in atomic flows for classical logic. In Jean-Pierre Jouannaud, editor, *25th Annual IEEE Symposium on Logic in Computer Science*, pages 284–293. IEEE, 2010. `http://www.lix.polytechnique.fr/~lutz/papers/AFII.pdf`.

12 VA Gurvich. Repetition-free boolean functions. *Uspekhi Matematicheskikh Nauk*, 32(1):183–184, 1977.

13 Emil Jeřábek. Proof complexity of the cut-free calculus of structures. *Journal of Logic and Computation*, 19(2):323–339, 2009. `http://www.math.cas.cz/~jerabek/papers/cos.pdf`.

14 Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory.* Cambridge University Press, New York, NY, USA, 1995.

15 François Lamarche. Exploring the gap between linear and classical logic. *Theory and Applications of Categories*, 18(17):473–535, 2007. `http://www.loria.fr/~lamarche/papers/Gap.pdf`.

16 Lutz Straßburger. MELL in the calculus of structures. *Theoretical Computer Science*, 309:213–285, 2003. `http://www.lix.polytechnique.fr/~lutz/papers/els.pdf`.

17 Lutz Straßburger. A characterisation of medial as rewriting rule. In Franz Baader, editor, *RTA 2007*, volume 4533 of *Lecture Notes in Computer Science*, pages 344–358. Springer-Verlag, 2007. `http://www.lix.polytechnique.fr/~lutz/papers/CharMedial.pdf`.

18 Lutz Straßburger. On the axiomatisation of boolean categories with and without medial. *Theory and Applications of Categories*, 18(18):536–601, 2007. `http://www.lix.polytechnique.fr/~lutz/papers/medial.pdf`.

19 Lutz Straßburger. Extension without cut. *Ann. Pure Appl. Logic*, 163(12):1995–2007, 2012.