Rewriting with linear inferences in propositional logic

Anupam Das

February 15, 2013

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 MS, utilising a notion of *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.

1 Introduction

Linear inferences are sound implications of propositional logic where each variable appears exactly once in the premiss and conclusion. 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 [Brü03]. In recent years there has been much work on understanding the role of medial in proofs and logic [BT01] [Lam07] [BG09] [Str07b]. Most recently, Straßburger commenced a study of it from the point of view of rewriting theory [Str07a].

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?

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 [Str07a] 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 [BG09]) 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 an atom 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 [GGS10] [GG08]. 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 $\boldsymbol{coNP \neq NP}$. Straßburger gives an explicit linear inference in [Str09] 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 [GGP10] 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

The author would like to thank Lutz Straßburger, Alessio Guglielmi and in particular Alvin Šipraga for helpful discussions on the current work.

2 Preliminaries

The language of propositional logic consists of countably many atoms $a, b, \ldots$ and their duals $\bar{a}, \bar{b}, \ldots$, possibly with superscripts or subscripts, units $\top, \bot$ and the connectives $\wedge, \vee$. Formulae are defined by the following grammar,

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

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

Definition 1 (Contexts)**.** A *context* is a formula with a single hole, denoted $\{\ \}$, occurring in place of a subformula. Formally,

$$\xi\{\ \} ::= \quad \{\ \} \quad | \quad (A \wedge \xi\{\ \}) \quad | \quad [A \vee \xi\{\ \}]$$

We write $\xi\{A\}$ to denote the formula resulting from substituting the formula A for the hole in $\xi\{\ \}$. We also consider contexts with multiple holes, denoted $\xi\{\ \}\cdots\{\ \}$, defined in the natural way.

All rewriting rules operate modulo associativity and commutativity, i.e. the equational theory generated by the following rules,

$$A \star B = B \star A \quad , \quad A \star (B \star C) = (A \star B) \star C$$

for $\star \in \{\wedge, \vee\}$. For this reason we often exclude internal brackets of a formula.

Definition 2 (Linear inferences)**.** A linear inference is a (sound) rewrite rule on unit-free propositional formulae $\rho : A \to B$ such that each atom occurs exactly once in A and B. We define L to be the set of all linear inferences.

We identify inference rules on formulae with 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 [GGP10] as a proof formalism, *open deduction*, but can be thought of as just a convenient notation for formula rewriting.

Definition 3. Let $\mathcal{S}$ be a set of rewrite rules on propositional formulae. We write $\begin{array}{c} A \\ \| \mathcal{S} \\ B \end{array}$ to denote a $\mathcal{S}$-derivation from a formula A to a formula B, defined as follows:

- $\rho\,\dfrac{A}{B}$ is a $\mathcal{S}$-derivation from A to B, if $\rho : A \to B$ is in $\mathcal{S}$.[1]

- $\begin{matrix} A & C \\ \| \mathcal{S} & \star & \| \mathcal{S} \\ B & & D \end{matrix}$ is a $\mathcal{S}$-derivation from $A \star C$ to $B \star D$, for $\star \in \{\wedge, \vee\}$.

- $\begin{matrix} A \\ \| \mathcal{S} \\ B \\ \| \mathcal{S} \\ C \end{matrix}$ is a $\mathcal{S}$-derivation from A to C.

Sometimes, if two formulae A, A' are considered equivalent up to some relation, e.g. associativity and commutativity, we may aid the reader by adding a 'fake' rewrite step: $\dfrac{A}{A'}$.

Definition 4. We define the system $\mathsf{MS}^\star$ to consist of the following rules,

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

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 MS is defined $\mathsf{MS}^\star \cup \mathsf{U}$.

3 Complexity of characterising $\mathsf{MS}^{(\star)}$

The motivation behind this section originates from the following result in [Str07a].

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

In the same work the task of characterising $\mathsf{MS}^\star$ was raised as an open problem.

In this section we give a polynomial-time reduction from the problem of finding a Frege proof[2] of a given tautology to the problem of finding a $\mathsf{MS}^\star$-rewrite path between two formulae. Consequently, we deduce that there is no polynomial-time characterisation of $\mathsf{MS}^\star$ (and also MS) under the assumption that integers cannot be factorised in polynomial-time.

Throughout this section we use the notation $A^n := \overbrace{A \wedge \cdots \wedge A}^{n}$ and $n \cdot A := \overbrace{A \vee \cdots \vee A}^{n}$.

[1] Note in particular that this is a one-step shallow rewrite.

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

3.1 Reducing proof-search to rewriting in $\mathsf{MS}^\star$

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 [Brü04],[BG09].

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. [Jeř09], [Das12]. □

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

$$\begin{array}{c} \bigwedge_i a_i \vee \bar{a}_i \vee B_i \\ \Vert \mathsf{MS}^\star \\ \tau' \end{array}$$

where τ' differs from τ only in that some atom occurrences a may be replaced by a disjunction $n \cdot a$.

Proof. See e.g. [Brü04], [Das11]. □

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

$$\begin{array}{c} A \\ \Vert \mathsf{S} \\ \bigwedge_i k_i \cdot a_i \vee k_i \cdot \bar{a}_i \vee B_i \end{array}$$

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

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

$$\begin{array}{c} [a_i \vee \bar{a}_i \vee B'_{i1}] \wedge \cdots \wedge [a_i \vee \bar{a}_i \vee B'_{ik}] \\ \Vert \mathsf{S} \\ \left[\begin{array}{r} B'_i \\ k \cdot a_i \vee k \cdot \bar{a}_i \vee \ \Vert \mathsf{S} \\ B_i \end{array}\right] \end{array}$$

Validity follows since each disjunction of A contains an atom and its dual. □

Lemma 9. *Let A be a valid formula in conjunctive normal form such that each atom occurs as many times as its dual. Then there is a polynomial-size derivation of the following shape:*

$$\begin{array}{c} \bigwedge_i a_i \vee \bar{a}_i \\ \Vert \mathsf{MS}^\star \\ A \end{array}$$

Proof. Since A is valid each of its disjunctions must contain two dual atoms. Choose such a pair for each disjunction, and match each other atom in a disjunction with an occurrence of its dual in another disjunction; the matching is bijective by the given condition.

Consider the following rewriting:

$$\begin{array}{l} 2{\cdot}\mathsf{S} \\ \mathsf{M} \end{array} \dfrac{\dfrac{A \wedge B \wedge [a \vee \bar{a}]}{(A \wedge \bar{a}) \vee (B \wedge a)} \wedge C}{[A \vee a] \wedge (B \wedge \bar{a})}$$

Read bottom-up, if a and $\bar{a}$ are a matching pair, then the total number of matching pairs in distinct disjunctions has reduced. Since the premiss of this rewriting is in the same form, we can inductively apply this rewriting (bottom-up) 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,*

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

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 $\mathsf{MS}^{(\star)}$, 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 $\mathsf{MS}^{(\star)}$-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 $\mathsf{MS}^\star$-rewrite path between two formulae on the premiss and conclusion determined by each value of k, from 1 upwards, until it returns. □

3.2 No polynomial-time characterisation for $\mathsf{MS}^{(\star)}$

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 [BPR97], conditional on the assumption that integer factoring is hard for $P/poly$.

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 hard for $P/poly$ then Frege is not weakly automatisable.*

Corollary 14. *If integer factoring is hard for $P/poly$ then there is no polynomial-time characterisation of $\mathsf{MS}^{(\star)}$.*

Remark 15. 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 integers can be factorised in polynomial time. This (conditionally) refutes a conjecture of Guglielmi that atomic flows form a proof system [GG08].

4 Length of paths with units

In this section we address the complexity of rewriting paths in MS. The length of $\mathsf{MS}^\star$-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 formula. Much tighter bounds can be obtained, and this is the subject of ongoing work by Bruscoli, Guglielmi and Straßburger.[3]

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 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 throughout.

Henceforth, we shall assume that all atoms occurrences in a formula are distinct, i.e. each atom occurs at most once.

Theorem 16. $\mathsf{MS}^\star$ *has only polynomial-length paths.*

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

[3] Personal correspondence.

Let M denote the product measure $n \times m : A \mapsto (n(A), m(A))$, then each step of an $\mathsf{MS}^\star$-derivation strictly reduces M. But n is linear in the size of a formula and m is quadratic, so an $\mathsf{MS}^\star$-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:

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

A standard approach here would be to conduct rewriting modulo the equational theory generated by U, i.e. consider formulae equivalent up to U-rewriting.[4] This does not quite work here, since we can still construct cycles, for example:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\top}{\top \wedge \top} \vee (a \wedge b)}{[\top \vee a] \wedge [\top \vee b]}\,\mathsf{M}}{\dfrac{\dfrac{a}{a \wedge \top} \vee \dfrac{b}{b \wedge \top}}{[a \vee \top] \wedge [b \vee \top]}\,\mathsf{M}}\,2{\cdot}\mathsf{S}}{\top \vee \top \vee (a \wedge b)}\,2{\cdot}\mathsf{S}}{\top \vee (a \wedge b)} \qquad \dfrac{\top \wedge \top}{\top} \vee$$

These situations only occur when an atom 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 formula is U'-equivalent to an unique unit-free formula or $\top$ or $\bot$.*

Proof. See e.g. [Das11]. □

Proposition 18. *Distinct unit-free formulae, modulo associativity and commutatitivity, compute distinct boolean functions.*

Proof. See e.g. [Gur77]. □

From these we can deduce the strong normalisation property.

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

Corollary 19. *Rewriting in* MS *modulo* U' *is strongly normalising.*

Proof. There are only 2^n assignments on n variables, and each boolean function determines an unique set of these assignments. Since rewriting 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 strong normalisation in the proof 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

We present a new rule, *supermix*, that is derivable in MS and show that one can construct exponential-length paths with it, modulo U' as defined above.

Definition 20 (Supermix)**.** We define the supermix rule below:

$$\mathsf{smix}\ \frac{a \wedge \bigvee_{i=1}^{n} b_i}{a \vee \bigwedge_{i=1}^{n} b_i}$$

Supermix 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 MS.

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

Proof.

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

□

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

Lemma 22. *There is a* MS*-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 $\dfrac{\bot}{\top} \vee b$.

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

$$\Phi_n \quad := \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{b_n}{\top \wedge b_n}\vee \quad \top \vee \bigwedge_{i=1}^{n-1} b_i}{\top \wedge \left[\top \vee \bigwedge_{i=1}^{n-1} b_i\right]}}{[\top \vee b_n] \wedge \left[\top \vee \top \vee \bigwedge_{i=1}^{n-1} b_i\right]}\mathsf{M}}{\top \vee \top \vee \top}\mathsf{2{\cdot}S}}{\top}\vee \left(b_n \wedge \bigwedge_{i=1}^{n-1} b_i\right)} \qquad \begin{array}{c}\bigvee_{i=1}^{n-1} b_i \\ \Phi_{n-1}\,\|\,\mathsf{MS}\end{array}$$

□

Theorem 23. *Supermix is derivable in* MS.

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

$$\dfrac{\dfrac{a \wedge \dfrac{\bigvee_i^n b_i}{\Phi_n\,\|\,\mathsf{MS}}}{\top \vee \bigwedge_i^n b_i}\mathsf{S}}{\dfrac{a \wedge \top}{a} = \vee \bigwedge_i^n b_i}$$

□

Note that the premiss and conlusion 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 as follows:

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

4.2 Construction of polynomial-length paths

The cause of problems in (complexity of) termination of MS seems to be the trivialising of atoms 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 formulae with

a MS-path between them has one of polynomial length. The general idea is to 'move' trivialised atoms to one side and reduce to the unit-free case, before reintroducing the trivialised atoms.

Definition 24 (Trivialised Atoms)**.** In a derivation we say that an atom is *trivialised* if at any point it occurs within the scope of a disjunction containing $\top$ or a conjunction containing $\bot$.

Proposition 25. *There are polynomial-size derivations* $\dfrac{\xi\{A\}}{A \vee \xi\{\bot\}}\,\mathsf{s}$, $\dfrac{A \wedge \xi\{\top\}}{\xi\{A\}}\,\mathsf{s}$.

Proof. See e.g. [Jeř09], [BGGP09], [Das12]. □

Lemma 26. *Let* $\xi\{a\} \Vdash_{\mathsf{MS}}$ *be a derivation where* a *is trivialised. Then there is a derivation* $\xi\{\top \vee a\} \Vdash_{\mathsf{MS}}$ *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,

$$\begin{array}{c}\xi\{a\}\\ \Phi\big\|_{\mathsf{MS}}\\ F\{\top \vee G\{a\}\}\\ \Psi\big\|_{\mathsf{MS}}\\ \zeta\{a\}\end{array} \quad \to \quad \begin{array}{c}\xi\{\top \vee a\}\\ \Phi'\big\|_{\mathsf{MS}}\\ F\left\{\begin{array}{c}\top \vee G\left\{\begin{array}{c}\dfrac{a}{\top \vee \dfrac{[\top \vee \bot] \wedge a}{\top \vee (\bot \wedge a)}\,\mathsf{s}}\\ \top \vee (\bot \wedge a)\end{array}\right\}\\ \bullet\big\|_{\mathsf{S}}\\ \top \vee G\{\bot \wedge a\}\end{array}\right\}\\ \top \vee G\{\bot \wedge a\}\\ \Psi'\big\|_{\mathsf{MS}}\\ \zeta\{\bot \wedge a\}\end{array}$$

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

transform the derivation as follows,

$$\begin{array}{c}\xi\{a\}\\ \Phi\big\|\mathsf{MS}\\ F\{\bot\wedge G\{a\}\}\\ \Psi\big\|\mathsf{MS}\\ \zeta\{a\}\end{array}\quad\to\quad F\left\{\begin{array}{c}\xi\{\top\vee a\}\\ \Phi'\big\|\mathsf{MS}\\ \dfrac{\dfrac{\bot}{\bot\wedge\bot}=\quad G\left\{\begin{array}{c}a\\ \hline \top\vee\ \mathsf{s}\ \dfrac{[\top\vee\bot]\wedge a}{\top\vee(\bot\wedge a)}\\ \hline \top\vee(\bot\wedge a)\end{array}\right\}}{\bot\wedge G\{\bot\wedge a\}}\wedge\\ \bullet\big\|\mathsf{s}\\ 2{\cdot}\mathsf{s}\ \dfrac{\top\vee G\{\bot\wedge a\}}{(\bot\wedge\top)\vee(\bot\wedge G\{a\})}\\ \Psi'\big\|\mathsf{MS}\\ \zeta\{\bot\wedge a\}\end{array}\right\}$$

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

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

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,

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

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

Lemma 28. *Every* MS*-derivation where no atoms occur trivialised can be transformed into an* $\mathsf{MS}^\star$*-derivation with same premiss and conclusion modulo* U.

Proof. We simply reduce every line in the derivation to a unit-free formula by U. Since no atoms are trivialised we do not need any U'-rules. We rewrite derivations using the four possible cases below, any other combination of rules with units results in some atom(s) in either the premiss or conclusion being trivialised.

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

$$\mathsf{M}\,\frac{(A\wedge B)\vee(\bot\wedge\bot)}{[A\vee\bot]\wedge[B\vee\bot]}\quad\to\quad A\wedge B \qquad\qquad \mathsf{M}\,\frac{(A\wedge\top)\vee(B\wedge\top)}{[A\vee B]\wedge[\top\vee\top]}\quad\to\quad A\vee B$$

□

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

Proof. Let Φ be an MS-derivation. If there are no trivialised atoms then transform it into an $\mathsf{MS}^\star$-derivation by Lemma 28 which must be of polynomial size by Thm. 16.

If there is a trivialised atom in Φ, say a_1, then transform Φ as follows:

$$\begin{array}{c}\xi\{a_1\}\\ \Phi\big\|\mathsf{MS}\\ \zeta\{a_1\}\end{array}\quad\to\quad\begin{array}{c}\xi\{\top\vee a_1\}\\ \Phi'\big\|\mathsf{MS}\\ \zeta\{\bot\wedge a_1\}\end{array}\quad\to\quad\begin{array}{c}\xi\left\{\begin{array}{c}\overset{a_1}{\overset{\cdots\cdots}{\top\vee\ \ }}\\ \mathsf{S}\,\dfrac{[\top\vee\bot]\wedge a_1}{\top\vee(\bot\wedge a_1)}\\ \cdots\cdots\\ \top\vee(\bot\wedge a_1)\end{array}\right\}\\ \bullet\big\|\mathsf{S}\\ \left[\begin{array}{l}\xi\{\top\vee\bot\}\\ \ \ \Phi_1\big\|\mathsf{MS}\quad\vee(\bot\wedge a_1)\\ \zeta\{\bot\wedge\bot\}\end{array}\right]\end{array}$$

where Φ' is obtained from Φ by Lemma 26, Φ_1 from Φ' by substituting $\bot$ for every instance of a_1, and the derivation marked $\bullet$ by Lemma 27.

Now do the same for Φ_1, and repeat this process until either there are no trivialised atoms in some Φ_k. (Note that it is not sufficient to just do all the trivialised atoms at once, since the act of substituting $\bot$ for a_i may result in new trivialisations.)

Now by Lemma 28 we can transform Φ_k to an $\mathsf{MS}^\star$-derivation Ψ with same premiss and conclusion modulo U, which we assume to have polynomial size by Thm. 16.

$$\begin{array}{c}\xi\{\top\vee\bot\}\cdots\{\top\vee\bot\}\\ \Phi_k\big\|\mathsf{MS}\\ \zeta\{\bot\wedge\bot\}\cdots\{\bot\wedge\bot\}\end{array}\quad\to\quad\begin{array}{c}\overset{\xi\{\top\vee\bot\}\cdots\{\top\vee\bot\}}{\overset{\cdots\cdots}{A}}\\ \Psi\big\|\mathsf{MS}^\star\\ \underset{\cdots\cdots}{B}\\ \zeta\{\bot\wedge\bot\}\cdots\{\bot\wedge\bot\}\end{array}$$

The complete transformation is as follows,

$$\begin{array}{ccc}
 & & \xi\left\{\begin{array}{c}=\dfrac{a_1}{\mathsf{S}\dfrac{[\top\vee\bot]\wedge a_1}{\top\vee(\bot\wedge a_1)}}\end{array}\right\}\cdots\left\{\begin{array}{c}=\dfrac{a_k}{\mathsf{S}\dfrac{[\top\vee\bot]\wedge a_k}{\top\vee(\bot\wedge a_k)}}\end{array}\right\} \\
 & & \Vert\mathsf{S} \\
\xi\{a_1\}\cdots\{a_k\} & & \left[\begin{array}{c}\xi\{\top\vee\bot\}\cdots\{\top\vee\bot\} \\ \hdashrule{3cm}{0.4pt}{1pt} \\ A \\ \Psi\Vert\mathsf{MS}^\star \\ B \\ \hdashrule{3cm}{0.4pt}{1pt} \\ \zeta\{\bot\wedge\bot\}\cdots\{\bot\wedge\bot\}\end{array}\quad\vee(\bot\wedge a_1)\vee\cdots\vee(\bot\wedge a_k)\right] \\
\Phi\Vert\mathsf{MS} & \to & \\
\zeta\{a_1\}\cdots\{a_k\} & & \bullet\Vert\mathsf{M} \\
 & & \zeta\left\{\begin{array}{c}\dfrac{\bot}{\top}\wedge a_1 \\ \hdashrule{1cm}{0.4pt}{1pt} \\ a_1\end{array}\right\}\cdots\left\{\begin{array}{c}\dfrac{\bot}{\top}\wedge a_k \\ \hdashrule{1cm}{0.4pt}{1pt} \\ a_k\end{array}\right\}
\end{array}$$

where the derivation marked • is obtained by repeatedly applying Lemma 27. □

Remark 30. As a consequence of 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. [BGGP09], [Das12], 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 inferences, from the point of view of complexity, due to the following result by Straßburger.

Proposition 31 (Straßburger)**.** L *is* ***coNP****-complete.*

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

5.1 A sound inference not derivable in MS

$\mathsf{MS}^{(\star)}$ 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 $\mathsf{MS}^\star$ [Str09].

Here we give an example on 10 variables, and conjecture that it is the minimal inference not derivable in $\mathsf{MS}^\star$. By observing that there are no trivial atoms, the same result follows for MS.

Theorem 32. *The following is a linear inference that is not derivable in* $\mathsf{MS}^\star$.

$$\frac{[a \vee (b \wedge b')] \wedge [(c \wedge c') \vee (d \wedge d')] \wedge [(e \wedge e') \vee f]}{([c \vee e] \wedge [a \vee (c' \wedge e')]) \vee ([(b \wedge d) \vee f] \wedge [b' \vee d'])}$$

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 two holes. Consider the following grid:

a	b b'
c c'	d d'
e e'	f

The linear inference roughly[5] 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 33. *The above inference cannot be derived in* MS

Proof. If it could then some atom 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 atom has this property (the aforementioned interpretation makes it easier to verify this). □

Remark 34. We conjecture that the inference above is the minimal inference not derivable in MS. This could theoretically be checked by brute force, but the task is complex computationally. Some work to this end can be found in [Š12].

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;

[5] Not exactly since not all combinations of variables in boxes are exhausted.

the encoding in Thm. 32 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 MS. It is also worth noting that any basis would have to admit (necessarily) superpolynomial-length paths, unless $\boldsymbol{coNP = NP}$.

Here we present an observation extending the previous notion of a trivialised atom. We considered previously *syntactic* trivialisation of an atom, when it is explicitly put in disjuntion 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 35 (Semantic trivialisation)**.** Let $\rho : \xi\{a\} \to \zeta\{a\}$ be a linear inference. We say that ρ is *(semantically) trivial* at a if $\xi\{\top\} \to \zeta\{\bot\}$ is sound.

Note that it does not make sense to talk about multiple trivialities at once, since they may depend on each other. One should say that an inference is "trivial at a *then* b" or "trivial at a or b". For example $\mathsf{mix} : a \wedge b \to a \vee b$ is trivial at a or b but not both at once.

Theorem 36. *If a linear inference ρ is trivial somewhere then there is a smaller linear inference ρ' that is not trivial anywhere and from which ρ is derivable in* MS.

Proof. Let $\rho : A \to B$ and let $a_1, \ldots, a_k$ be the trivial atoms (in order). We construct the following derivation,

$$\dfrac{\dfrac{A}{\xi\left\{a_1 \vee \dfrac{\bot}{\top}\right\}\cdots\left\{a_k \vee \dfrac{\bot}{\top}\right\}}\bullet\Vert\mathsf{M}}{\left(\begin{array}{c}[a_1 \vee \top] \wedge \cdots \wedge [a_k \vee \top] \wedge \dfrac{\dfrac{\xi\{\top\}\cdots\{\top\}}{\rho'\,\dfrac{A'}{B'}}}{\zeta\left\{\dfrac{\bot}{\top \wedge \bot}\right\}\cdots\left\{\dfrac{\bot}{\top \wedge \bot}\right\}}\end{array}\right)}\circ\Vert\mathsf{S}$$

$$\dfrac{\zeta\left\{\mathsf{s}\,\dfrac{[a_1 \vee \top] \wedge \bot}{a_1 \vee (\top \wedge \bot)}\right\}\cdots\left\{\mathsf{s}\,\dfrac{[a_1 \vee \top] \wedge \bot}{a_1 \vee (\top \wedge \bot)}\right\}}{B}$$

where the derivation marked $\bullet$ is obtained from Lemma 27, the derivation marked $\circ$ from Prop. 25 and A', B' are the unique unit-free formulae 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-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.

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

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 [Kra95], 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 formula are preserved by linear inferences, and secondly since we already have some understanding of various subproblems, namely a characterisation of S and M in [Str07a]. 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 [Kra95], and using a trick from [Str09] these can be encoded as linear inference rules which could be added to MS, again preserving analyticity.

References

[BG09] 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`.

[BGGP09] 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.

[BPR97] 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.

[Brü03] 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`.

[Brü04] Kai Brünnler. *Deep Inference and Symmetry in Classical Proofs*. Logos Verlag, Berlin, 2004. `http://www.iam.unibe.ch/~kai/Papers/phd.pdf`.

[BT01] Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In R. Nieuwenhuis and A. Voronkov, editors, *LPAR 2001*, volume 2250 of *Lecture Notes in Computer Science*, pages 347–361. Springer-Verlag, 2001. `http://www.iam.unibe.ch/~kai/Papers/lcl-lpar.pdf`.

[Das11] Anupam Das. On the proof complexity of cut-free bounded deep inference. 2011. Tableaux '11.

[Das12] 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`.

[GG08] 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`.

[GGP10] 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`.

[GGS10] 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.

[Gur77] VA Gurvich. Repetition-free boolean functions. *Uspekhi Matematicheskikh Nauk*, 32(1):183–184, 1977.

[Jeř09] 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.

[Kra95] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*. Cambridge University Press, New York, NY, USA, 1995.

[Lam07] 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.

[Str07a] 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.

[Str07b] 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.

[Str09] Lutz Straßburger. Extension without cut. Submitted. http://www.lix.polytechnique.fr/~lutz/papers/psppp.pdf, 2009.

[Š12] Alvin Šipraga. An automated search of linear inference rules. http://arcturus.su/mimir/autolininf.pdf, 2012.