Scientific Annals of Computer Science vol. 25(2), 2015, pp. 1–70

The Consistency and Complexity of Multiplicative Additive System Virtual

Ross HORNE[1]

Abstract

This paper investigates the proof theory of multiplicative additive system virtual (MAV). MAV combines two established proof calculi: multiplicative additive linear logic (MALL) and basic system virtual (BV). Due to the presence of the self-dual non-commutative operator from BV, the calculus MAV is defined in the calculus of structures — a generalisation of the sequent calculus where inference rules can be applied in any context. A generalised cut elimination result is proven for MAV, thereby establishing the consistency of linear implication defined in the calculus. The cut elimination proof involves a termination measure based on multisets of multisets of natural numbers to handle subtle interactions between operators of BV and MAV. Proof search in MAV is proven to be a PSPACE-complete decision problem. The study of this calculus is motivated by observations about applications in computer science to the verification of protocols and to querying.

Keywords: *proof theory, deep inference, non-commutative logic*

1 Introduction

This paper provides proof theoretic results supporting a line of work that makes the case for using systems defined in the calculus of structures for formal verification of protocols. The companion paper [11] makes the case for an extension of the calculus BV [20] with the additive operators as a

[1] School of Computer Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore and Institute of Computer Science, Romanian Academy, Blvd. Carol I no. 8, 700505 Iaşi, Romania, Email: rhorne@ntu.edu.sg

foundation for finite session types [24, 26] inspired by the Scribble protocol modelling language [25]. A session type is a specification of the types of messages exchanged in a protocol along with control flow information about the order in which messages are sent and received. Session types can be used for both the static [37, 29] and runtime [28] verification of protocols.

Advantages of using the session types formalised in the calculus of structures, highlighted in the companion paper [11], include the following:

- Provability in the calculus of structures provides a natural notion of *multi-party compatibility*. Given a multi-set of session types, representing the local behaviour of participants in a protocol, multi-party compatibility determines whether the participants can work together to successfully complete a session (without deadlock due to a hanging receive with no corresponding send for example).

- Provable linear implications define a subtype relation over session types. The subtype relation allows not only the types of messages exchanged to be varied but also for the control flow of messages to be compared. A participant satisfying a super-type is always capable of fulfilling the role of any participant satisfying any of the corresponding sub-types.

- A new operator is introduced to the field of session types that is dual to parallel composition. This new operator can be used to model the parallel synchronisation of separate inputs, for example.

A further, more objective, justification for the use of the calculus of structures as a foundation for session types is that the formal model is a logical system in its own right. We provide this logical system with the technical name *multiplicative additive system virtual* (MAV). The calculus is a combination of two established proof calculi *basic system virtual*[2] (BV) and *multiplicative additive linear logic* (MALL). However, it is not sufficient to assume that the proposed combination of these two existing proof calculi preserve the desirable properties of a proof calculus. Nor is it sufficient just to cite the techniques employed [20, 46, 49, 22, 9] and hope they work. A thorough check is required. This paper addresses these issues, so that we can confidently recommend the use of systems based on MAV, such as the session type system introduced in the companion paper [11].

[2]The term *virtual* refers to an alternative intuition from physics where rules can create and annihilate virtual particle pairs [4].

This paper answers two important questions about MAV. Firstly, does MAV really define a logical system? Secondly, is the complexity bound for proof search reasonable?

The question of whether MAV really defines a logical system is approached by proof theoretic techniques. Inside MAV there is an internally derived notion of linear implication. If MAV is a good logical system, then implication should at least do the basic things that implication is expected to do. For example, every logical system agrees that if A holds then A holds, i.e. A implies A. The other property that is expected of any deductive system since the notion of a syllogism was introduced by Aristotle in Prior Analytics [35], is that if A implies B and B implies C, then A implies C. Considering all logical systems in the broadest sense, any other property that might be expected of implication is challenged by another logical system where that property of implication does not hold. Thus the presence of a notion of implication satisfying these two properties highlighted is an indicator of the consistency of a logical system, where deductive reasoning can be performed using implication. This paper establishes that linear implication in MAV obeys these most fundamental properties expected of implication.

MAV possesses a self-dual non-commutative operator — an operator, say "op", where "A op B" is not necessarily equivalent to "B op A", and also the de Morgan dual of "op" is "op" itself. Contrast this with classical conjunction $\wedge$, which has classical disjunction $\vee$ as its De Morgan dual. A motivating observation for this work is that, in the original paper initiating investigations into session types [24], both a self-dual non-commutative operator and a pair of de Morgan dual lattice operators are employed. In that original paper, the lattice operators were directly inspired [1] by the additives in MALL, and are used in session types to control choice or branching in protocols.

Due to the presence of a self-dual non-commutative operator, the consistency of linear implication is investigated in a generalisation of the sequent calculus, called the calculus of structures [20]. The sequent calculus, due to Gentzen [16], is a flexible formalism for expressing proof systems and establishing consistency results, but is constrained to reasoning in a shallow structure called a sequent. Tiu [50] established that a calculus with a self-dual non-commutative operator called BV cannot be expressed without a technique enabled by the calculus of structures, called deep inference. In deep inference, rules are applied at any depth within a proposition. The main contribution of this paper is to establish that techniques developed in the calculus of structures can be adapted to the system MAV.

The question of the reasonable complexity of proof search is of course subjective. This paper establishes that proof search is a PSPACE-complete problem, . . . but is that reasonable? To justify whether the complexity bound is reasonable, applications should be considered. Concerning the problems associated with verifying protocols in the companion paper [11], a good protocol is likely to be of a limited size, so a PSPACE-complete verification tool is reasonable. In the setting of query languages, PSPACE-complete problems are common, including the *combined complexity* of Codd-equivalent languages [51] such as relational algebra. By the combined complexity we mean the complexity in terms of arbitrary queries and data. However, other complexity measures, such as *query complexity*, that reflect the fact that the data is large compared to a query and either the data or query is likely to be mostly static, explain why in practice most queries on a database run efficiently. Therefore, we argue that for the envisioned applications, a PSPACE-complete complexity bound for proof search is comparable to what would be expected for an expressive but finite system.

Section 2 provides background material on the sequent calculus and the logical system multiplicative additive linear logic. The reader comfortable with linear logic can skip this section. Section 3 introduces the syntax and semantics of MAV expressed in the calculus of structures. Section 4 provides the proof theoretic devices that establish the consistency of MAV, via a generalised cut elimination result. Finally, in Section 5, several proof theoretic results and known complexity results are invoked to establish the complexity of MAV.

2 Multiplicative Additive Linear Logic

For reference, we introduce the logical system multiplicative additive linear logic (MALL) expressed in the sequent calculus. MALL is a sub-system of linear logic. Linear logic was discovered by Girard [17] when investigating the separation of the roles of duplication and disposal of formulae, called *contraction* and *weakening*, from the role of negation in proof systems for intuitionistic logic. By removing the powerful *exponential* operators that control the use of contraction and weakening from propositional linear logic, we obtain a well behaved logical system with two pairs of conjunction and disjunction operators — the multiplicatives and the additives.

The semantics of MALL can be expressed in a proof calculus called the sequent calculus. The sequent calculus involves two levels of syntax – the object level and the meta level. The object level concerns the propositions themselves, while the meta level concerns the language for describing proofs.

The meta level sequents. Sequents are meta level constructs that consist of a bag of propositions separated by commas. Another name for a bag is a commutative monoid which is a structure satisfying associativity and commutativity, with a unit. Sequents range over Γ, Δ, as defined by the following grammar, where T is any proposition.

$$\Gamma ::= T \mid \Gamma, \Gamma$$

The following structural congruence (a reflexive, transitive, symmetric relation that holds in any context) over sequents induces the structural rule exchange, where the exchange rule allows any two formulae inside a sequent to exchange position. The unit I is an elegant way of handling empty sequents. Also, due to associativity, brackets can be omitted in sequents.

$$(\Gamma, \Delta), E \equiv \Gamma, (\Delta, E) \qquad \Gamma, \Delta \equiv \Delta, \Gamma \qquad \Gamma, \mathrm{I} \equiv \Gamma$$

$$\Gamma \equiv \Gamma \qquad \text{if } \Gamma \equiv \Delta \text{ then } \Delta \equiv \Gamma \qquad \text{if } \Gamma \equiv \Delta \text{ and } \Delta \equiv E, \text{ then } \Gamma \equiv E$$

$$\text{if } \Gamma \equiv \Delta \text{ then } \Gamma, E \equiv \Delta, E \qquad \text{if } \Gamma \equiv \Delta \text{ then } E, \Gamma \equiv E, \Delta$$

Premises and conclusions of rules are considered modulo the structural congruence over sequents. Three forms of rules are used to define MALL: axioms with no premise and one conclusion that always holds; and rules with either one or two premises, where the conclusion holds only if all of the premises hold. The forms of rules are expressed below.

$$\text{if } \Gamma \equiv \Gamma' \text{ and } \Delta \equiv \Delta' \text{ and } E \equiv E' \text{ and } \frac{\vdash \Gamma \quad \vdash \Delta}{\vdash E}, \text{ then } \frac{\vdash \Gamma' \quad \vdash \Delta'}{\vdash E'}$$

$$\text{if } \Gamma \equiv \Gamma' \text{ and } \Delta \equiv \Delta' \text{ and } \frac{\vdash \Gamma}{\vdash \Delta}, \text{ then } \frac{\vdash \Gamma'}{\vdash \Delta'}$$

$$\text{if } \Gamma \equiv \Delta \text{ and } \frac{}{\vdash \Gamma} \text{ then } \frac{}{\vdash \Delta}$$

We are deliberately putting more emphasis than normal on the structural rule of exchange, since harnessing this structural rule is central to the development of non-commutative logic in the forthcoming sections of this paper. Just removing exchange is insufficient to achieve a consistent non-commutative logical system. Removing the distinction between the object level and meta level syntax have been found to be critical [50] for the study of non-commutative operators in a proof calculus. For ease of comparison with the following sections a structural congruence style explanation of exchange is presented, rather than simply stating, as in the presentation by Girard [17], that exchange permutes all propositions in a sequent.

The object level propositions. Propositions are formed from units, atoms, negative atoms and binary operators. There is one unit written I. The grammar for propositions is defined as follows.

$$T ::= \text{I} \mid a \mid \overline{a} \mid T \otimes T \mid T \parallel T \mid T \oplus T \mid T \,\&\, T$$

The atoms of the calculus are drawn from some set of atomic propositions and can either be positive a or negative $\overline{a}$. The remaining syntactic constructs can be divided into multiplicative and additive constructs, hence the name multiplicative additive linear logic. The multiplicatives are the unit I, *times* $\otimes$ and *par* $\parallel$. The additives are *plus* $\oplus$ and *with* $\&$.

Derived concepts of negation and implication. Notice that in the syntax of propositions, only atoms are negated or *complemented*, using an overline. Negation is extended to all propositions by the following function that transforms a proposition into the complementary proposition in *negation normal form*, where negation applies only to atoms as permitted by the syntax.

$$\overline{\overline{a}} = a \qquad \overline{\text{I}} = \text{I} \qquad \overline{(T \otimes U)} = \overline{T} \parallel \overline{U} \qquad \overline{(T \parallel U)} = \overline{T} \otimes \overline{U}$$

$$\overline{(T \oplus U)} = \overline{T} \,\&\, \overline{U} \qquad \overline{(T \,\&\, U)} = \overline{T} \oplus \overline{U}$$

The above functions state that $\otimes$ and $\parallel$ are de Morgan dual to each other, as are $\oplus$ and $\&$; similarly to the de Morgan duality between *and* and *or* in classical logic. Similarly to classical logic, where classical implication $T \Rightarrow U$ is defined as *not* T *or* U, *linear implication*, written $V \multimap W$, is defined as $\overline{V} \parallel W$.

Rules for MALL. The propositions of the calculus are characterised by their deductive rules in Fig. 1.

The rules for multiplicative conjunction, *times* $\otimes$, and additive conjunction, *with* &, are equivalent in a classical setting, where the structural rules of weakening and contraction are permitted. By using the structural rule of weakening, that allows propositions in a sequent to be forgotten, $A \otimes B$ implies $A \mathbin{\&} B$ would be provable. By using the structural rule of contraction, that allows propositions in a sequent to be duplicated, $A \mathbin{\&} B$ implies $A \otimes B$ would be provable. However, neither weakening nor contraction are present in MALL, hence neither of the above two implications hold in general. Hence multiplicative and additive conjunction are distinguished operators.

The *with* rule for additive conjunction $A \mathbin{\&} B$ suggest that both A and B must hold the same given context. An additive disjunction $A \oplus B$ has a dual meaning where A or B must hold in the given context. Additive conjunction and disjunction define greatest lower bounds and least upper bounds respectively, in the lattice of propositions ordered by implication.

The intuition behind the multiplicative connectives is best understood in terms of resources and interaction. Both multiplicative conjunction (times $\otimes$) and multiplicative disjunction (par $\parallel$) indicate the partitioning of resources. The difference is that par permits interaction between atoms on either side of the operator, while times forbids interaction. The interactions are enacted by the *atomic interaction* rule where a positive and negative atom may cancel each other out. The *atomic interaction* rule has a more general form than normal that permits any preorder over atoms to be defined, where a preorder is a reflexive transitive relation. This enables what we will call *subsorting* over atoms, that we introduce due to applications of this work to subtyping [15, 11].

Considering propositions in a sequent as resources, the rules that partition resources are the *times* rule and the *mix* rule. The *mix* rule allows propositions in a sequent to be partitioned in any way, whereas the *times* rule ensures that the partition is chosen such that the two propositions separated by the multiplicative conjunction remain separate. The presence of the *mix* rule simplifies the calculus since there is only one self-dual multiplicative unit I [17], that we call simply *unit*. Elsewhere in the literature, presentations of MALL without the *mix* rule have two distinct multiplicative units, but most models of linear logic identify these units [2].

$$\frac{}{\vdash \text{I}}\ \textit{unit} \qquad \frac{\vdash a \leq b}{\vdash \overline{a} \parallel b}\ \textit{atomic interaction}$$

$$\frac{\vdash \Gamma, T \quad \vdash \Delta, U}{\vdash \Gamma, \Delta, T \otimes U}\ \textit{times} \qquad \frac{\vdash \Gamma, T, U}{\vdash \Gamma, T \parallel U}\ \textit{par} \qquad \frac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta}\ \textit{mix}$$

$$\frac{\vdash \Gamma, T \quad \vdash \Gamma, U}{\vdash \Gamma, T \mathbin{\&} U}\ \textit{with} \qquad \frac{\vdash \Gamma, T}{\vdash \Gamma, T \oplus U}\ \textit{left} \qquad \frac{\vdash \Gamma, U}{\vdash \Gamma, T \oplus U}\ \textit{right}$$

Figure 1: The deductive rules of MALL, where $\Gamma \not\equiv \text{I}$ and $\Delta \not\equiv \text{I}$ in the rule *mix*. In atomic interaction, $\vdash a \leq b$ is a conclusion for any deductive system defined such that $\leq$ is a preorder over atoms.

The proof theory. A proof in the sequent calculus is a tree of rules such that all leaves of the proof tree are axioms. Proofs in MALL enjoy a cut elimination result, which means that any proof established using the following *cut* rule can also be established without the *cut* rule.

$$\frac{\vdash \Gamma, U \quad \vdash \overline{U}, \Delta}{\vdash \Gamma, \Delta}\ \textit{cut}$$

In proof theory, a rule that can be added to a proof system without changing the propositions that are provable are called *admissible*. Thus the following result is a special case of Girard's cut elimination proof for linear logic [17], elaborated in several other references [38, 18].

Theorem 1 *The cut rule is admissible for MALL. Specifically, if there is a proof a proposition T using the rules of MALL and cut, then we can construct a proof of the proposition T using only the rules of MALL.*

The proof is *constructive* since the proof is an algorithm that transforms one proof into another proof. The cut elimination result can be regarded as a transitivity property of linear implication in MALL, since a corollary is that: if $\vdash T \multimap U$ and $\vdash U \multimap V$ hold, then $\vdash T \multimap V$ holds.

Several standard properties of MALL will be employed in this work. Firstly, the following result follows from a straightforward induction and establishes the reflexivity of implication.

Proposition 1 *For any proposition T, $\vdash \overline{T}, T$ holds. Consequently, the following axiom is admissible in* MALL.

$$\frac{}{\vdash \overline{T}, T}\ \textit{interaction}$$

Define a *MALL context* to be a context with one hole $\{\ \cdot\ \}$ constructed from the following grammar, where $\odot \in \{\otimes, \parallel, \oplus, \&\}$ and T is any proposition of MALL.

$$\mathcal{C}\{\ \ \} ::= \{\ \cdot\ \} \mid T \odot \mathcal{C}\{\ \ \} \mid \mathcal{C}\{\ \ \} \odot T$$

Note that negation is not part of the syntax of MALL, except over atoms, so cannot appear in the context. The absence of negation in contexts is to ensure that contexts preserve the direction of implication. Thereby, the following proposition follows by straightforward induction.

Proposition 2 *If $\vdash T \multimap U$ holds then, for any* MALL *context $\mathcal{C}\{\ \ \}$, it holds that $\vdash \mathcal{C}\{\ T\ \} \multimap \mathcal{C}\{\ U\ \}$.*

We also know that the fragment MALL is decidable, by the following result due to Lincoln et al. [33].

Theorem 2 *The problem of searching for a proof of a proposition in* MALL *is PSPACE-complete.*

The above result in the original paper by Lincoln et al. was for MALL without the *mix* rule or subsorting for atoms. However, neither the inclusion of the *mix* rule nor subsorting of atoms affect the proof of the above proposition, as long as the decision problem for subsorting of atoms is in PSPACE. Thus MALL is of the same complexity as intuitionistic propositional logic [43], relational algebra [51], and the canonical PSPACE-complete problem QBF, hence there exist mutual polynomial time encodings.

In anticipation of results later in the paper, we establish the following lemma.

Lemma 1 *The following propositions hold in* MALL*, assuming $\vdash a \leq b$.*

$$\vdash \mathrm{I} \multimap \overline{a} \parallel b \qquad\qquad \vdash T \otimes (U \parallel V) \multimap (T \otimes U) \parallel V$$

$$\vdash \mathrm{I} \multimap \mathrm{I} \mathbin{\&} \mathrm{I} \qquad\qquad \vdash T \multimap T \oplus U \qquad\qquad \vdash U \multimap T \oplus U$$

$$\vdash (T \parallel U) \mathbin{\&} (T \parallel V) \multimap T \parallel (U \mathbin{\&} V)$$

$$\vdash \left(\overline{P} \oplus \overline{Q}\right) \otimes \left(\overline{R} \oplus \overline{S}\right) \parallel (P \parallel R) \mathbin{\&} (Q \parallel S)$$

Proof: Assuming $\vdash a \leq b$ holds in the subsorting system, the following proofs hold.

$$\dfrac{\dfrac{\vdash a \leq b}{\vdash \overline{a} \parallel b}}{\vdash \text{I} \multimap \overline{a} \parallel b} \qquad\qquad \dfrac{\dfrac{\dfrac{}{\vdash \text{I}} \qquad \dfrac{}{\vdash \text{I}}}{\vdash \text{I} \,\&\, \text{I}}}{\vdash \text{I} \multimap \text{I} \,\&\, \text{I}}$$

By using the *interaction* axiom and the rules of MALL the following proofs can be constructed.

$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{T}, T} \qquad \dfrac{\dfrac{}{\vdash \overline{U}, U} \qquad \dfrac{}{\vdash \overline{V}, V}}{\vdash \left(\overline{U} \otimes \overline{V}\right), U, V}}{\vdash \overline{T}, \left(\overline{U} \otimes \overline{V}\right), (T \otimes U), V}}{\vdash T \otimes (U \parallel V) \multimap (T \otimes U) \parallel V} \qquad \dfrac{\dfrac{\dfrac{}{\vdash \overline{T}, T}}{\vdash \overline{T}, T \oplus U}}{\vdash T \multimap T \oplus U} \qquad \dfrac{\dfrac{\dfrac{}{\vdash \overline{U}, U}}{\vdash \overline{U}, T \oplus U}}{\vdash U \multimap T \oplus U}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \overline{T}, T} \qquad \dfrac{}{\vdash \overline{U}, U}}{\vdash \overline{T} \otimes \overline{U}, T, U}}{\vdash \left(\overline{T} \otimes \overline{U}\right) \oplus \left(\overline{T} \otimes \overline{V}\right), T, U} \qquad \dfrac{\dfrac{\dfrac{}{\vdash \overline{T}, T} \qquad \dfrac{}{\vdash \overline{V}, V}}{\vdash \overline{T} \otimes \overline{V}, T, V}}{\vdash \left(\overline{T} \otimes \overline{U}\right) \oplus \left(\overline{T} \otimes \overline{V}\right), T, V}}{\vdash \left(\overline{T} \otimes \overline{U}\right) \oplus \left(\overline{T} \otimes \overline{V}\right), T, U \,\&\, V}}{\vdash (T \parallel U) \,\&\, (T \parallel V) \multimap T \parallel (U \,\&\, V)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \overline{P \parallel R}, (P \parallel R)}}{\vdash \overline{P} \otimes \left(\overline{R} \oplus \overline{S}\right), (P \parallel R)}}{\vdash \left(\overline{P} \oplus \overline{Q}\right) \otimes \left(\overline{R} \oplus \overline{S}\right), (P \parallel R)} \qquad \dfrac{\dfrac{\dfrac{}{\overline{Q \parallel S}, (Q \parallel S)}}{\vdash \overline{Q} \otimes \left(\overline{R} \oplus \overline{S}\right), (Q \parallel S)}}{\vdash \left(\overline{P} \oplus \overline{Q}\right) \otimes \left(\overline{R} \oplus \overline{S}\right), (Q \parallel S)}}{\vdash \left(\overline{P} \oplus \overline{Q}\right) \otimes \left(\overline{R} \oplus \overline{S}\right), (P \parallel R) \,\&\, (Q \parallel S)}}{\vdash \left(\overline{P} \oplus \overline{Q}\right) \otimes \left(\overline{R} \oplus \overline{S}\right) \parallel (P \parallel R) \,\&\, (Q \parallel S)}$$

By Proposition 1, the above proofs also hold in MALL. □

The above lemma can be considered initially to be examples of proofs in MALL. However, the above lemma will be used in Section 5, where MALL is used as a reference to establish complexity results.

3 Introducing the Non-commutative Operator

By introducing a non-commutative operator in MAV, a new proof theoretic formalism is required, called the calculus of structures [20]. The calculus of structures enables certain logical systems that can not be expressed in the sequent calculus [50], to be treated proof theoretically.

A variety of logical systems, including the calculus BV, have been studied in the calculus of structures. BV is a conservative extension of multiplicative-only linear logic (with mix) extended with a self-dual non-commutative operator called *seq*. In this work, we consider a conservative extension of multiplicative-additive linear logic (with mix), as introduced in Section 2, with the self-dual non-commutative operator *seq*.

When introducing the calculus of structures [20], Guglielmi makes the following statements as one of his two major aims, further to the aim of a deeper understanding of the non-commutative logic called pomset logic [39] — a logic whose semantics is defined using generalised proof nets:

> If one wants to extend pomset logic to more expressive logics, then the sequent calculus usually is a better formalism than proof nets, because it is more versatile, for example with exponentials and additives.

Following the above stated aim, the versatility of the calculus of structures has been demonstrated by expressing the semantics of BV extended with exponentials, called NEL — a system that enjoys a generalised cut elimination result [49, 22], and is undecidable [46].

Straßburger [45] provides a proof of a generalised elimination result for propositional linear logic, including the additives, directly in the calculus of structures. Straßburger's work heavily inspires the proof in this paper. However, the presence of the non-commutative self-dual operator and also a self-dual unit considerably complicate the proof in this work. This paper is the first to explicitly and directly address a proof calculus where the additives and self-dual non-commutative operator *seq* coexist, in a system named multiplicative additive system virtual (MAV). MAV is an extension of basic system virtual (BV) and multiplicative additive linear logic (MALL).

The syntax of MAV. The syntax of MAV is the syntax of MALL extended with a non-commutative operator called *seq*. Seq was introduced in the system BV. The following grammar defines the syntax of propositions in

MAV.

$$
\begin{array}{rlll}
T ::= & \text{I} & & \text{unit} \\
| & a & & \text{positive atom} \\
| & \overline{a} & & \text{negative atom} \\
| & T \mathbin{;} T & & \text{sequential composition (seq)} \\
| & T \parallel T & & \text{parallel composition (par)} \\
| & T \otimes T & & \text{times} \\
| & T \oplus T & & \text{internal choice or plus} \\
| & T \mathbin{\&} T & & \text{external choice or with}
\end{array}
$$

We clarify the notation to facilitate comparison with related work. We use the notation $\parallel$ for par where elsewhere the notion $\parr$ or square brackets $[\,\cdot\,,\,\cdot\,]$ is used. This is to draw an intuitive connection between par and parallel composition operators in process calculi that permit interaction and interleaving. We use overline $\overline{a}$ to denote negative atoms, where elsewhere $a^{\perp}$ is used. This is to drawn an intuitive connection between negated atoms and output in process calculi. Also we prefer the semi-colon to the operator $\triangleleft$ or angular brackets $\langle\,\cdot\,;\,\cdot\,\rangle$ due to the ubiquitous use of the semi-colon for sequential composition. Work by Bruscoli [6] and forthcoming work by the authors on weak complete distributed simulation put the process calculus intuition on a precise foundation.

To reduce the number of brackets in propositions we assume an operator precedence. We assume that the multiplicatives times $\otimes$, par $\parallel$ and seq $;$ bind more strongly than the additives plus $\oplus$ and with $\&$.

The semantics of MAV. The semantics of MAV is defined by a term rewriting system modulo an equational theory. The rewrite rules and equational theory are presented in Fig. 2. As standard for term rewriting, the (bidirectional) equations can be applied at any point in a derivation, and the (unidirectional) rules can be applied in any context, where a context $\mathcal{C}\{\ \}$ is any proposition with one hole $\{\,\cdot\,\}$ in which any proposition can be plugged, as defined by the following grammar where $\odot \in \{;, \parallel, \otimes, \oplus, \&\}$ and T is any proposition.

$$\mathcal{C}\{\ \} ::= \{\,\cdot\,\} \mid T \odot \mathcal{C}\{\ \} \mid \mathcal{C}\{\ \} \odot T$$

Thus we have the following implicit rule for applying any rule in any context.

$$\mathcal{C}\{\ T\ \} \longrightarrow \mathcal{C}\{\ U\ \} \text{ only if } T \longrightarrow U \quad \text{context closure}$$

We also have the following congruence relation that serves a similar role to the exchange rule in the sequent calculus. The main differences compared to sequents is that exchange can occur deep within any context and can be applied to par, seq and times structures, not only par structures.

$$(T \parallel U) \parallel V \equiv T \parallel (U \parallel V) \qquad T \parallel U \equiv U \parallel V \qquad T \parallel \mathrm{I} \equiv T$$

$$(T \otimes U) \otimes V \equiv T \otimes (U \otimes V) \qquad T \otimes U \equiv U \otimes V \qquad T \otimes \mathrm{I} \equiv T$$

$$(T\,;U)\,;V \equiv T\,;(U\,;V) \qquad \mathrm{I}\,;T \equiv T \qquad T\,;\mathrm{I} \equiv T$$

Since equivalence is a congruence — a reflexive, transitive, symmetric relation that holds in any context — we have the following standard assumptions.

$$T \equiv T \qquad \text{if } T \equiv U \text{ and } U \equiv V\text{, then } T \equiv V$$

$$\text{if } T \equiv U \text{ then } U \equiv T \qquad \text{if } T \equiv U \text{ then } \mathcal{C}\{\ T\ \} \equiv \mathcal{C}\{\ U\ \}$$

The equational system ensures that $(T, ;, \mathrm{I})$ is a monoid, and both $(T, \parallel, \mathrm{I})$ and $(T, \otimes, \mathrm{I})$ are commutative monoids. To quotient propositions by the equational theory defined above, the following congruence rule can always be applied to any rule.

$$\text{if } V \equiv T \text{ and } T \longrightarrow U \text{ and } U \equiv W\text{, then } V \longrightarrow W \quad \text{congruence}$$

The term rewriting system in Fig 2 defines the deductive rules of multiplicative additive system virtual (MAV). We briefly explain the rewrite rules.

- The atomic interaction rules enable a negative atom and positive atom to annihilate each other, whenever the negated atom is a subsort of the positive atom. The only assumptions are: firstly, to preserve consistency, the subsorting system must define a preorder (a reflexive transitive relation); secondly, to preserve the time complexity bound, the complexity of determining whether one atom is a subsort of another atom must be in PSPACE.

  Permitting any preorder as a subsorting relation enables considerable creativity. For example, in the companion paper for this work [11], the authors define atoms such that they carry the type of message exchanged in a protocol. For example, if sorts are regular expression

$$\mathrm{I} \mathbin{\&} \mathrm{I} \longrightarrow \mathrm{I} \quad \textit{tidy} \qquad\qquad \overline{a} \parallel b \longrightarrow \mathrm{I} \text{ only if} \vdash a \leq b \quad \textit{atomic interaction}$$

$$(T \otimes U) \parallel V \longrightarrow T \otimes (U \parallel V) \quad \textit{switch}$$

$$(T \,;\, U) \parallel (V \,;\, W) \longrightarrow (T \parallel V) \,;\, (U \parallel W) \quad \textit{sequence}$$

$$T \oplus U \longrightarrow T \quad \textit{left} \qquad\qquad T \oplus U \longrightarrow U \quad \textit{right}$$

$$(T \mathbin{\&} U) \parallel V \longrightarrow (T \parallel V) \mathbin{\&} (U \parallel V) \quad \textit{external}$$

$$(T \,;\, U) \mathbin{\&} (V \,;\, W) \longrightarrow (T \mathbin{\&} V) \,;\, (U \mathbin{\&} W) \quad \textit{medial}$$

Figure 2: Term rewriting system modulo an equational theory for MAV.

types for XML [27], the subsorting can be induced by a subtype system, which defines a preorder hence preserves consistency but increases time complexity since subtyping is EXPTIME-complete. In contrast, when sorts are any partial order over finite types (without recursive types) defined by a finite number of subtype inequalities [14], then the complexity class is also preserved.

- The *switch* rule captures the essence of the rule for times in linear logic. The rule focuses a parallel composition on where an interaction takes place and forbids interaction elsewhere. A similar rule appears in categorical models of linear logic [12].

- The *sequence* rule arises in the theory of pomsets [19]. The rules also appears in concurrent Kleene algebras [23]. The rule strengthens causal dependencies. If we consider two parallel propositions to be two threads, then seq introduced a barrier across two parallel threads where there is a certain point that both threads must have reached before either thread can proceed.

- The *left* and *right* rules represent an internal choice where we, as the prover or designer of a runtime, have control over the branch to select. The *external* rule represents when we the prover cannot determine which branch will be selected; hence must analyse both possibilities as independent branches of the proof in parallel. The *tidy* rule simply acknowledges when two branches in an external choice have both completed successfully.

We assume that following restrictions, to avoid rules that can be applied infinitely. The most subtle case below is for the *medial* rule, which will be explained when required in the proofs.

- The *switch* rule is such that $T \not\equiv \mathrm{I}$ and $V \not\equiv \mathrm{I}$.
- The *sequence* rule is such that $T \not\equiv \mathrm{I}$ and $W \not\equiv \mathrm{I}$.
- The *external* rule is such that $V \not\equiv \mathrm{I}$.
- The *medial* rule is such that: either $P \not\equiv \mathrm{I}$ or $R \not\equiv \mathrm{I}$, and also either $Q \not\equiv \mathrm{I}$ or $S \not\equiv \mathrm{I}$.

Since rules can only be applied finitely, proof search is finite. Thereby, MAV defines an *analytic* proof system, which is a system that behaves well for proof search. The exact definition of an analytic proof system varies depending on the proof calculus, but hinges on the rules being *finitely generating*. For a discussion on analytic proof systems in the calculus of structures see [7].

We extend the complementation operator, overline, to all propositions using the following function that transforms a proposition into its complementary proposition. The only new case compared to the complementation operator for MALL in Section 2 is for the non-commutative operator *seq*.

$$\overline{\overline{a}} = a \qquad \overline{\mathrm{I}} = \mathrm{I} \qquad \overline{(T \otimes U)} = \overline{T} \parallel \overline{U} \qquad \overline{(T \parallel U)} = \overline{T} \otimes \overline{U}$$

$$\overline{P \mathbin{;} Q} = \overline{P} \mathbin{;} \overline{Q} \qquad \overline{(T \oplus U)} = \overline{T} \mathbin{\&} \overline{U} \qquad \overline{(T \mathbin{\&} U)} = \overline{T} \oplus \overline{U}$$

The above function transforms any proposition into a proposition in *negation normal form*, where complementation applies only to atoms, as permitted by the syntax of propositions. We deliberately do not include complementation for arbitrary propositions in the syntax for propositions, since the contravariant nature of complementation complicates the rewriting system without any gain in expressive power [20].

Proofs in MAV. In the calculus of structures a *proof* is a special derivation that reduces to the unit, where the unit represents a successfully completed proof. As a slight abuse of notation, $\longrightarrow$ denotes its own reflexive and transitive closure.

Definition 1 *A derivation $T \longrightarrow U$ of length 0, holds only if $T \equiv U$. Given a derivation $P \longrightarrow Q$ of length n and a rule instance $Q \longrightarrow R$, $P \longrightarrow R$ is a derivation of length $n+1$.*

If for any derivation $T \longrightarrow \mathrm{I}$ holds according to the term rewriting system of MAV, then we write $\vdash T$, and say that T is provable.

As with MALL, complementation is used to define linear implication in MAV, where $T \multimap U$ is defined as $\overline{T} \parallel U$. Since linear implication involves complementation, linear implication is not part of the syntax of propositions but is a derived concept. The consistency of MAV can be seen as establishing that the relation defined by all provable linear implications is a preorder, i.e. a reflexive transitive closed relation.

Reflexivity. Reflexivity of linear implication can be established straightforwardly. Since $T \multimap T$ is defined as $\overline{T} \parallel T$, the following proposition is simply a reflexivity property of linear implication in MAV.

Proposition 3 (Reflexivity) *For any proposition T, $\vdash \overline{T} \parallel T$ holds.*

Proof: The proof proceeds by induction on the structure of T.

The base cases for any atom a follows immediately from the atomic interaction rule. Since subsorting over atoms is reflexive, $\vdash \overline{a} \parallel a$. The base case for the unit is immediate by definition of a proof.

For the induction hypothesis assume that $\vdash \overline{T} \parallel T$ and $\vdash \overline{U} \parallel U$. Thereby, the following cases hold.

Consider when the root connective in the proposition is the *times* operator. The following proof holds, by *switch* and the induction hypothesis.

$$\overline{(T \otimes U)} \parallel (T \otimes U) = \quad \overline{T} \parallel \overline{U} \parallel (T \otimes U) \longrightarrow \left(\overline{T} \parallel T\right) \otimes \left(\overline{U} \parallel U\right) \longrightarrow \mathrm{I}$$

The case when the root connective is the *par* operator is symmetric to the above.

Consider when the root connective in the proposition is the *seq* operator. The following proof holds, by the *sequence* rule and the induction hypothesis.

$$\overline{(T \mathbin{;} U)} \parallel (T \mathbin{;} U) = \quad \left(\overline{T} \mathbin{;} \overline{U}\right) \parallel (T \mathbin{;} U) \longrightarrow \left(\overline{T} \parallel T\right) \mathbin{;} \left(\overline{U} \parallel U\right) \longrightarrow \mathrm{I}$$

Consider when the root connective in the proposition is &, the *external choice* operator. By induction, *external*, *left*, *right*, and *tidy*, the following proof holds.

$$\begin{array}{rl} \overline{(T \mathbin{\&} U)} \parallel (T \mathbin{\&} U) = & \left(\overline{T} \oplus \overline{U}\right) \parallel (T \mathbin{\&} U) \\ \longrightarrow & \left(\overline{T} \oplus \overline{U}\right) \parallel T \mathbin{\&} \left(\overline{T} \oplus \overline{U}\right) \parallel U \\ \longrightarrow & \overline{T} \parallel T \mathbin{\&} \overline{U} \parallel U \\ \longrightarrow & \mathrm{I} \mathbin{\&} \mathrm{I} \longrightarrow \mathrm{I} \end{array}$$

The case for when internal choice, $\oplus$, is the root connective is symmetric to the case for external choice.

This completes the case analysis. Therefore, by induction on the size of the negated proposition, the proposition holds. $\square$

Cut elimination. The main result of this paper is the key result required to establish that linear implication is a transitive relation. The following result is a generalisation of a consistency result called *cut elimination* that appears commonly in proof theory.

Theorem 3 (Cut elimination) *For any proposition T, if $\vdash \mathcal{C}\{\, T \otimes \overline{T} \,\}$, then $\vdash \mathcal{C}\{\, \mathrm{I} \,\}$.*

The above theorem can be stated alternatively by supposing that there is a proof in MAV that also uses the extra rule:

$$\mathrm{I} \longrightarrow T \otimes \overline{T} \quad \text{(co-interact)}$$

Given such a proof, a new proof can be constructed that uses only the rules of MAV. In this case, we say that the rule co-interact is *admissible*.

The proof of Theorem 3 involves a technique known as *splitting* introduced in [20]. The following section proves the necessary lemmata to establish the above theorem.

Before proceeding with lemmata, we provide a corollary that demonstrates that a consequence of cut elimination is indeed that linear implication defines a preorder. A stronger statement is proven: since implication is preserved in any context, it is a precongruence.

Corollary 1 *Linear implication is a precongruence — a reflexive transitive relation that holds in any context.*

Proof: For reflexivity, $T \multimap T$ holds immediately by Proposition 3.

For transitivity, suppose that $T \multimap U$ and $U \multimap V$ hold. Thereby the following proof can be constructed.

$$\left(\overline{T} \parallel \left(U \otimes \overline{U}\right) \parallel V\right) \longrightarrow \left(\overline{T} \parallel U\right) \otimes \left(\overline{U} \parallel V\right) \longrightarrow \mathrm{I}$$

Hence, by Theorem 3, $\vdash \overline{T} \parallel V$ as required.

For contextual closure, assume that $T \multimap U$ holds. By Proposition 3, and *switch* we can construct the following proof.

$$\begin{array}{rl} \overline{\mathcal{C}\{\ T\ \}} \parallel \mathcal{C}\{\ \left(T \otimes \overline{T}\right) \parallel U\ \} & \longrightarrow \overline{\mathcal{C}\{\ T\ \}} \parallel \mathcal{C}\{\ T \otimes \left(\overline{T} \parallel U\right)\ \} \\ & \longrightarrow \overline{\mathcal{C}\{\ T\ \}} \parallel \mathcal{C}\{\ T\ \} \longrightarrow \mathrm{I} \end{array}$$

Hence by Theorem 3, $\vdash \overline{\mathcal{C}\{\ T\ \}} \parallel \mathcal{C}\{\ U\ \}$ as required. □

Disussion on the medial rule. Most rules of the calculus are either lifted directly from BV or directly from a system for MALL in the calculus of structures, such as LS [44]. The exception is the *medial* rule.

$$(P\ ;\ Q) \mathbin{\&} (R\ ;\ S) \longrightarrow (P \mathbin{\&} R)\ ;\ (Q \mathbin{\&} S) \quad \text{medial}$$

To consider a situation where this *medial* rule is necessary consider the following example propositions, with atoms a to j.

$$\begin{array}{rl} Q \triangleq & \left(\overline{a}\ ;\ \left(\overline{b}\ ;\ \overline{c} \mathbin{\&} \overline{d}\ ;\ \overline{e}\right)\right) \parallel \left(\overline{f}\ ;\ \left(\overline{g}\ ;\ \overline{h} \mathbin{\&} \overline{i}\ ;\ \overline{j}\right)\right) \\ R \triangleq & (a\ ;\ (b \oplus d)\ ;\ (c \oplus e)) \otimes (f\ ;\ (g \oplus i)\ ;\ (h \oplus j)) \\ S \triangleq & ((a\ ;\ (b \oplus d)) \otimes (f\ ;\ (g \oplus i)))\ ;\ ((c \oplus e) \otimes (h \oplus j)) \end{array}$$

Now notice that, without the *medial* rule the following implications are provable: $\vdash \overline{Q} \multimap R$ and $\vdash R \multimap S$. Therefore, for a system satisfying cut elimination and hence with a transitive implication, we would expect that $\vdash \overline{Q} \multimap S$ holds. However, if we exclude the *medial* rule from MAV then $\vdash \overline{Q} \multimap S$ does not hold.

If we include the *medial* rules in MAV, then we can establish the following proof of $\vdash \overline{Q} \multimap S$, where firstly the *medial* rule is applied twice inside Q, secondly the *sequence* rule is applied twice, and finally reflexivity of implication is applied twice.

$$\begin{array}{rl} Q \parallel S \longrightarrow & \left(\overline{a}\ ;\ \left(\overline{b} \mathbin{\&} \overline{d}\right)\ ;\ \left(\overline{c} \mathbin{\&} \overline{e}\right)\right) \parallel \left(\overline{f}\ ;\ \left(\left(\overline{g} \mathbin{\&} \overline{i}\right)\ ;\ \left(\overline{h} \mathbin{\&} \overline{j}\right)\right)\right) \\ \parallel & (((a\ ;\ (b \oplus d)) \otimes (f\ ;\ (g \oplus i)))\ ;\ ((c \oplus e) \otimes (h \oplus j))) \\ \\ \longrightarrow & \left(\left(\overline{a}\ ;\ \left(\overline{b} \mathbin{\&} \overline{d}\right)\right) \parallel \left(\overline{f}\ ;\ \left(\overline{g} \mathbin{\&} \overline{i}\right)\right) \parallel ((a\ ;\ (b \oplus d)) \otimes (f\ ;\ (g \oplus i)))\right)\ ; \\ & \left(\left(\overline{c} \mathbin{\&} \overline{e}\right) \parallel \left(\overline{h} \mathbin{\&} \overline{j}\right) \parallel ((c \oplus e) \otimes (h \oplus j))\right) \\ \\ \longrightarrow & \mathrm{I} \end{array}$$

Thus the *medial* rule is sufficient to achieve transitivity of implication in this case. The fact that it is sufficient in all cases is of course established by the main cut elimination result of this paper.

4 Splitting, Context Reduction and Elimination

Proofs of generalised cut elimination results in the calculus of structures can be achieved through several means. Several approaches were investigated in obtaining the current proofs presented. Before proceeding further we briefly explain why the current approach has been adopted.

For classical propositional logic, a graphical normalisation approach, called *atomic flows* [21], has been developed. Atomic flows are graphs that track the contraction and interaction of atoms in proofs. Unfortunately, atomic flows have not yet been successfully adapted to logics based on linear logic, such as MALL. This is likely to be because current work on atomic flows relies on an interplay between interaction and contraction that cannot be exploited when, as in linear logic, contraction applies only to the additives while interaction applies only to the multiplicatives. However, we suspect that further insight into cut elimination can be gleaned from adapting atomic flows. The hint that such an approach may be possible is that the medial rule that mysteriously appears in MAV, arises naturally when contraction is reduced to an atomic form [44].

Another approach, used for the non-commutative exponential system NEL [49] is to apply a technique called *decomposition* that decomposes a proof into normal forms where rules are applied in a certain order. The decomposition result for NEL is complex. The proof requires a vast case analysis and a complex termination measure. Part of the difficulty with decomposition is that it is related to results in proof theory that are known to be difficult, such as interpolation [36]. Thus proving a decomposition result in order to prove cut elimination is likely to be tackling a harder result than necessary.

Thus our approach proceeds by proving the splitting lemma more directly [22], without a decomposition result. However, the decomposition technique influences the approach in this work, since the splitting proof handles operators in a specific order — firstly the *with* operator is treated, secondly the *multiplicatives* are treated simultaneously, finally the plus operator and atoms are handled. This suggests that there is probably also a proof using the decomposition technique.

The main challenge in this section is devising a termination measure that handles a key case where the associativity of *seq* and the one-way distributivity of *with* over *seq* interact badly.

4.1 Branching and Splitting

The reason that proofs in MAV are more complex than BV, which is NP-complete [30], is the presence of the *with* operator $\&$. The presence of *with* operators can result in an exponential number of independent branches to fully explore during proof search. However, in MALL, each independent branch of a proof is polynomial in the size of the syntax tree of the proposition proven. This is the basis of the argument that MALL is in PSPACE, as expressed in Theorem 2. A similar argument applies to the system MAV, as applied in Section 5.

The trick to control the complexity of normalisation is to hide independent branches of a proof. To illustrate the technique, we provide an example of a derivation before proving the lemma in general. Consider the following annotated derivation, assuming the following subsorting over atoms: $\vdash a \leq c$, $\vdash b \leq c$, $\vdash a \leq d$, $\vdash b \leq d$.

$$
\begin{aligned}
\left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel (c \mathbin{\&} (d \oplus e)) \longrightarrow\ & \left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel (c \mathbin{\&} d) \\
\longrightarrow\ & \left(\left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel c\right) \mathbin{\&} \left(\left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel d\right) \\
\longrightarrow\ & \left((\overline{a} \parallel c)\ \underline{\boldsymbol{\&}\ \left(\overline{b} \parallel c\right)}\right) \mathbin{\&} \left(\left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel d\right) \\
\longrightarrow\ & \left(\mathrm{I}\,\underline{\boldsymbol{\&}\ \left(\overline{b} \parallel c\right)}\right) \mathbin{\&} \left(\left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel d\right) \\
\longrightarrow\ & \left(\mathrm{I}\,\underline{\boldsymbol{\&}\,\mathrm{I}}\right) \mathbin{\&} \left(\left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel d\right) \\
\longrightarrow\ & \mathrm{I} \mathbin{\&} \left(\left(\overline{a}\,\underline{\boldsymbol{\&}\,\overline{b}}\right) \parallel d\right) \\
\longrightarrow\ & \mathrm{I} \mathbin{\&} \left((\overline{a} \parallel d)\ \underline{\boldsymbol{\&}\ \left(\overline{b} \parallel d\right)}\right) \\
\longrightarrow\ & \mathrm{I} \mathbin{\&} \left(\mathrm{I}\,\underline{\boldsymbol{\&}\ \left(\overline{b} \parallel d\right)}\right) \\
\longrightarrow\ & \mathrm{I} \mathbin{\&} \left(\mathrm{I}\,\underline{\boldsymbol{\&}\,\mathrm{I}}\right) \longrightarrow \mathrm{I} \mathbin{\&} \mathrm{I} \longrightarrow \mathrm{I}
\end{aligned}
$$

In the above derivation, one of the with operators is highlighted in bold $\boldsymbol{\&}$ and the term to the right of the operator is underscored. This indicates that we aim to hide the right branch of that operator, leaving only the part of the proposition not underlined, as performed by a function ℓ over propositions. The function ℓ is defined as follows, where $\odot \in \{;, \parallel, \otimes, \oplus, \&\}$ is any (non-bold) binary connective and $k \in \{a, \overline{a}, \mathrm{I}\}$ is any atom or constant proposition.

$$\ell\,(T \mathbin{\boldsymbol{\&}} U) = T \qquad \ell\,(T \odot U) = \ell(T) \odot \ell(U) \qquad \ell(k) = k$$

By applying the function ℓ to the propositions at each step in the above proof and by removing steps that become redundant, we obtain the following valid proof.

$$\begin{array}{rl} \overline{a} \parallel (c \mathbin{\&} (d \oplus e)) \longrightarrow & \overline{a} \parallel (c \mathbin{\&} d) \\ \longrightarrow & (\overline{a} \parallel c) \mathbin{\&} (\overline{a} \parallel d) \\ \longrightarrow & \mathrm{I} \mathbin{\&} (\overline{a} \parallel d) \\ \longrightarrow & \mathrm{I} \mathbin{\&} \mathrm{I} \longrightarrow \mathrm{I} \end{array}$$

Notice in the example derivation above that there are two *with* operators initially, indicated by $\boldsymbol{\&}$ and $\&$, where we do not want to delete the right branch of the later. Also notice that, in the course of a derivation the bold *external choice* or *with* is duplicated by the *external* rule acting over a non-bold *with* operator, hence there may be multiple bold occurrences of *with* in a proposition.

By generalising the above observations, the following lemma is obtained. The lemma states that we can split a proof involving the *with* operator & into two proofs.

Lemma 2 (Branching) *If* $\vdash \mathcal{C}\{\ T \mathbin{\&} U\ \}$ *then both* $\vdash \mathcal{C}\{\ T\ \}$ *and* $\vdash \mathcal{C}\{\ U\ \}$.

Proof: The proof works by constructing two proofs such that the respective left and right formula of the with connective are removed. To do so, we remove deductive rules that either involve the with connective concerned, or appear inside the branch to be removed. We provide only the case where the left branch is selected, the other case is symmetric.

The induction hypothesis is that if T has a proof of length n, then we can construct a proof of $\ell(T)$. The base case is when $\ell(T) = T$ (e.g. when $T = \mathrm{I}$), in which case we are done. The inductive cases are listed below.

Consider when the bottommost rule of a proof involves a bold *with* as follows:

$$\mathcal{C}\{\ T \mathbin{\boldsymbol{\&}} \mathcal{D}\{\ U\ \}\ \} \longrightarrow \mathcal{C}\{\ T \mathbin{\boldsymbol{\&}} \mathcal{D}\{\ V\ \}\ \}$$

where $\mathcal{C}\{\ T \mathbin{\boldsymbol{\&}} \mathcal{D}\{\ V\ \}\ \}$ has a proof of length n. Hence, by the induction hypothesis, $\vdash \ell\,(\mathcal{C}\{\ T \mathbin{\boldsymbol{\&}} \mathcal{D}\{\ V\ \}\ \})$ holds. Furthermore, $\ell\,(\mathcal{C}\{\ T \mathbin{\boldsymbol{\&}} \mathcal{D}\{\ V\ \}\ \}) = \ell\,(\mathcal{C}\{\ T \mathbin{\boldsymbol{\&}} \mathcal{D}\{\ U\ \}\ \})$. Hence $\vdash \ell\,(\mathcal{C}\{\ T \mathbin{\boldsymbol{\&}} \mathcal{D}\{\ U\ \}\ \})$ holds, as required.

Consider when the bottommost rule of a proof involves a bold *with* as follows:

$$\mathcal{C}\{\ (T \mathbin{\&} U) \parallel V\ \} \longrightarrow \mathcal{C}\{\ (T \parallel V) \mathbin{\&} (U \parallel V)\ \}$$

where $\mathcal{C}\{\ (T \parallel V) \mathbin{\&} (U \parallel V)\ \}$ has a proof of length n. By the induction hypothesis, $\vdash \ell\,(\mathcal{C}\{\ (T \parallel V) \mathbin{\&} (U \parallel V)\ \})$ holds. Furthermore, it is clear that $\ell\,(\mathcal{C}\{\ (T \parallel V) \mathbin{\&} (U \parallel V)\ \}) = \ell\,(\mathcal{C}\{\ (T \mathbin{\&} U) \parallel V\ \})$. Thereby $\vdash \ell\,(\mathcal{C}\{\ (T \mathbin{\&} U) \parallel V\ \})$ holds, as required.

Consider when the bottommost rule of a proof involves a bold *with* operator as follows:

$$\mathcal{C}\{\ (T\ ;U) \mathbin{\&} (V\ ;W)\ \} \longrightarrow \mathcal{C}\{\ (T \mathbin{\&} V)\ ;(U \mathbin{\&} W)\ \}$$

where $\mathcal{C}\{\ (T \mathbin{\&} V)\ ;(U \mathbin{\&} W)\ \}$ has a proof of length n. By the induction hypothesis, $\vdash \ell\,(\mathcal{C}\{\ (T \mathbin{\&} V)\ ;(U \mathbin{\&} W)\ \})$ holds. Furthermore, it is clear that $\ell\,(\mathcal{C}\{\ (T \mathbin{\&} V)\ ;(U \mathbin{\&} W)\ \}) = \ell\,(\mathcal{C}\{\ (T\ ;U) \mathbin{\&} (V\ ;W)\ \})$. Thereby $\vdash \ell\,(\mathcal{C}\{\ (T\ ;U) \mathbin{\&} (V\ ;W)\ \})$ holds, as required.

Consider the case where $\mathcal{C}\{\ \mathrm{I} \mathbin{\&} \mathrm{I}\ \} \longrightarrow \mathcal{C}\{\ \mathrm{I}\ \}$, where $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$ has a proof of length n. By the induction hypothesis, $\vdash \ell\,(\vdash \mathcal{C}\{\ \mathrm{I}\ \})$ holds. Furthermore $\ell\,(\mathcal{C}\{\ \mathrm{I} \mathbin{\&} \mathrm{I}\ \}) = \ell\,(\mathcal{C}\{\ \mathrm{I}\ \})$; hence $\vdash \ell\,(\mathcal{C}\{\ \mathrm{I} \mathbin{\&} \mathrm{I}\ \})$ as required.

In all other cases, $\mathcal{C}\{\ T\ \} \longrightarrow \mathcal{C}\{\ U\ \}$, by any rule, such that $\mathcal{C}\{\ T\ \}$ has a proof of length n and also $\ell\,(\mathcal{C}\{\ T\ \}) \not\equiv \ell\,(\mathcal{C}\{\ U\ \})$. By induction, $\vdash \ell\,(\mathcal{C}\{\ U\ \})$ holds. Therefore, by applying the same rule, we can obtain a proof of $\ell\,(U)$.

All cases are exhausted, thereby if $\vdash T$ holds then $\vdash \ell(T)$ for any length of proof. Whence, by assuming that $\mathcal{C}\{\ T \mathbin{\&} U\ \}$ holds, we can construct a proof of $\ell\,(\mathcal{C}\{\ T \mathbin{\&} U\ \}) = \mathcal{C}\{\ T\ \}$. A symmetric argument using a right projection on the bold *with* operator constructs a proof of $\mathcal{C}\{\ U\ \}$. □

Killing contexts. To handle branching caused by the with operator, all independent branches of a proof must be tracked until they are all completed. To track independent branches of a proof search, similarly to Straßburger [45, 9], we require the following notion of a killing context.

Definition 2 *An n-ary killing context $\mathcal{T}\{\ \ \}$ is a context with n holes such that:*

- *if $n = 1$, then $\mathcal{T}\{\ \ \} = \{\ \cdot\ \}$ where $\{\ \cdot\ \}$ is a hole into which any proposition can be plugged;*

- *if $m \geq 1$ and $n \geq 1$, then if $\mathcal{T}^0\{\ \}$ is a m-ary killing context and $\mathcal{T}^1\{\ \}$ is an n-ary killing context, then $\mathcal{T}^0\{\ \}\&\mathcal{T}^1\{\ \}$ is a $(m+n)$-ary killing context.*

Killing contexts have several nice properties. Firstly, if you fill all holes with the unit, then the resulting proposition is provable. Secondly, killing contexts distribute over parallel composition, as expressed in the following lemma.

Lemma 3 *For any killing context $\mathcal{T}\{\ \}$, $\vdash \mathcal{T}\{\ \mathrm{I}, \ldots, \mathrm{I}\ \}$ and the following derivation holds.*

$$T \parallel \mathcal{T}\{\ U_1, U_2, \ldots U_n\ \} \longrightarrow \mathcal{T}\{\ T \parallel U_1, T \parallel U_2, \ldots T \parallel U_n\ \}$$

Proof: The proofs follow by straightforward inductions over the structure of a killing context.

There are two base cases. When the killing context is the top only $T \parallel \top \longrightarrow \top$ and $\top \longrightarrow \mathrm{I}$, as required. When the killing context is one hole only $T \parallel \{\ U\ \} = \{\ T \parallel U\ \}$ and $\{\ \mathrm{I}\ \} = \mathrm{I}$, as required. Now assume that by the induction hypothesis the following hold for killing contexts $\mathcal{T}^1\{\ \}$ and $\mathcal{T}^2\{\ \}$, and also $\vdash \mathcal{T}^1\{\ \mathrm{I}, \ldots, \mathrm{I}\ \}$ and $\vdash \mathcal{T}^2\{\ \mathrm{I}, \ldots, \mathrm{I}\ \}$.

$$\begin{aligned} T \parallel \mathcal{T}^1\{\ U_1, \ldots, U_m\ \} &\longrightarrow \mathcal{T}^1\{\ T \parallel U_1, \ldots, T \parallel U_m\ \} \\ T \parallel \mathcal{T}^2\{\ U_{m+1}, \ldots, U_{m+n}\ \} &\longrightarrow \mathcal{T}^2\{\ T \parallel U_{m+1}, \ldots, T \parallel U_{m+n}\ \} \end{aligned}$$

Hence, by distributivity the following derivation can be constructed.

$$\begin{aligned} & T \parallel \left(\mathcal{T}^1\{\ U_1, \ldots, U_m\ \} \,\&\, \mathcal{T}^2\{\ U_{m+1}, \ldots, U_{m+n}\ \}\right) \\ & \quad \longrightarrow T \parallel \mathcal{T}^1\{\ U_1, \ldots, U_m\ \} \,\&\, T \parallel \mathcal{T}^2\{\ U_{m+1}, \ldots, U_{m+n}\ \} \\ & \quad \longrightarrow \mathcal{T}^1\{\ T \parallel U_1, \ldots, T \parallel U_m\ \} \,\&\, \mathcal{T}^2\{\ T \parallel U_{m+1}, \ldots, T \parallel U_{m+n}\ \} \end{aligned}$$

Furthermore, $\mathcal{T}^1\{\ \mathrm{I}, \ldots, \mathrm{I}\ \} \,\&\, \mathcal{T}^2\{\ \mathrm{I}, \ldots, \mathrm{I}\ \} \longrightarrow \mathrm{I} \,\&\, \mathrm{I} \longrightarrow \mathrm{I}$ holds. □

For readability of large formulae involving an n-ary killing context, $\mathcal{T}\{\ \}$ and family of n propositions U_1, U_2, …, U_n, we introduce the shortcut notion. $\mathcal{T}\{\ U_i \colon 1 \leq i \leq n\ \}$ is a shortcut for $\mathcal{T}\{\ U_1, U_2, \ldots, U_n\ \}$. In special cases, we also use the notation $\mathcal{T}\{\ U_i \colon i \in I\ \}$ where I is a finite subset of natural numbers indexing U_i.

The following lemma is used for the most troublesome case in the splitting lemma. It is critical for coping with the sequential operator in the precence of the additives — the only case of the splitting lemma that demands the *medial* rule. The case analysis considers carefully the restiction on the *medial* rule, by using the obseration that $(P \mathbin{;} \mathrm{I}) \,\&\, (Q \mathbin{;} \mathrm{I}) \equiv (P \,\&\, Q) \mathbin{;} \mathrm{I}$ and hence the *medial* rule is not required in such cases.

Lemma 4 *Assume that I is a finite subset of natural numbers, P_i and Q_i are propositions, for $i \in I$, and $\mathcal{T}\{\ \}$ is an n-ary killing context. There exist killing contexts $\mathcal{T}^0\{\ \}$ and $\mathcal{T}^1\{\ \}$ and sets of natural numbers $J \subseteq I$ and $K \subseteq I$ such that the following derivation holds.*

$$\mathcal{T}\{\ P_i \mathbin{;} Q_i \colon i \in I\ \} \longrightarrow \mathcal{T}^0\{\ P_j \colon j \in J\ \} \mathbin{;} \mathcal{T}^1\{\ Q_k \colon k \in K\ \}$$

Proof: Proceed by induction on the structure of the killing context. For the base, case consider the killing context consisting of one hole, hence $\{P \mathbin{;} Q\} = \{P\} \mathbin{;} \{Q\}$, as required.

Now consider the case for a $(m+n)$-ary killing context defined as follows.

$$\mathcal{T}^0\{\ P_i \mathbin{;} Q_i \colon i \in I_0\ \} \mathbin{\&} \mathcal{T}^1\{\ P_i \mathbin{;} Q_i \colon i \in I_1\ \}$$

There are three cases to consider. If $P_i \equiv \text{I}$, for all $i \in I_0 \cup I_1$, then the following equivalence holds.

$$\begin{aligned} &\mathcal{T}^0\{\ P_i \mathbin{;} Q_i \colon i \in I_0\ \} \mathbin{\&} \mathcal{T}^1\{\ P_i \mathbin{;} Q_i \colon i \in I_1\ \} \\ &\qquad\qquad \equiv \text{I} \mathbin{;} \mathcal{T}^0\{\ Q_i \colon i \in I_0\ \} \mathbin{\&} \mathcal{T}^1\{\ Q_i \colon i \in I_1\ \} \end{aligned}$$

Similarly, if $Q_i \equiv \text{I}$ for all $i \in I_0 \cup I_1$, then the following equivalence holds.

$$\begin{aligned} &\mathcal{T}^0\{\ P_i \mathbin{;} Q_i \colon i \in I_0\ \} \mathbin{\&} \mathcal{T}^1\{\ P_i \mathbin{;} Q_i \colon i \in I_1\ \} \\ &\qquad\qquad \equiv \mathcal{T}^0\{\ P_i \colon i \in I_0\ \} \mathbin{\&} \mathcal{T}^1\{\ P_i \colon i \in I_1\ \} \mathbin{;} \text{I} \end{aligned}$$

Otherwise, by induction we have the following derivations where $J_0 \subseteq I_0$, $K_0 \subseteq I_0$, $J_1 \subseteq I_1$ and $K_1 \subseteq I_1$.

$$\mathcal{T}^0\{\ P_i \mathbin{;} Q_i \colon i \in I_0\ \} \longrightarrow \mathcal{T}^0_0\{\ P_j \colon j \in J_0\ \} \mathbin{;} \mathcal{T}^0_1\{\ Q_k \colon k \in K_0\ \}$$

$$\mathcal{T}^1\{\ P_i \mathbin{;} Q_i \colon i \in I_1\ \} \longrightarrow \mathcal{T}^1_0\{\ P_j \colon j \in J_1\ \} \mathbin{;} \mathcal{T}^1_1\{\ Q_k \colon k \in K_1\ \}$$

Hence by the *medial* rule the following derivation can be constructed as required, since either $\mathcal{T}^0_0\{\ P_j \colon j \in J_0\ \} \not\equiv \text{I}$ or $\mathcal{T}^1_0\{\ P_j \colon j \in J_1\ \} \not\equiv \text{I}$ and also either $\mathcal{T}^0_1\{\ Q_k \colon k \in K_0\ \} \not\equiv \text{I}$ or $\mathcal{T}^1_1\{\ Q_k \colon k \in K_1\ \} \not\equiv \text{I}$.

$$\begin{aligned} &\mathcal{T}^0\{\ P_i \mathbin{;} Q_i \colon i \in I_0\ \} \mathbin{\&} \mathcal{T}^1\{\ P_i \mathbin{;} Q_i \colon i \in I_1\ \} \\ &\qquad\qquad \longrightarrow \bigl(\mathcal{T}^0_0\{\ P_j \colon j \in J_0\ \} \mathbin{;} \mathcal{T}^0_1\{\ Q_k \colon k \in K_0\ \}\bigr) \mathbin{\&} \\ &\qquad\qquad\ \bigl(\mathcal{T}^1_0\{\ P_j \colon j \in J_1\ \} \mathbin{;} \mathcal{T}^1_1\{\ Q_k \colon k \in K_1\ \}\bigr) \\ &\qquad\qquad \longrightarrow \bigl(\mathcal{T}^0_0\{\ P_j \colon j \in J_0\ \} \mathbin{\&} \mathcal{T}^1_0\{\ P_j \colon j \in J_1\ \}\bigr) \mathbin{;} \\ &\qquad\qquad\ \bigl(\mathcal{T}^0_1\{\ Q_k \colon k \in K_0\ \} \mathbin{\&} \mathcal{T}^1_1\{\ Q_k \colon k \in K_1\ \}\bigr) \end{aligned}$$

Notice that $\mathcal{T}^0_0\{\ \} \mathbin{\&} \mathcal{T}^1_0\{\ \}$ and $\mathcal{T}^0_1\{\ \} \mathbin{\&} \mathcal{T}^1_1\{\ \}$ are two killing contexts and $J_0 \cup J_1 \subseteq I_0 \cup I_1$ and $K_0 \cup K_1 \subseteq I_0 \cup I_1$ as required. $\square$

The size of a proof. As an induction measure in the splitting lemma, we will require a measure of the size of a proof. To define the size of a proof we require the following definition of the size of a proposition. The size of the proposition is defined using multisets of multisets of natural numbers with a particular ordering. Multiset orderings are an established technique for proving the termination of procedures [13].

The multiset of multisets employed here is more complex than the multiset ordering for LS [46] (a formulation of MALL in the calculus of structures), due to subtle interaction problems between the unit, *seq* and *with* operators. In particular, applying the structural rules $\text{I} \mathbin{;} P \equiv P \equiv P \mathbin{;} \text{I}$ and the medial gives rise to the following rewrite.

$$\mathcal{C}\{\ P \mathbin{\&} Q\ \} \equiv \mathcal{C}\{\ (P \mathbin{;} \text{I}) \mathbin{\&} (\text{I} \mathbin{;} Q)\ \} \rightarrow \mathcal{C}\{\ (P \mathbin{\&} \text{I}) \mathbin{;} (\text{I} \mathbin{\&} Q)\ \}$$

In the above derivation, the units cannot in general be removed from the proposition on the right hand side; hence extra care should be taken that these units do not increase the size of the proposition. This observation leads us to the notion of multisets of multisets of natural numbers defined below.

A multiset of natural numbers is a set of natural numbers where numbers may occur more than once. To define the multiset ordering, we require the standard multiset (disjoint) union operator $\cup$ and a multiset sum operator defined such that $M + N = \{m + n \colon m \in M \text{ and } n \in N\}$.

We also define the following two operators over multisets of multisets of natural numbers. If $\mathcal{M}$ and $\mathcal{N}$ are multisets of multisets, then we define pointwise plus and pointwise union as follows.

$$\begin{aligned} \mathcal{M} \boxplus \mathcal{N} &= \{M + N, M \in \mathcal{M} \text{ and } N \in \mathcal{N}\} \\ \mathcal{M} \sqcup \mathcal{N} &= \{M \cup N, M \in \mathcal{M} \text{ and } N \in \mathcal{N}\} \end{aligned}$$

The following function defines the multiset of multisets representing the size of a proposition.

$$|\text{I}| = \{\{0\}\} \qquad\qquad |a| = |\overline{a}| = \{\{1\}\}$$

$$|P \parallel Q| = |P| \boxplus |Q| \qquad\qquad |P \mathbin{\&} Q| = |P \oplus Q| = |P| \sqcup |Q|$$

$$|P \otimes Q| = |P \mathbin{;} Q| = \begin{cases} |P| & \text{if } Q \equiv \text{I} \\ |Q| & \text{if } P \equiv \text{I} \\ |P| \sqcup |Q| & \text{otherwise} \end{cases}$$

Over multisets of natural numbers, we define a multiset ordering $M \leq N$ defined if and only if there exists an injective multiset function $f \colon M \to N$ such that, for all $m \in M$, $m \leq f(m)$. Strict multiset ordering $M < N$ is defined such that $M \leq N$ but $M \neq N$.

We now define a different multiset order over multisets of multisets of natural numbers. Given two multisets of multisets $\mathcal{M}$ and $\mathcal{N}$, $\mathcal{M} \sqsubseteq \mathcal{N}$ holds if and only if $\mathcal{M}$ can be obtained from $\mathcal{N}$ by repeatedly removing a multiset N from $\mathcal{N}$ and replacing N with zero or more multisets M_i such that $M_i \leq M$. $\mathcal{M} \sqsubset \mathcal{N}$ is defined when $\mathcal{M} \sqsubseteq \mathcal{N}$ but $\mathcal{M} \neq \mathcal{N}$.

Most of the following properties, required in proofs, are standard for multisets. The properties concerning multisets of multisets of natural numbers are treated more carefully.

Lemma 5 *The following properties hold for multisets of natural numbers K, M and N and multisets of multisets of natural numbers $\mathcal{K}$, $\mathcal{M}$ and $\mathcal{N}$.*

$$M + N = N + M \qquad (K + M) + N = K + (M + N)$$

$$M \cup N = N \cup M \qquad (K \cup M) \cup N = K \cup (M \cup N)$$

$$K + (M \cup N) = (K + M) \cup (K + N)$$

$$M + \{0\} = M \qquad M < M \cup N \qquad M < M + \{1\} \qquad \{0\} \leq M$$

$$\textit{if } \{\{0\}\} \sqsubset \mathcal{M} \textit{ and } \{\{0\}\} \sqsubset \mathcal{N} \textit{ then } \mathcal{M} \cup \mathcal{N} \sqsubset \mathcal{M} \boxplus \mathcal{N}$$

$$\mathcal{K} \sqcup (\mathcal{M} \cup \mathcal{N}) = (\mathcal{K} \sqcup \mathcal{M}) \cup (\mathcal{K} \sqcup \mathcal{N})$$

$$\mathcal{K} \boxplus (\mathcal{M} \sqcup \mathcal{N}) = (\mathcal{K} \boxplus \mathcal{M}) \sqcup (\mathcal{K} \boxplus \mathcal{N})$$

$$\mathcal{K} \boxplus (\mathcal{M} \cup \mathcal{N}) = (\mathcal{K} \boxplus \mathcal{M}) \cup (\mathcal{K} \boxplus \mathcal{N})$$

Furthermore, $\leq$ and $\sqsubseteq$ are a precongruences.

Proof: Most properties are standard for multisets. We provide only proofs for the final four properties, which involve interactions between the two distinct multiset orderings.

Firstly, assume that $\{\{0\}\} \sqsubset \mathcal{M}$ and $\{\{0\}\} \sqsubset \mathcal{N}$. Hence either $\{\{1\}\} \sqsubseteq \mathcal{M}$ or $\{\{0, 0\}\} \sqsubseteq \mathcal{M}$ and also either $\{\{1\}\} \sqsubseteq \mathcal{N}$ or $\{\{0, 0\}\} \sqsubseteq \mathcal{N}$. For any

$M \in \mathcal{M}$ and $N \in \mathcal{N}$, we have that

$$M \in \mathcal{M} \cup \mathcal{N} \text{ and } N \in \mathcal{M} \cup \mathcal{N}$$

and also

$$M + N \in \mathcal{M} \boxplus \mathcal{N}$$

Now, there are four cases to consider. If $\{0,0\} \leq M$ then $N < N \cup N = \{0,0\} + N \leq M + N$; and similarly if $\{0,0\} \leq N$ then $M < M + N$. If $\{1\} \leq M$ then $N < \{1\} + N \leq M + N$; and similarly if $\{1\} \leq N$ then $M < M + N$. In all cases $M < M + N$ and $N < M + N$. Hence $\mathcal{M} \cup \mathcal{N} \sqsubset \mathcal{M} \boxplus \mathcal{N}$.

Secondly, consider every $M \in \mathcal{M}$, $N \in \mathcal{N}$, $K \in \mathcal{K}$, in which case the following hold.

$$M \cup K \in (\mathcal{M} \sqcup \mathcal{K}) \cup (\mathcal{N} \sqcup \mathcal{K}) \text{ and } N \cup K \in (\mathcal{M} \sqcup \mathcal{K}) \cup (\mathcal{N} \sqcup \mathcal{K})$$

and also

$$M \cup K \in (\mathcal{M} \cup \mathcal{N}) \sqcup \mathcal{K} \text{ and } N \cup K \in (\mathcal{M} \cup \mathcal{N}) \sqcup \mathcal{K}$$

Hence $(\mathcal{M} \sqcup \mathcal{K}) \cup (\mathcal{N} \sqcup \mathcal{K}) = (\mathcal{M} \cup \mathcal{N}) \sqcup \mathcal{K}$.

Thirdly, consider distributivity of $\boxplus$ over $\sqcup$. In this case the following resoning holds, as required.

$$\begin{aligned}
(\mathcal{M} \boxplus \mathcal{K}) \sqcup (\mathcal{N} \boxplus \mathcal{K}) = & \ \{(M + K) \cup (N + K) \colon M \in \mathcal{M}, N \in \mathcal{N}, K \in \mathcal{K}\} \\
= & \ \{(M \cup N) + K \colon M \in \mathcal{M}, N \in \mathcal{N}, K \in \mathcal{K}\} \\
= & \ (\mathcal{M} \sqcup \mathcal{N}) \boxplus \mathcal{K}
\end{aligned}$$

Fourthly, consider when $M \in \mathcal{M}$, $N \in \mathcal{N}$ and $K \in \mathcal{K}$. In this case the following holds

$$M + K \in \mathcal{K} \boxplus (\mathcal{M} \cup \mathcal{N}) \text{ and } N + K \in \mathcal{K} \boxplus (\mathcal{M} \cup \mathcal{N})$$

and also

$$M + K \in (\mathcal{K} \boxplus \mathcal{M}) \cup (\mathcal{K} \boxplus \mathcal{N}) \text{ and } N + K \in (\mathcal{K} \boxplus \mathcal{M}) \cup (\mathcal{K} \boxplus \mathcal{N})$$

Therefore $\mathcal{K} \boxplus (\mathcal{M} \cup \mathcal{N}) = (\mathcal{K} \boxplus \mathcal{M}) \cup (\mathcal{K} \boxplus \mathcal{N})$. □

The key property of multisets is the distributivity of $+$ over $\cup$, from which we can establish $|(P \,\&\, Q) \parallel R| = |(P \parallel R) \,\&\, (Q \parallel R)|$. Thus, although the abstract syntax tree grows when the *external* rule is applied, the multiset defined size of the proposition remains bounded by the size of the conclusion. The following four lemmas formalise the property of rewrite rules that rewriting reduces the size of the proposition, where Lemma 7 and Lemma 8 emphasise the strict multiset inequality in these cases.

Lemma 6 *If* $P \equiv Q$ *then* $|P| = |Q|$.

Proof: Consider the cases for the unit hold by the following reasoning, using Lemma 5.

$$|P \parallel \mathrm{I}| = |P| \boxplus \{\{0\}\} = |P|$$

$$|\mathrm{I}\ ;\ P| = |P\ ;\ \mathrm{I}| = |P \otimes \mathrm{I}| = |P|$$

For commutativity the following arguments hold for *par* and *times* respectively.

$$\begin{aligned} |P \parallel Q| = |P| \boxplus |Q| = &\ \{M + N \colon M \in |P|, N \in |Q|\} \\ = &\ \{N + M \colon M \in |P|, N \in |Q|\} = |Q| \boxplus |P| = |P \parallel Q| \end{aligned}$$

$$|P \otimes Q| = |P| \cup |Q| = |Q| \cup |P| = |Q \otimes P|$$

Associativity properties hold by extending associativity of multisets to multisets of multisets.

$$\begin{aligned} |(P \parallel Q) \parallel R| = &\ (|P| \boxplus |Q|) \boxplus |R| \\ = &\ \{(M + N) + K \colon M \in |P|, N \in |Q|, K \in |R|\} \\ = &\ \{M + (N + K) : M \in |P|, N \in |Q|, K \in |R|\} \\ = &\ |P| \boxplus (|Q| \boxplus |R|) = |P \parallel (Q \parallel R)| \end{aligned}$$

If any one of $P \equiv \mathrm{I}$, $Q \equiv \mathrm{I}$ or $R \equiv \mathrm{I}$ hold, then $|(P\ ;\ Q)\ ;\ R| = |P\ ;\ (Q\ ;\ R)|$ by definition. If $P \not\equiv \mathrm{I}$ and $Q \not\equiv \mathrm{I}$ and $R \not\equiv \mathrm{I}$, then the following equalities hold.

$$|(P\ ;\ Q)\ ;\ R| = (|P| \cup |Q|) \cup |R| = |P| \cup (|Q| \cup |R|) = |P\ ;\ (Q\ ;\ R)|$$

The same associativity argument works for the *times* operator. $\square$

Lemma 7 *Assuming that* $P \not\equiv \mathrm{I}$ *and* $R \not\equiv \mathrm{I}$*, the following strict multiset inequality holds.*

$$|\mathcal{C}\{\ P \otimes (Q \parallel R)\ \}| \sqsubset |\mathcal{C}\{\ (P \otimes Q) \parallel R\ \}|$$

Proof: If $Q \not\equiv \text{I}$, then, since $R \not\equiv \text{I}$ we have $\{\{0\}\} \sqsubset |R|$ and hence $|P| = |P| \boxplus \{\{0\}\} \sqsubset |P| \boxplus |R|$; and therefore the following holds by Lemma 5.

$$\begin{array}{rcl} |P \otimes (Q \parallel R)| = & & |P| \cup (|Q| \boxplus |R|) \\ & \sqsubset & (|P| \boxplus |R|) \cup (|Q| \boxplus |R|) \\ & = & (|P| \cup |Q|) \boxplus |R| = |(P \otimes Q) \parallel R| \end{array}$$

If $Q \equiv \text{I}$ then, since $\{\{0\}\} \sqsubset |P|$ and $\{\{0\}\} \sqsubset |R|$, the following holds by Lemma 5 and Lemma 6.

$$|P \otimes (\text{I} \parallel R)| = |P| \cup |R| \sqsubset |P| \boxplus |R| = |(P \otimes \text{I}) \parallel R|$$

□

Lemma 8 *Assuming that $Q \not\equiv \text{I}$ and $R \not\equiv \text{I}$ the following strict multiset inequality holds.*

$$|\mathcal{C}\{\ (P \parallel R) ; (Q \parallel S)\ \}| \sqsubset \mathcal{C}\{\ (P ; Q) \parallel (R ; S)\ \}$$

Proof: If $Q \not\equiv \text{I}$ and $R \not\equiv \text{I}$, then the following holds by Lemma 5.

$$\begin{array}{rcl} |(P \parallel R) ; (Q \parallel S)| = & & (|P| \boxplus |R|) \cup (|Q| \boxplus |S|) \\ & \sqsubset & (|P| \boxplus |R|) \cup (|Q| \boxplus |S|) \cup (|P| \boxplus |S|) \cup (|Q| \boxplus |R|) \\ & = & (|P| \cup |Q|) \boxplus (|R| \cup |S|) = |(P ; Q) \boxplus (R \parallel S)| \end{array}$$

If $Q \equiv \text{I}$ and $R \not\equiv \text{I}$, then, since $\{\{0\}\} \sqsubset |R|$, and hence $|S| = |S| \boxplus \{\{0\}\} \sqsubset |S| \boxplus |R|$, therefore by Lemma 5 and Lemma 6 the following strict inequality holds.

$$\begin{array}{rcl} |(P \parallel R) ; (\text{I} \parallel S)| = & & (|P| \boxplus |R|) \cup |S| \\ & \sqsubset & (|P| \boxplus |R|) \cup (|S| \boxplus |R|) \\ & \sqsubseteq & |P| \boxplus (|R| \cup |S|) = |(P ; \text{I}) \boxplus (R \parallel S)| \end{array}$$

A symmetric argument holds when $Q \not\equiv \text{I}$ and $R \equiv \text{I}$.

If $Q \equiv \text{I}$ and $R \equiv \text{I}$, then $\{\{0\}\} \sqsubset |P|$ and $\{\{0\}\} \sqsubset |S|$; hence the following strict inequality holds by Lemma 5 and Lemma 6.

$$|(P \parallel \text{I}) ; (\text{I} \parallel S)| = |P| \cup |S| \sqsubset |P| \boxplus |S| = |(P ; \text{I}) \parallel (\text{I} ; S)|$$

□

Lemma 9 *If $P \longrightarrow Q$, then $|Q| \sqsubseteq |P|$.*

Proof: The proof proceeds by induction on the number of rules in a derivation. The base case holds, by Lemma 6.

Consider the case for the *switch* rule, in a derivation of the following form, where $P \not\equiv \text{I}$ and $R \not\equiv \text{I}$.

$$S \longrightarrow \mathcal{C}\{\ (P \otimes Q) \parallel R\ \} \longrightarrow \mathcal{C}\{\ P \otimes (Q \parallel R)\ \}$$

By Lemma 7, $|\mathcal{C}\{\ P \otimes (Q \parallel R)\ \}| \sqsubset |\mathcal{C}\{\ (P \otimes Q) \parallel R\ \}|$ and, by induction, $|\mathcal{C}\{\ (P \otimes Q) \parallel R\ \}| \sqsubseteq |S|$; therefore $|\mathcal{C}\{\ P \otimes (Q \parallel R)\ \}| \sqsubset |S|$.

Consider the case for the *sequence* rule, for a derivation of the following form, where $P \not\equiv \text{I}$ and $Q \not\equiv \text{I}$.

$$T \longrightarrow \mathcal{C}\{\ (P\ ;\ Q) \parallel (R\ ;\ S)\ \} \longrightarrow \mathcal{C}\{\ (P \parallel R)\ ;\ (Q \parallel S)\ \}$$

By Lemma 8, $|\mathcal{C}\{\ (P \parallel R)\ ;\ (Q \parallel S)\ \}| \sqsubset |\mathcal{C}\{\ (P\ ;\ Q) \parallel (R\ ;\ S)\ \}|$ and, by induction, $|\mathcal{C}\{\ (P\ ;\ Q) \parallel (R\ ;\ S)\ \}| \sqsubseteq |S|$; therefore $|\mathcal{C}\{\ (P \parallel R)\ ;\ (Q \parallel S)\ \}| \sqsubset |S|$, as required.

Consider the case for the *medial* rule, for a derivation of the following form, where either $P \not\equiv \text{I}$ or $R \not\equiv \text{I}$ and also either $Q \not\equiv \text{I}$ or $S \not\equiv \text{I}$.

$$T \longrightarrow \mathcal{C}\{\ (P\ ;\ Q)\ \&\ (R\ ;\ S)\ \} \longrightarrow \mathcal{C}\{\ (P\ \&\ R)\ ;\ (Q\ \&\ S)\ \}$$

For when all of P, Q, R and S are not equivalent to the unit.

$$\begin{aligned} |(P\ \&\ R)\ ;\ (Q\ \&\ S)| &= (|P| \sqcup |R|) \cup (|Q| \sqcup |S|) \\ &\sqsubset (|P| \sqcup |R|) \cup (|Q| \sqcup |S|) \cup (|P| \sqcup |S|) \cup (|Q| \sqcup |R|) \\ &= (|P| \cup |Q|) \sqcup (|R| \cup |S|) = |(P\ ;\ Q)\ \&\ (R\ ;\ S)| \end{aligned}$$

For when exactly one of P, Q, R and S is equivalent to the unit, all cases are symmetric. Without loss of generality suppose that $S \equiv \text{I}$ (and possibly also $Q \equiv \text{I}$). By Lemma 5 and Lemma 6 the following holds.

$$\begin{aligned} |(P\ \&\ R)\ ;\ (Q\ \&\ \text{I})| &= (|P| \sqcup |R|) \cup (|Q| \sqcup \{\{0\}\}) \\ &\sqsubseteq (|P| \sqcup |R|) \cup (|Q| \sqcup |R|) \\ &= (|P| \cup |Q|) \sqcup |R| = |(P\ ;\ Q)\ \&\ (R\ ;\ \text{I})| \end{aligned}$$

There is one more form of case to consider for the medial: either $P \not\equiv \text{I}$, $Q \equiv \text{I}$, $R \equiv \text{I}$ and $S \not\equiv \text{I}$; or $P \equiv \text{I}$, $Q \not\equiv \text{I}$, $R \not\equiv \text{I}$ and $S \equiv \text{I}$. We consider only the former case. The later case, can be treated symmetrically. Since $P \not\equiv \text{I}$ and $S \not\equiv \text{I}$, $\{\{0\}\} \sqsubset |P|$ and $\{\{0\}\} \sqsubset |S|$. Therefore, $|P| \sqcup \{\{0\}\} \sqsubset$

$|P| \sqcup |S|$ and $|Q| \sqcup \{\{0\}\} \sqsubset |P| \sqcup |S|$. Hence, we have established that $(|P| \sqcup \{\{0\}\}) \cup (|Q| \sqcup \{\{0\}\}) \sqsubseteq |P| \sqcup |S|$.

Note that the restriction on the *medial* rule either $P \not\equiv \mathrm{I}$ or $R \not\equiv \mathrm{I}$ and also either $Q \not\equiv \mathrm{I}$ or $S \not\equiv \mathrm{I}$ excludes any further cases. Hence we have established that $\mathcal{C}\{\ (P \,\&\, R) \mathbin{;} (Q \,\&\, S)\ \} \sqsubseteq \mathcal{C}\{\ (P \mathbin{;} Q) \,\&\, (R \mathbin{;} S)\ \}$ and since, by induction $\mathcal{C}\{\ (P \mathbin{;} Q) \,\&\, (R \mathbin{;} S)\ \} \sqsubseteq |T|$ we have that $\mathcal{C}\{\ (P \,\&\, R) \mathbin{;} (Q \,\&\, S)\ \} \sqsubseteq |T|$ as required.

Consider the case for the *external* rule, in which case we have a derivation of the following form, where $R \not\equiv \mathrm{I}$.

$$S \longrightarrow \mathcal{C}\{\ (P \,\&\, Q) \parallel R\ \} \longrightarrow \mathcal{C}\{\ (P \parallel R) \,\&\, (Q \parallel R)\ \}$$

Now, by Lemma 5 we know that the following multiset equality holds.

$$\begin{aligned} |(P \,\&\, Q) \parallel R| = &\ (|P| \sqcup |Q|) \boxplus R \\ = &\ (|P| \boxplus R) \sqcup (|Q| \boxplus R) = |(P \parallel R) \,\&\, (Q \parallel R)| \end{aligned}$$

Hence, $|\mathcal{C}\{\ (P \parallel R) \,\&\, (Q \parallel R)\ \}| = |\mathcal{C}\{\ (P \,\&\, Q) \parallel R\ \}|$ and also, by induction, $|\mathcal{C}\{\ (P \,\&\, Q) \parallel R\ \}| \sqsubseteq |S|$, hence $|\mathcal{C}\{\ (P \parallel R) \,\&\, (Q \parallel R)\ \}| \sqsubseteq |S|$ as required.

The cases for the rules *tidy*, *left*, *right*, *atomic interact* are relatively straightforward to establish by using Lemma 5, since the following multiset inequalities hold.

$$|\mathrm{I}| \sqsubset |\mathrm{I} \,\&\, \mathrm{I}| \quad |\mathrm{I}| \sqsubset |\overline{a} \,\&\, a| \quad |P| \sqsubset |P \oplus Q| \quad |Q| \sqsubset |P \oplus Q|$$

Hence the lemma holds by induction on the length of the derivation. $\square$

We now define the *size of a proof* $\vdash P$ using a pair consisting of the size of the proposition, $|P|$, and the number of rules applied in the proof of the proposition. The pairs representing the size of a proof are ordered lexicographically.

Definition 3 *Consider a proof of proposition P that applies m rule instances. The size of this proof is given by the pair $(|P|, m)$. Suppose that the size of a proof of Q is $(|Q|, n)$ then we say that $(|P|, m) \prec (|Q|, n)$ if and only if $|P| \sqsubset |Q|$ or $|P| = |Q|$ and $m < n$.*

Termination Lemmas. The following notable lemma, will be used to deal with a troublesome case concerning the interaction between associativity of seq and partial distributivity of the additives. For now, consider Lemma 10 as a substantial example of applying the above lemmata for multisets.

Lemma 10 *Assume that $T_0 \not\equiv \mathrm{I}$, $T_2 \not\equiv \mathrm{I}$ and, either $U \not\equiv \mathrm{I}$ or $V \not\equiv \mathrm{I}$, and the following derivations hold.*

$$W \longrightarrow \mathcal{T}\{\ P_i \mathbin{;} Q_i \colon 1 \leq i \leq n\ \}$$

There are two symmetric cases to consider. For the first case, also assume that the following derivation holds for every i.

$$V \parallel Q_i \longrightarrow \mathcal{T}^i\left\{\ R^i_j \mathbin{;} S^i_j \colon 1 \leq j \leq m_i\ \right\}$$

In this case, the following two strict multiset inequalities hold.

$$\left|(T_0 \mathbin{;} T_1) \parallel \left((U \parallel P_i) \mathbin{;} \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right)\right| \sqsubset |(T_0 \mathbin{;} T_1 \mathbin{;} T_2) \parallel (U \mathbin{;} V) \parallel W|$$

$$\left|T_2 \parallel \mathcal{T}^i\left\{\ S^i_j \colon 1 \leq j \leq m_i\ \right\}\right| \sqsubset |(T_0 \mathbin{;} T_1 \mathbin{;} T_2) \parallel (U \mathbin{;} V) \parallel W|$$

For the second case, symmetric to the above. Instead assume that the following derivation holds for every i.

$$U \parallel P_i \longrightarrow \mathcal{T}^i\left\{\ R^i_j \mathbin{;} S^i_j \colon 1 \leq j \leq m_i\ \right\}$$

In this second case, the following two strict multiset inequalities hold.

$$\left|(T_1 \mathbin{;} T_2) \parallel \left(\mathcal{T}^i\left\{\ S^i_j \colon 1 \leq j \leq m_i\ \right\} \mathbin{;} (Q_i \parallel V)\right)\right| \sqsubset |(T_0 \mathbin{;} T_1 \mathbin{;} T_2) \parallel (U \mathbin{;} V) \parallel W|$$

$$\left|T_0 \parallel \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right| \sqsubset |(T_0 \mathbin{;} T_1 \mathbin{;} T_2) \parallel (U \mathbin{;} V) \parallel W|$$

Proof: Consider the case when $U \not\equiv \mathrm{I}$ and $V \not\equiv \mathrm{I}$. By definition, the size of the proposition on the left is as follows.

$$\mathcal{M} \triangleq |(T_0 \mathbin{;} T_1 \mathbin{;} T_2) \parallel (U \mathbin{;} V) \parallel W| = (|T_0 \mathbin{;} T_1| \cup |T_2|) \boxplus |U \mathbin{;} V| \boxplus |W|$$

Since $W \longrightarrow \mathcal{T}\{\ P_i \mathbin{;} Q_i \colon 1 \leq i \leq n\ \}$, by Lemma 9, the following inequality holds.

$$|P_i \mathbin{;} Q_i| \sqsubseteq \bigcup_{1 \leq i \leq n} |P_i \mathbin{;} Q_i| = |\mathcal{T}\{\ P_i \mathbin{;} Q_i \colon 1 \leq i \leq n\ \}| \sqsubseteq |W|$$

Hence, since $\sqsubseteq$ is a precongruence the following inequality holds.

$$(|T_0 \mathbin{;} T_1| \cup |T_2|) \boxplus |U \mathbin{;} V| \boxplus |P_i \mathbin{;} Q_i| \sqsubseteq \mathcal{M}$$

Now since $V \parallel Q_i \longrightarrow \mathcal{T}^i\Big\{\ R^i_j \,;\, S^i_j \colon 1 \leq j \leq m_i\ \Big\}$, by Lemma 9, the following inequality holds.

$$\left|\mathcal{T}^i\{\ R^i_j \,;\, S^i_j \colon 1 \leq j \leq m_i\ \}\right| \sqsubseteq |V \parallel Q_i|$$

Hence the following multiset inequalities hold.

$$\bigcup_{1\leq j\leq m_i} \left|R^i_j\right| \sqsubseteq |V| \boxplus |Q_i| \qquad \text{and} \qquad \bigcup_{1\leq j\leq m_i} \left|S^i_j\right| \sqsubseteq |V| \boxplus |Q_i|$$

We can therefore establishes the following strict multiset inequality, by Lemma 5.

$$\begin{array}{ll}
\multicolumn{2}{l}{\left|T_2 \parallel \mathcal{T}^i\Big\{\ S^i_j \colon 1 \leq j \leq m_i\ \Big\}\right|} \\
= & |T_2| \boxplus \left|\mathcal{T}^i\Big\{\ S^i_j \colon 1 \leq j \leq m_i\ \Big\}\right| \\
\sqsubseteq & |T_2| \boxplus |V| \boxplus |Q_i| \\
\sqsubset & (|T_0 \,;\, T_1| \cup |T_2|) \boxplus |U \,;\, V| \boxplus |P_i \,;\, Q_i| \sqsubseteq \mathcal{M}
\end{array}$$

For the other strict multiset inequality, observe that the following strict multiset inequality holds.

$$(|T_0 \,;\, T_1|) \boxplus |U \,;\, V| \boxplus |P_i \,;\, Q_i| \sqsubset \mathcal{M}$$

Hence it is sufficient to establish that the following multiset inequality holds.

$$\left|(T_0 \,;\, T_1) \parallel \big((U \parallel P_i) \,;\, \mathcal{T}^i\{\ R^i_j \colon 1 \leq j \leq m_i\ \}\big)\right| \sqsubseteq (|T_0 \,;\, T_1|) \boxplus |U \,;\, V| \boxplus |P_i \,;\, Q_i|$$

To establish this consider three cases:

- when $U \not\equiv \text{I}$ and $V \not\equiv \text{I}$;
- when $U \equiv \text{I}$ and $V \not\equiv \text{I}$;
- when $U \not\equiv \text{I}$ and $V \equiv \text{I}$.

At this point, consider when $U \not\equiv \text{I}$ and $V \not\equiv \text{I}$. By repeatedly applying distributivity of $\boxplus$ over $\cup$ and since $|P| \sqsubseteq |P \,;\, Q|$ and $|Q| \sqsubseteq |P \,;\, Q|$, by Lemma 5, the following holds.

$$\begin{array}{ll}
\multicolumn{2}{l}{|T_0 \,;\, T_1| \boxplus (|U| \cup |V|) \boxplus |P_i \,;\, Q_i|} \\
= & |T_0 \,;\, T_1| \boxplus ((|U| \boxplus |P_i \,;\, Q_i|) \cup (|V| \boxplus |P_i \,;\, Q_i|)) \\
\sqsupseteq & |T_0 \,;\, T_1| \boxplus ((|U| \boxplus |P_i|) \cup (|V| \boxplus |Q_i|))
\end{array}$$

Since $\sqsubseteq$ is a precongruence the following multiset inequality is established, as required.

$$\begin{array}{rl}\multicolumn{2}{l}{\left|(T_0 \mathbin{;} T_1) \parallel \left((U \parallel P_i) \mathbin{;} \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right)\right|} \\ = & |T_0 \mathbin{;} T_1| \boxplus \left((|U| \boxplus |P_i|) \cup \bigcup_{1 \leq j \leq m_i} \left|R^i_j\right|\right) \\ \sqsubseteq & |T_0 \mathbin{;} T_1| \boxplus ((|U| \boxplus |P_i|) \cup (|V| \boxplus |Q_i|))\end{array}$$

At this point, consider when $U \equiv \mathrm{I}$ and $V \not\equiv \mathrm{I}$, for which we must consider three sub-cases:

- when $P_i \not\equiv \mathrm{I}$ and $Q_i \not\equiv \mathrm{I}$;
- when $P_i \equiv \mathrm{I}$;
- when $P_i \not\equiv \mathrm{I}$ and $Q_i \equiv \mathrm{I}$.

If $P_i \not\equiv \mathrm{I}$ and $Q_i \not\equiv \mathrm{I}$ then by Lemma 5 the following multiset inequality holds, as required.

$$\begin{array}{rl}\multicolumn{2}{l}{|T_0 \mathbin{;} T_1| \boxplus |V| \boxplus (|P_i| \cup |Q_i|)} \\ = & |T_0 \mathbin{;} T_1| \boxplus ((|V| \boxplus |P_i|) \cup (|V| \boxplus |Q_i|)) \\ \sqsupseteq & |T_0 \mathbin{;} T_1| \boxplus (|P_i| \cup (|V| \boxplus |Q_i|)) \\ \sqsupseteq & |T_0 \mathbin{;} T_1| \boxplus \left(|P_i| \cup \left|\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right|\right) \\ = & \left|(T_0 \mathbin{;} T_1) \parallel \left(P_i \mathbin{;} \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right)\right|\end{array}$$

If $P_i \equiv \mathrm{I}$ then by Lemma 5 the following multiset inequality holds, as required.

$$\begin{array}{rl}\multicolumn{2}{l}{|T_0 \mathbin{;} T_1| \boxplus |V| \boxplus |Q_i|} \\ \sqsupseteq & |T_0 \mathbin{;} T_1| \boxplus \left|\mathcal{T}^i\left\{\ R^i_j \mathbin{;} S^i_j \colon 1 \leq j \leq m_i\ \right\}\right| \\ = & \left|(T_0 \mathbin{;} T_1) \parallel \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right|\end{array}$$

If $Q_i \equiv \mathrm{I}$ and $P_i \not\equiv \mathrm{I}$, hence $|P_i| \cup |V| \sqsubset |P_i| \boxplus |V|$ by Lemma 5, the following multiset inequality holds, as required.

$$\begin{array}{rl}\multicolumn{2}{l}{|T_0 \mathbin{;} T_1| \boxplus |P_i| \boxplus |V|} \\ \sqsupseteq & |T_0 \mathbin{;} T_1| \boxplus (|P_i| \cup |V|) \\ \sqsupseteq & |T_0 \mathbin{;} T_1| \boxplus \left(|P_i| \cup \left|\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right|\right) \\ = & \left|(T_0 \mathbin{;} T_1) \parallel \left(P_i \mathbin{;} \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right)\right|\end{array}$$

This completes all sub-cases for when $U \equiv \mathrm{I}$ and $V \not\equiv \mathrm{I}$.

In the third and final case consider when $U \not\equiv \mathrm{I}$ and $V \equiv \mathrm{I}$. In this case, there are three sub-cases to consider.

- when $P_i \not\equiv \mathrm{I}$ and $Q_i \not\equiv \mathrm{I}$;
- when $P_i \equiv \mathrm{I}$ and $\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\} \not\equiv \mathrm{I}$;
- when $\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\} \equiv \mathrm{I}$;

Consider the sub-case where $P_i \not\equiv \mathrm{I}$ and $Q_i \not\equiv \mathrm{I}$, in which case the following multiset inequality holds, as required.

$$\begin{aligned}
&\left|(T_0\ ;T_1) \parallel \left((U \parallel P_i)\ ; \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right)\right| \\
&\qquad = \quad |T_0\ ;T_1| \boxplus \left((|U| \boxplus |P_i|) \cup \left|\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right|\right) \\
&\qquad \sqsubseteq \quad |T_0\ ;T_1| \boxplus ((|U| \boxplus |P_i|) \cup |Q_i|) \\
&\qquad \sqsubseteq \quad |T_0\ ;T_1| \boxplus ((|U| \boxplus |P_i|) \cup (|U| \boxplus |Q_i|)) \\
&\qquad = \quad |T_0\ ;T_1| \boxplus |U| \boxplus (|P_i| \cup |Q_i|)
\end{aligned}$$

Consider the sub-case where $\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\} \not\equiv \mathrm{I}$ and $P_i \equiv \mathrm{I}$. Hence $|U| \cup \left|\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right| \sqsubseteq |U| \boxplus \left|\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right|$, by Lemma 5 since also $U \not\equiv \mathrm{I}$. Thereby the following multiset inequality holds, as required.

$$\begin{aligned}
&\left|(T_0\ ;T_1) \parallel \left(U\ ; \mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right)\right| \\
&\qquad = \quad |T_0\ ;T_1| \boxplus \left(|U| \cup \left|\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right|\right) \\
&\qquad \sqsubseteq \quad |T_0\ ;T_1| \boxplus \left(|U| \boxplus \left|\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\}\right|\right) \\
&\qquad \sqsubseteq \quad |T_0\ ;T_1| \boxplus (|U| \boxplus |Q_i|) \\
&\qquad = \quad |T_0\ ;T_1| \boxplus |U| \boxplus |Q_i|
\end{aligned}$$

Consider the sub-case where $\mathcal{T}^i\left\{\ R^i_j \colon 1 \leq j \leq m_i\ \right\} \equiv \mathrm{I}$, in which case the following multiset inequality holds since $|P_i| \sqsubseteq |P_i\ ;Q_i|$ by Lemma 5, as required.

$$\begin{aligned}
&|(T_0\ ;T_1) \parallel U \parallel P_i| \\
&\qquad = \quad |T_0\ ;T_1| \boxplus |U| \boxplus |P_i| \\
&\qquad \sqsubseteq \quad |T_0\ ;T_1| \boxplus |U| \boxplus |P_i\ ;Q_i|
\end{aligned}$$

This completes the sub-case analysis of the case when $U \not\equiv \mathrm{I}$ and $V \equiv \mathrm{I}$.

Thereby all cases have been considered for the first part of the lemma. The analysis of the second part of the lemma is symmetric to the first. $\square$

We will also require the following lemma for the most involved case concerning times in the proof of splitting.

Lemma 11 *For the following assume that $T \not\equiv \mathrm{I}$ and $U \not\equiv \mathrm{I}$ and also the following derivations hold.*

$$W \longrightarrow \mathcal{T}\{\ R_i \parallel S_i \colon 1 \leq i \leq n\ \}$$
$$R_i \longrightarrow \mathcal{T}_i^0\left\{\ P_j^{i,0} \parallel Q_j^{i,0} \colon 1 \leq j \leq m_i^0\ \right\}$$
$$V \parallel S_i \longrightarrow \mathcal{T}_i^1\left\{\ P_k^{i,1} \parallel Q_k^{i,1} \colon 1 \leq k \leq m_i^1\ \right\}$$

For any i, j and k, the following two strict multiset inequalities hold.

$$\left|T \parallel P_j^{i,0} \parallel P_k^{i,1}\right| \sqsubset |(T \otimes U) \parallel V \parallel W|$$

$$\left|U \parallel Q_j^{i,0} \parallel Q_k^{i,1}\right| \sqsubset |(T \otimes U) \parallel V \parallel W|$$

Proof: Since $T \not\equiv \mathrm{I}$ and $U \not\equiv \mathrm{I}$, by definition.

$$\mathcal{M} \triangleq |(T \otimes U) \parallel V \parallel W| = (|T| \cup |U|) \boxplus |V| \boxplus |W|$$

Since $W \longrightarrow \mathcal{T}\{\ R_i \parallel S_i \colon 1 \leq i \leq n\ \}$, by Lemma 9, and by Lemma 5 we have the following.

$$|R_i| \boxplus |S_i| \sqsubseteq |\mathcal{T}\{\ R_i \parallel S_i \colon 1 \leq i \leq n\ \}| \sqsubseteq |W|$$

Hence, since $\sqsubseteq$ is a precongruence we have.

$$(|T| \cup |U|) \boxplus |V| \boxplus |R_i| \boxplus |S_i| \sqsubseteq (|T| \cup |U|) \boxplus |V| \boxplus |W|$$

Now since $V \parallel S_i \longrightarrow \mathcal{T}_i^1\left\{\ P_k^{i,1} \parallel Q_k^{i,1} \colon 1 \leq k \leq m_i^1\ \right\}$, by Lemma 9 and Lemma 5 we have.

$$\left|P_k^{i,1}\right| \boxplus \left|Q_k^{i,1}\right| \sqsubseteq \left|\mathcal{T}_i^1\left\{\ P_k^{i,1} \parallel Q_k^{i,1} \colon 1 \leq k \leq m_i^1\ \right\}\right| \sqsubseteq |V \parallel S_i|$$

Similarly, since $R_i \longrightarrow \mathcal{T}_i^0\left\{\ P_j^{i,0} \parallel Q_j^{i,0} \colon 1 \leq j \leq m_i^0\ \right\}$, by Lemma 9 and Lemma 5 we have.

$$\left|P_j^{i,0}\right| \boxplus \left|Q_j^{i,0}\right| \sqsubseteq \left|\mathcal{T}_i^0\left\{\ P_j^{i,0} \parallel Q_j^{i,0} \colon 1 \leq j \leq m_i^0\ \right\}\right| \sqsubseteq |R_i|$$

Since $\sqsubseteq$ is a precongruence the following multiset inequality must hold.

$$(|T| \cup |U|) \boxplus \left|P_j^{i,0}\right| \boxplus \left|Q_j^{i,0}\right| \boxplus \left|P_k^{i,1}\right| \boxplus \left|Q_k^{i,1}\right| \sqsubseteq (|T| \cup |U|) \boxplus |V| \boxplus |R_i| \boxplus |S_i|$$

Hence we have the following two strict inequalities, since $M \sqsubset M \cup N$ by Lemma 5, as required.

$$|T| \boxplus \left|P_j^{i,0}\right| \boxplus \left|P_k^{i,1}\right| \sqsubset (|T| \cup |U|) \boxplus \left|P_j^{i,0}\right| \boxplus \left|Q_j^{i,0}\right| \boxplus \left|P_k^{i,1}\right| \boxplus \left|Q_k^{i,1}\right| \sqsubseteq \mathcal{M}$$

$$|U| \boxplus \left|Q_j^{i,0}\right| \boxplus \left|Q_k^{i,1}\right| \sqsubset (|T| \cup |U|) \boxplus \left|P_j^{i,0}\right| \boxplus \left|Q_j^{i,0}\right| \boxplus \left|P_k^{i,1}\right| \boxplus \left|Q_k^{i,1}\right| \sqsubseteq \mathcal{M}$$

□

The splitting technique. The splitting proof technique was established in the calculus of structures to prove cut elimination for the calculus BV [20], and has been extended to other systems [22, 40]. Splitting works strictly in a shallow context, which is a context like a sequent, where the object-level operator $\parallel$ and meta-level operator comma collapse to one operator.

Splitting says that you can pick any proposition in a shallow context, which we call the *principal proposition*, and rewrite the rest of the shallow context into a form consisting of several independent branches, tracked by a killing context, where in each branch a rule for the principal proposition can be applied, e.g. the *sequence* rule for seq, or the *left* and *right* rules for plus.

The splitting is divided into the remaining lemmas in this sub-section (Lemmas 12, 13 and 14). The multiplicative operators $\otimes$ and ; must be treated together since they involve a mutual recursion, Lemma 2 and the lemmas regarding multiset orders. The remaining splitting lemmas for plus (Lemma 13) and atoms (Lemma 14) can be treated independently, since they each rely only on Lemmas 2, 12 and simple properties of multisets. Notice that the splitting lemmas for plus and atoms are weaker than the splitting lemma for the multiplicatives, since the termination measure for the multiplicatives is used in the other two proofs, but not vice-versa.

The proof of each splitting lemma proceeds by induction on the size of a proof in MAV. In each splitting lemma, there are three forms of cases to consider. When the principal proposition is actively involved in the bottommost rule in the proof, we call it the *principal case*. When the principal proposition is inside the part of the proposition modified by the bottommost rule in a proof, but the root connective of the principal formula itself is not touched, we call it a *commutative case*. The final form of case is when a rule is applied entirely inside or independently of the principal formula, which we call a *deep inference case.*

Lemma 12 (Splitting multiplicatives) *The following statements hold.*

- *If* $\vdash (S \otimes T) \parallel U$*, then there exist propositions* V_i *and* W_i *such that* $\vdash S \parallel V_i$ *and* $\vdash T \parallel W_i$*, where* $1 \leq i \leq n$*, and* n*-ary killing context* $\mathcal{T}\{\ \}$ *such that* $U \longrightarrow \mathcal{T}\{\ V_1 \parallel W_1, \ldots, V_n \parallel W_n\ \}$*.*
- *If* $\vdash (S\ ; T) \parallel U$*, then there exist propositions* V_i *and* W_i *such that* $\vdash S \parallel V_i$ *and* $\vdash T \parallel W_i$*, where* $1 \leq i \leq n$*, and* n*-ary killing context* $\mathcal{T}\{\ \}$ *such that* $U \longrightarrow \mathcal{T}\{\ V_1 ; W_1, \ldots, V_n ; W_n\ \}$*.*

Furthermore the size of the proofs of $S \parallel V_i$ *and* $T \parallel W_i$ *are less than the size of the proofs of* $(S \otimes T) \parallel U$ *and* $(S\ ; T) \parallel U$*.*

Proof: The proof proceeds by induction on the size of proofs of the forms $(S\ ; T) \parallel U$ and $(S \otimes T) \parallel U$. The size of proofs is given by the lexicographical order of the size of the proposition and the number of rule instances, as in Defn. 3. The base case is when the length of such proofs are 0, hence $S \equiv \text{I}$, $T \equiv \text{I}$ and $U \equiv \text{I}$. In this case the following derivations of length zero, $\text{I} \equiv \text{I} \parallel \text{I}$ and $\text{I} \equiv \text{I}\ ; \text{I}$, satisfy the induction invariant.

Principal times case: Consider the principal case for times. The principal case, when times is actively involved in the bottommost rule, is a proof that begins as follows, where $T_0 \otimes U_0 \not\equiv \text{I}$ and also $V \not\equiv \text{I}$, otherwise the *switch* rule cannot be applied, and also $T_0 \otimes T_1 \not\equiv \text{I}$ and $U_0 \otimes U_1 \not\equiv \text{I}$ otherwise splitting follows by a trivial equivalence:

$$(T_0 \otimes T_1 \otimes U_0 \otimes U_1) \parallel V \parallel W \longrightarrow (T_0 \otimes U_0 \otimes ((T_1 \otimes U_1) \parallel V)) \parallel W$$

such that $\vdash (T_0 \otimes U_0 \otimes ((T_1 \otimes U_1) \parallel V)) \parallel W$. Furthermore, since $T_0 \otimes U_0 \not\equiv \text{I}$ and also $V \not\equiv \text{I}$, the following strict inequality holds by Lemma 7.

$$|(T_0 \otimes U_0 \otimes ((T_1 \otimes U_1) \parallel V)) \parallel W| \sqsubset |(T_0 \otimes T_1 \otimes U_0 \otimes U_1) \parallel V \parallel W|$$

Therefore the size of the proof is reduced and hence the hypothesis may be applied.

By the induction hypothesis, there exist R_i and S_i such that $\vdash (T_0 \otimes U_0) \parallel R_i$ and $\vdash (T_1 \otimes U_1) \parallel V \parallel S_i$, for $1 \leq i \leq n$, and an n-ary killing context $\mathcal{T}\{\ \}$ such that the following holds.

$$W \longrightarrow \mathcal{T}\{\ R_1 \parallel S_1, \ldots, R_n \parallel S_n\ \}$$

Furthermore $|(T_0 \otimes U_0) \parallel R_i|$ and $|(T_1 \otimes U_1) \parallel V \parallel S_i|$ are bounded above by $|(T_0 \otimes U_0 \otimes ((T_1 \otimes U_1) \parallel V)) \parallel W|$.

Hence, by the induction hypothesis twice more there exist propositions $P_j^{i,0}$, $Q_j^{i,0}$, $P_k^{i,1}$ and $Q_k^{i,1}$ such that $\vdash T_0 \parallel P_j^{i,0}$, $\vdash U_0 \parallel Q_j^{i,0}$, $\vdash T_1 \parallel P_k^{i,1}$ and $\vdash U_1 \parallel Q_k^{i,1}$, for $1 \leq j \leq m_i^0$ and $1 \leq k \leq m_i^1$, and m_i^0-ary killing context $\mathcal{T}_i^0\{\ \}$ and m_i^1-ary killing context $\mathcal{T}_i^1\{\ \}$ such that the following derivations hold.

$$\begin{aligned} R_i &\longrightarrow \mathcal{T}_i^0\left\{\ P_j^{i,0} \parallel Q_j^{i,0} \colon 1 \leq j \leq m_i^0\ \right\} \\ V \parallel S_i &\longrightarrow \mathcal{T}_i^1\left\{\ P_k^{i,1} \parallel Q_k^{i,1} \colon 1 \leq k \leq m_i^1\ \right\} \end{aligned}$$

Thereby the following derivation can be constructed, by Lemma 3.

$$\begin{aligned} V \parallel W &\longrightarrow V \parallel \mathcal{T}\{\ R_i \parallel S_i \colon 1 \leq i \leq n\ \} \\ &\longrightarrow \mathcal{T}\{\ R_i \parallel V \parallel S_i \colon 1 \leq i \leq n\ \} \\ &\longrightarrow \mathcal{T}\left\{ \begin{array}{c} \mathcal{T}_i^0\left\{\ P_j^{i,0} \parallel Q_j^{i,0} \colon 1 \leq j \leq m_i^0\ \right\} \\ \parallel\ \mathcal{T}_i^1\left\{\ P_k^{i,1} \parallel Q_k^{i,1} \colon 1 \leq k \leq m_i^1\ \right\} \end{array} \colon 1 \leq i \leq n \right\} \\ &\longrightarrow \mathcal{T}\left\{ \mathcal{T}_i^1\left\{ \begin{array}{l} \mathcal{T}_i^0\left\{\ P_j^{i,0} \parallel Q_j^{i,0} \colon 1 \leq j \leq m_i^0\ \right\} \\ \parallel P_k^{i,1} \parallel Q_k^{i,1} \colon 1 \leq k \leq m_i^1 \end{array} \right\} \colon 1 \leq i \leq n \right\} \\ &\longrightarrow \mathcal{T}\left\{ \mathcal{T}_i^1\left\{ \begin{array}{l} \mathcal{T}_i^0\left\{ \begin{array}{l} P_j^{i,0} \parallel P_k^{i,1} \parallel Q_j^{i,0} \parallel Q_k^{i,1} \\ \colon 1 \leq j \leq m_i^0 \end{array} \right\} \\ \colon 1 \leq k \leq m_i^1 \end{array} \right\} \colon 1 \leq i \leq n \right\} \end{aligned}$$

Now observe that the following proofs can be constructed.

$$(T_0 \otimes T_1) \parallel P_j^{i,0} \parallel P_k^{i,1} \longrightarrow \left(T_0 \parallel P_j^{i,0}\right) \otimes \left(T_1 \parallel P_k^{i,1}\right) \longrightarrow \mathrm{I}$$

$$(U_0 \otimes U_1) \parallel Q_j^{i,0} \parallel Q_k^{i,1} \longrightarrow \left(U_0 \parallel Q_j^{i,0}\right) \otimes \left(U_1 \parallel Q_k^{i,1}\right) \longrightarrow \mathrm{I}$$

Furthermore, since $T_0 \otimes T_1 \not\equiv \mathrm{I}$ and $U_0 \otimes U_1 \not\equiv \mathrm{I}$ by Lemma 11, we have the following strict multiset inequalities.

$$\left|(T_0 \otimes T_1) \parallel P_j^{i,0} \parallel P_k^{i,1}\right| \sqsubset |(T_0 \otimes T_1 \otimes U_0 \otimes U_1) \parallel V \parallel W|$$

$$\left|(U_0 \otimes U_1) \parallel Q_j^{i,0} \parallel Q_k^{i,1}\right| \sqsubset |(T_0 \otimes T_1 \otimes U_0 \otimes U_1) \parallel V \parallel W|$$

Thereby the size of either of the above two proofs is strictly less than the size of any proof of $(T_0 \otimes T_1 \otimes U_0 \otimes U_1) \parallel V \parallel W$, as required.

Principal seq case: Consider the principal case for sequential composition. The difficulty in this case is that, due to associativity of sequential composition, the *sequence* rule may be applied in several ways when there are multiple sequential compositions. Consider a principal proposition of the form $(T_0 ; T_1) ; T_2$, where we aim to split the formula around the second sequential composition. The difficulty is that the bottommost rule may be an instance of the *sequence* rule applied between T_0 and $T_1 ; T_2$. Symmetrically, the principal formula may be of the form $T_0 ; (T_1 ; T_2)$ but the bottommost rule may be an instance of the *sequence* rule applied between $T_0 ; T_1$ and T_2. In the following analysis, only the former case is considered. The symmetric case follows the same pattern.

Consider when the principal proposition is of the form $(T_0 ; T_1) ; T_2$ and the bottommost rule in a proof is of the following form, where $T_0 \not\equiv \text{I}$, $T_2 \not\equiv \text{I}$, otherwise splitting is trivial, and either $U \not\equiv \text{I}$ or $V \not\equiv \text{I}$ otherwise the *sequence* rule cannot be applied:

$$(T_0 ; T_1 ; T_2) \parallel (U ; V) \parallel W \longrightarrow ((T_0 \parallel U) ; ((T_1 ; T_2) \parallel V)) \parallel W$$

such that $((T_0 \parallel U) ; ((T_1 ; T_2) \parallel V)) \parallel W$ has a proof. By Lemma 8, $|((T_0 \parallel U) ; ((T_1 ; T_2) \parallel V)) \parallel W| \sqsubset (T_0 ; T_1 ; T_2) \parallel (U ; V) \parallel W$ hence the induction hypothesis may be applied.

By the induction hypothesis, there exist P_i and Q_i such that $\vdash T_0 \parallel U \parallel P_i$ and $\vdash (T_1 ; T_2) \parallel V \parallel Q_i$, for $1 \leq i \leq n$, and an n-ary killing context $\mathcal{T}\{\ \}$ such that the following holds.

$$W \longrightarrow \mathcal{T}\{\ P_1 ; Q_1, \ldots, P_n ; Q_n\ \}$$

where furthermore $|(T_1 ; T_2) \parallel V \parallel Q_i| \sqsubseteq |((T_0 \parallel U) ; ((T_1 ; T_2) \parallel V)) \parallel W|$, hence the induction hypothesis is enabled again.

By the induction hypothesis, there exists R^i_j and S^i_j such that $\vdash T_1 \parallel R^i_j$ and $\vdash T_2 \parallel S^i_j$, for $1 \leq j \leq m_i$, and m_i-ary killing context $\mathcal{T}^i\{\ \}$ such that the following derivation holds.

$$V \parallel Q_i \longrightarrow \mathcal{T}^i\{\ R^i_1 ; S^i_1, \ldots, R^i_{m_i} ; S^i_{m_i}\ \}$$

Furthermore, by Lemma 3 there exist killing context $\mathcal{T}^i_0\{\ \}$ and $\mathcal{T}^i_1\{\ \}$ and sets of integers $J \subseteq \{1, \ldots, n\}$, $K \subseteq \{1, \ldots, n\}$ such that.

$$\mathcal{T}^i\{\ R^i_1 ; S^i_1, \ldots, R^i_{m_i} ; S^i_{m_i}\ \} \longrightarrow \mathcal{T}^i_0\{\ R^i_j \colon j \in J\ \} ; \mathcal{T}^i_1\{\ S^i_k \colon k \in K\ \}$$

Thereby, the following derivation can be constructed.

$$
\begin{array}{ll}
(U\ ;V)\parallel W & \longrightarrow (U\ ;V)\parallel \mathcal{T}\{\ P_1\ ;Q_1,\ldots,P_n\ ;Q_n\ \} \\
& \longrightarrow \mathcal{T}\{\ (U\ ;V)\parallel (P_1\ ;Q_1)\,,\ldots,(U\ ;V)\parallel (P_n\ ;Q_n)\ \} \\
& \longrightarrow \mathcal{T}\{\ (U\parallel P_1)\ ;(V\parallel Q_1)\,,\ldots,(U\parallel P_n)\ ;(V\parallel Q_n)\ \} \\
& \longrightarrow \mathcal{T}\left\{\ (U\parallel P_1)\ ;\mathcal{T}^i\left\{\ R^i_j\ ;S^i_j\colon 1\leq j\leq m_i\ \right\}\colon 1\leq i\leq n\ \right\} \\
& \longrightarrow \mathcal{T}\left\{\begin{array}{r} (U\parallel P_1)\ ;\mathcal{T}^i_0\left\{\ R^i_j\colon j\in J\ \right\}\ ;\mathcal{T}^i_1\{\ S^i_k\colon k\in K\ \} \\ \colon 1\leq i\leq n \end{array}\right\}
\end{array}
$$

Furthermore, the following proofs can be constructed.

$$
\begin{array}{rl}
T_2\parallel \mathcal{T}^i\left\{\ S^i_j\colon 1\leq j\leq m_i\ \right\}\longrightarrow & \mathcal{T}^i\left\{\ T_2\parallel S^i_j\colon 1\leq j\leq m_i\ \right\} \\
\longrightarrow & \mathcal{T}^i\{\ \mathrm{I}\colon 1\leq j\leq m_i\ \}\longrightarrow \mathrm{I}
\end{array}
$$

$$
\begin{array}{ll}
\multicolumn{2}{l}{(T_0\ ;T_1)\parallel \left((U\parallel P_i)\ ;\mathcal{T}^i\left\{\ R^i_j\colon 1\leq j\leq m_i\ \right\}\right)} \\
\longrightarrow & (T_0\parallel U\parallel P_i)\ ;\left(T_1\parallel \mathcal{T}^i\left\{\ R^i_j\colon 1\leq j\leq m_i\ \right\}\right) \\
\longrightarrow & T_1\parallel \mathcal{T}^i\left\{\ R^i_j\colon 1\leq j\leq m_i\ \right\} \\
\longrightarrow & \mathcal{T}^i\left\{\ T_1\parallel R^i_j\colon 1\leq j\leq m_i\ \right\} \\
\longrightarrow & \mathcal{T}^i\{\ \mathrm{I}\colon 1\leq j\leq m_i\ \}\longrightarrow \mathrm{I}
\end{array}
$$

By Lemma 10, we know that the size of the above two proofs is strictly less than the size of any proof of $(T_0\ ;T_1\ ;T_2)\parallel (U\ ;V)\parallel W$.

Commutative cases: The commutative cases to consider are for &, $\otimes$ and ; where the principal proposition is involved in the bottommost rules, but the principal proposition is not modified. There are six cases to consider, three each for $\otimes$ and ; as the root connective of the principal proposition.

We present the commutative cases for & distributing over the principal proposition. Notice that killing contexts are necessary due to an application of the *external* rule in the context of another operator, thereby branching the proof search.

Consider the commutative case for & where $T\otimes U$ is the principal proposition. The bottommost rule is of the following form.

$$(T\otimes U)\parallel (V\ \&\ W)\parallel Q\longrightarrow ((T\otimes U)\parallel V\ \&\ (T\otimes U)\parallel W)\parallel Q$$

such that $\vdash ((T\otimes U)\parallel V\ \&\ (T\otimes U)\parallel W)\parallel Q$ holds.

By Lemma 2, $\vdash (T \otimes U) \parallel V \parallel Q$ and also $\vdash (T \otimes U) \parallel W \parallel Q$. Furthermore, by Lemma 5, $|(T \otimes U) \parallel V \parallel Q| \sqsubset |(T \otimes U) \parallel (V \mathbin{\&} W) \parallel Q|$ and $|(T \otimes U) \parallel W \parallel Q| \sqsubset |(T \otimes U) \parallel (V \mathbin{\&} W) \parallel Q|$, hence the induction hypothesis is enabled.

Therefore, by the induction hypothesis twice, there exist R_i^0 and S_i^0 such that $\vdash T \parallel R_i^0$ and $\vdash U \parallel S_i^0$, where $1 \leq i \leq m$, and R_j^1 and S_j^1 such that $\vdash T \parallel R_j^1$ and $\vdash U \parallel S_j^1$, where $1 \leq j \leq n$, and m-ary and n-ary killing contexts $\mathcal{T}^0\{\ \ \}$ and $\mathcal{T}^1\{\ \ \}$ respectively such that the following holds.

$$
\begin{array}{ll}
V \parallel Q & \longrightarrow \mathcal{T}^0\{\ R_1^0 \parallel S_1^0, R_2^0 \parallel S_2^0, \ldots, R_m^0 \parallel S_m^0\ \} \\
W \parallel Q & \longrightarrow \mathcal{T}^1\{\ R_1^1 \mathbin{;} S_1^1, R_2^1 \parallel S_2^1, \ldots, R_n^1 \parallel S_n^1\ \}
\end{array}
$$

Furthermore, $\left|T \parallel R_i^0\right| \sqsubseteq |(T \otimes U) \parallel V \parallel Q|$ and $\left|U \parallel S_i^0\right| \sqsubseteq |(T \otimes U) \parallel V \parallel Q|$ and $\left|T \parallel R_j^1\right| \sqsubseteq |(T \otimes U) \parallel W \parallel Q|$ and $\left|U \parallel S_j^1\right| \sqsubseteq |(T \otimes U) \parallel W \parallel Q|$.

Thereby the following derivation can be constructed, as required.

$$
\begin{array}{l}
(V \mathbin{\&} W) \parallel Q \\
\qquad\qquad \longrightarrow V \parallel Q \mathbin{\&} W \parallel Q \\
\qquad\qquad \longrightarrow \mathcal{T}^1\{\ V_1 \parallel R_1, \ldots, V_m \parallel R_m\ \} \mathbin{\&} \mathcal{T}^2\{\ W_1 \parallel S_1, \ldots, W_n \parallel S_n\ \}
\end{array}
$$

Notice that $\mathcal{T}^1\{\ \ \} \mathbin{\&} \mathcal{T}^2\{\ \ \}$ is an $(m+n)$-ary killing context satisfying the induction invariant.

Consider the commutative case for & where $T \mathbin{;} U$ is the principal proposition. The bottommost rule is of the following form.

$$
(T \mathbin{;} U) \parallel (V \mathbin{\&} W) \parallel Q \longrightarrow ((T \mathbin{;} U) \parallel V \mathbin{\&} (T \mathbin{;} U) \parallel W) \parallel Q
$$

such that $\vdash ((T \mathbin{;} U) \parallel V \mathbin{\&} (T \mathbin{;} U) \parallel W) \parallel Q$ holds.

By Lemma 2, $\vdash (T \mathbin{;} U) \parallel V \parallel Q$ and $\vdash (T \mathbin{;} U) \parallel W \parallel Q$. Furthermore, by Lemma 5 we have that $|(T \mathbin{;} U) \parallel V \parallel Q| \sqsubset |(T \mathbin{;} U) \parallel (V \mathbin{\&} W) \parallel Q|$ and $|(T \mathbin{;} U) \parallel W \parallel Q| \sqsubset |(T \mathbin{;} U) \parallel (V \mathbin{\&} W) \parallel Q|$, hence the induction hypothesis is enabled.

Therefore, by the induction hypothesis, there exist R_i^0 and S_i^0 such that $\vdash T \parallel R_i^0$ and $\vdash U \parallel S_i^0$, where $1 \leq i \leq m$, and R_j^1 and R_j^1 such that $\vdash T \parallel R_j^1$ and $\vdash U \parallel S_j^1$, where $1 \leq j \leq n$, and m-ary and n-ary killing contexts $\mathcal{T}^0\{\ \ \}$, $\mathcal{T}^1\{\ \ \}$ respectively such that the following derivation holds.

$$
\begin{array}{ll}
V \parallel Q & \longrightarrow \mathcal{T}^0\{\ R_1^0 \mathbin{;} S_1^0, R_2^0 \mathbin{;} S_2^0, \ldots, R_m^0 \mathbin{;} S_m^0\ \} \\
W \parallel Q & \longrightarrow \mathcal{T}^1\{\ R_1^1 \mathbin{;} S_1^1, R_2^1 \mathbin{;} S_2^1, \ldots, R_n^1 \mathbin{;} S_n^1\ \}
\end{array}
$$

Furthermore, $\left|T \parallel R_i^0\right| \sqsubseteq |(T\,;U) \parallel V \parallel Q|$, $\left|U \parallel S_i^0\right| \sqsubseteq |(T\,;U) \parallel V \parallel Q|$, $\left|T \parallel R_i^1\right| \sqsubseteq |(T\,;U) \parallel W \parallel Q|$, $\left|U \parallel S_i^1\right| \sqsubseteq |(T\,;U) \parallel W \parallel Q|$, hence strictly bounded above by $|(T\,;U) \parallel (V \mathbin{\&} W) \parallel Q|$.

Thereby the following derivation can be constructed.

$$\begin{aligned} &(V \mathbin{\&} W) \parallel Q \\ &\qquad\qquad \longrightarrow V \parallel Q \mathbin{\&} W \parallel Q \\ &\qquad\qquad \longrightarrow \mathcal{T}^0\{\ R_1^0\,;S_1^0, \ldots, R_m^0\,;S_m^0\ \} \mathbin{\&} \mathcal{T}^1\{\ R_1^1\,;S_1^1, \ldots, R_n^1\,;S_n^1\ \} \end{aligned}$$

Notice that $\mathcal{T}^1\{\quad\} \mathbin{\&} \mathcal{T}^2\{\quad\}$ is an $(m+n)$-ary killing context satisfying the induction invariant.

We present the cases where the *sequence* rule and *switch* rule commute with the principal proposition without direct involvement in the root connective of the principal proposition. The cases are presented where the principal proposition moves entirely to the left hand side of seq operator. The cases where the principal proposition moves entirely to the right hand side of the seq operator, and the cases for times, are similar to the cases presented below; as are the commutative cases for the *switch* rule. Simply exchange seq for times and par at appropriate points.

Consider the commutative case for sequential composition in the presence of principal proposition $T\,;U$, where the *seq* connective in the principal proposition is not active on the *sequence* rule. In this case, the bottommost rule in a proof is of the following form, where $T\,;U \not\equiv \mathrm{I}$ and $P \not\equiv \mathrm{I}$.

$$(T\,;U) \parallel (V\,;P) \parallel W \parallel Q \longrightarrow (((T\,;U) \parallel V \parallel W)\,;P) \parallel Q$$

such that $\vdash (((T\,;U) \parallel V \parallel W)\,;P) \parallel Q$ holds. Furthermore, by Lemma 8, $|(((T\,;U) \parallel V \parallel W)\,;P) \parallel Q| \sqsubset |(T\,;U) \parallel (V\,;P) \parallel W \parallel Q|$, hence the induction hypothesis is enabled.

By the induction hypothesis, there exists R_i, S_i such that $\vdash (T\,;U) \parallel V \parallel W \parallel R_i$ and $\vdash P \parallel S_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{T}\{\quad\}$ such that the following derivation holds.

$$Q \longrightarrow \mathcal{T}\{\ R_1\,;S_1, \ldots, R_n\,;S_n\ \}$$

Furthermore, $(T\,;U) \parallel V \parallel W \parallel R_i \sqsubseteq |(((T\,;U) \parallel V \parallel W)\,;P) \parallel Q|$ hence the induction hypothesis is enabled again.

By the induction hypothesis, for $1 \leq i \leq n$, there exist propositions P_j^i, Q_j^i such that $\vdash T \parallel P_j^i$ and $\vdash U \parallel Q_j^i$ hold, for $1 \leq j \leq m_i$, and killing contexts $\mathcal{T}^i\{\ \}$ such that the following derivation holds.

$$V \parallel W \parallel R_i \longrightarrow \mathcal{T}^i\{\ P^i_1 \,;\, Q^i_1, \ldots, P^i_{m_i} \,;\, Q^i_{m_i}\ \}$$

Furthermore the following strict multiset inequalities hold.

$$\left|T \parallel P^i_j\right| \sqsubset |(T \,;\, U) \parallel (V \,;\, P) \parallel W \parallel Q|$$

$$\left|U \parallel Q^i_j\right| \sqsubset |(T \,;\, U) \parallel (V \,;\, P) \parallel W \parallel Q|$$

Hence the following derivation can be constructed, as required.

$$\begin{array}{l}
(V \,;\, P) \parallel W \parallel Q \\
\qquad \longrightarrow (V \,;\, P) \parallel W \parallel \mathcal{T}\{\ R_1 \,;\, S_1, \ldots, R_n \,;\, S_n\ \} \\
\qquad \longrightarrow \mathcal{T}\{\ (V \,;\, P) \parallel W \parallel (R_1 \,;\, S_1), \ldots, (V \,;\, P) \parallel W \parallel (R_n \,;\, S_n)\ \} \\
\qquad \longrightarrow \mathcal{T}\{\ (V \parallel W \parallel R_1) \,;\, (P \parallel S_1), \ldots, (V \parallel W \parallel R_n) \,;\, (P \parallel S_n)\ \} \\
\qquad \longrightarrow \mathcal{T}\{\ V \parallel W \parallel R_1, \ldots, V \parallel W \parallel R_n\ \} \\
\qquad \longrightarrow \mathcal{T}\left\{\ \mathcal{T}^i\left\{\ P^i_j \,;\, Q^i_j \colon 1 \leq j \leq m_i\ \right\} \colon 1 \leq i \leq n\ \right\}
\end{array}$$

The case for the *sequence* rule commuting with the principal proposition $T \otimes U$ is similar to the above case. Also the cases for the *switch* rule commuting with seq and times as the principal proposition, follow a similar pattern.

Deep inference cases: The remaining cases are the deep inference cases, where the bottommost rule does not interfere with the root connective of the principal proposition. We provide one illustrative case where sequential composition is the principal proposition and the rule applies only outside that connective. Assume that the following application of any rule is the bottommost rule in a proof.

$$(T \,;\, U) \parallel \mathcal{C}\{\ V\ \} \longrightarrow (T \,;\, U) \parallel \mathcal{C}\{\ W\ \}$$

such that $\vdash (T \,;\, U) \parallel \mathcal{C}\{\ W\ \}$. By the induction hypothesis, there exist n-ary killing context $\mathcal{T}\{\ \}$ and propositions Q_i and R_i such that $\vdash T \parallel Q_i$ and $\vdash U \parallel R_i$, for $1 \leq i \leq n$, such that the following holds.

$$\mathcal{C}\{\ W\ \} \longrightarrow \mathcal{T}\{\ Q_1 \,;\, R_1, \ldots, Q_n \,;\, R_n\ \}$$

Hence, the following derivation holds, satisfying the induction invariant.

$$\begin{array}{rl}
\mathcal{C}\{\ V\ \} \longrightarrow & \mathcal{C}\{\ W\ \} \\
\longrightarrow & \mathcal{T}\{\ Q_1 \,;\, R_1, \ldots, Q_n \,;\, R_n\ \}
\end{array}$$

A similar proof holds for any principal proposition.

Alternatively, the bottommost rule may appear inside the context of principal proposition without affecting the root connective of the principal proposition. We provide one illustrative case where sequential composition is the principal proposition. Assume that the following application of any rule is the bottommost rule in a proof.

$$(\mathcal{C}\{\ T\ \}\ ;V) \parallel W \longrightarrow (\mathcal{C}\{\ U\ \}\ ;V) \parallel W$$

such that $\vdash (\mathcal{C}\{\ U\ \}\ ;V) \parallel W$ has a proof of length n. Hence by induction, there exist n-ary killing context $\mathcal{T}\{\ \ \}$ and propositions P_i and Q_i such that $\vdash \mathcal{C}\{\ U\ \} \parallel P_i$ and $\vdash V \parallel Q_i$ hold and have a proof no longer than n, for $1 \leq i \leq n$, and furthermore the following holds.

$$W \longrightarrow \mathcal{T}\{\ P_1\ ; Q_1, \ldots, P_n\ ; Q_n\ \}$$

Hence we can construct the following proof of length no longer than $n+1$, for all i, as required.

$$\mathcal{C}\{\ T\ \} \parallel P_i \longrightarrow \mathcal{C}\{\ U\ \} \parallel P_i \longrightarrow \mathrm{I}$$

A similar proof holds for any principal proposition.

Thereby, all cases for the splitting lemma for multiplicatives have been considered. □

Lemma 13 (Splitting plus) *If* $\vdash (T \oplus U) \parallel V$*, then there exist propositions* W_i *such that either* $\vdash T \parallel W_i$ *or* $\vdash U \parallel W_i$ *where* $1 \leq i \leq n$*, and* n*-ary killing context* $\mathcal{T}\{\ \ \}$ *such that* $V \longrightarrow \mathcal{T}\{\ W_1, W_2, \ldots, W_n\ \}$*.*

Proof: The proof is by induction on the size of the proof of the proposition to which splitting is applied, where the size of a proof is as in Defn. 3. Consider the base case for the plus operator. The cases for the *left* rule and *right* rule are symmetric. Without loss of generality, consider when the *left* rule is the bottommost rule in a proof as follows.

$$(T \oplus U) \parallel V \longrightarrow T \parallel V$$

such that $\vdash T \parallel V$, which immediately satisfies the conditions of the lemma.

The three commutative cases for &, ; and $\otimes$, are similar to the commutative cases in Lemma 12.

Consider the commutative case for & when $\oplus$ is the principal operator. In this case, the bottommost rule in a proof is of the following form.

$$(T \oplus U) \parallel (V \mathbin{\&} W) \parallel P \parallel Q \longrightarrow ((T \oplus U) \parallel V \parallel P \mathbin{\&} (T \oplus U) \parallel W \parallel P) \parallel Q$$

such that $\vdash ((T \oplus U) \parallel V \parallel P \mathbin{\&} (T \oplus U) \parallel W \parallel P) \parallel Q$.

By Lemma 2, $\vdash (T \oplus U) \parallel V \parallel P \parallel Q$ and $\vdash (T \oplus U) \parallel W \parallel P \parallel Q$ hold. Furthermore, the size of the above proofs are bound as follows, by Lemma 5.

$$|(T \oplus U) \parallel V \parallel P \parallel Q| \sqsubset |(T \oplus U) \parallel (V \mathbin{\&} W) \parallel P \parallel Q|$$

$$|(T \oplus U) \parallel W \parallel P \parallel Q| \sqsubset |(T \oplus U) \parallel (V \mathbin{\&} W) \parallel P \parallel Q|$$

Hence by induction there exists m-ary and n-ary killing contexts $\mathcal{T}^1\{\ \}$ and $\mathcal{T}^2\{\ \}$ respectively and propositions R_i and S_j, where $1 \leq i \leq m$ and $1 \leq j \leq n$, such that the following derivations hold:

$$\begin{array}{rl} V \parallel P \parallel Q \longrightarrow & \mathcal{T}^1\{\ R_1, \ldots, R_m\ \} \\ W \parallel P \parallel Q \longrightarrow & \mathcal{T}^2\{\ S_1, \ldots, S_n\ \} \end{array}$$

and either $\vdash T \parallel R_i$ or $\vdash U \parallel R_i$; and also either $\vdash T \parallel S_j$ or $\vdash U \parallel S_j$. Hence the following derivation can be constructed, as required.

$$\begin{array}{rl} (V \mathbin{\&} W) \parallel P \parallel Q \longrightarrow & V \parallel P \parallel Q \mathbin{\&} W \parallel P \parallel Q \\ \longrightarrow & \mathcal{T}^1\{\ R_1, \ldots, R_m\ \} \mathbin{\&} \mathcal{T}^2\{\ S_1, \ldots, S_n\ \} \end{array}$$

Notice that $\mathcal{T}^1\{\ \} \mathbin{\&} \mathcal{T}^2\{\ \}$ is an $(m+n)$-ary killing context satisfying the induction invariant.

Consider the commutative case for seq in the presence of principal proposition $T \oplus U$. There are two cases to consider, when the principal proposition ends up on the left or right of the seq operator. Consider the case where the operator ends up on the left of seq. In this case, the bottommost rule in a proof is of the following form, where $P \not\equiv \mathrm{I}$.

$$(T \oplus U) \parallel (V\ ;\ W) \parallel P \parallel Q \longrightarrow (((T \oplus U) \parallel V \parallel W)\ ;\ P) \parallel Q$$

such that $\vdash (((T \oplus U) \parallel V \parallel W)\ ;\ P) \parallel Q$ holds. Furthermore, by Lemma 8 $|(((T \oplus U) \parallel V \parallel W)\ ;\ P) \parallel Q| \sqsubset |(T \oplus U) \parallel (V\ ;\ W) \parallel P \parallel Q|$. By Lemma 12, there exist R_i and S_i such that $\vdash (T \oplus U) \parallel V \parallel W \parallel R_i$ and $\vdash P \parallel S_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{T}\{\ \}$ such that the following derivation holds.

$$Q \longrightarrow \mathcal{T}\{\ R_1\ ;\ S_1, \ldots, R_n\ ;\ S_n\ \}$$

Furthermore, also by Lemma 12, the following multiset inequality holds, enabling the induction hypothesis.

$$|(T \oplus U) \parallel V \parallel W \parallel R_i| \sqsubseteq |(((T \oplus U) \parallel V \parallel W) \mathbin{;} P) \parallel Q|$$

By the induction hypothesis, for $1 \leq i \leq n$, there exist propositions P^i_j such that either $\vdash T \parallel P^i_j$ or $\vdash U \parallel P^i_j$ holds, for $1 \leq j \leq m_i$, and killing contexts $\mathcal{T}^i\{\ \ \}$ such that the following derivation holds.

$$V \parallel W \parallel R_i \longrightarrow \mathcal{T}^i\{\ P^i_1, \ldots, P^i_{m_i}\ \}$$

Hence the following derivation can be constructed, as required.

$$\begin{array}{l}
(V \mathbin{;} W) \parallel P \parallel Q \\
\quad \longrightarrow (V \mathbin{;} W) \parallel P \parallel \mathcal{T}\{\ R_1 \mathbin{;} S_1, \ldots, R_n \mathbin{;} S_n\ \} \\
\quad \longrightarrow \mathcal{T}\{\ (V \mathbin{;} W) \parallel P \parallel R_1 \mathbin{;} S_1, \ldots, (V \mathbin{;} W) \parallel P \parallel R_n \mathbin{;} S_n\ \} \\
\quad \longrightarrow \mathcal{T}\{\ (V \parallel W \parallel R_1) \mathbin{;} (P \parallel S_1), \ldots, (V \parallel W \parallel R_n) \mathbin{;} (P \parallel S_n)\ \} \\
\quad \longrightarrow \mathcal{T}\{\ V \parallel W \parallel R_1, \ldots, V \parallel W \parallel R_n\ \} \\
\quad \longrightarrow \mathcal{T}\{\ \mathcal{T}^1\{\ P^1_1, \ldots, P^1_{m_1}\ \}, \ldots, \mathcal{T}^i\{\ P^n_1, \ldots, P^n_{m_n}\ \}\ \}
\end{array}$$

The other commutative cases for the *sequence* rule and *switch* rule are similar to the above case.

The remaining cases are deep inference cases, where the bottommost rule does not interfere with the root connective of the principal proposition. We provide one illustrative case where plus is the root connective of the principal proposition and the rule applies only outside that connective. Assume that the following is the bottommost rule in a proof of length $k + 1$.

$$(T \oplus U) \parallel \mathcal{C}\{\ V\ \} \longrightarrow (T \oplus U) \parallel \mathcal{C}\{\ W\ \}$$

such that $\vdash (T \mathbin{;} U) \parallel \mathcal{C}\{\ W\ \}$ has a proof of length k. By Lemma 9 $|(T \oplus U) \parallel \mathcal{C}\{\ W\ \}| \sqsubseteq |(T \oplus U) \parallel \mathcal{C}\{\ V\ \}|$, hence the induction hypothesis is enabled.

By the induction hypothesis, there exist n-ary killing context $\mathcal{T}\{\ \ \}$ and propositions P_i such that either $\vdash T \parallel P_i$ or $\vdash U \parallel P_i$, for $1 \leq i \leq n$, such that the following holds.

$$\mathcal{C}\{\ W\ \} \longrightarrow \mathcal{T}\{\ P_1, \ldots, P_n\ \}$$

Hence clearly, the following derivation holds, satisfying the induction invariant.

$$\begin{array}{rl}
\mathcal{C}\{\ V\ \} \longrightarrow & \mathcal{C}\{\ W\ \} \\
\longrightarrow & \mathcal{T}\{\ P_1, \ldots, P_n\ \}
\end{array}$$

Alternatively, the bottommost rule may appear inside the context of principal proposition without affecting the root connective of the principal proposition. We consider the case for when the rule is applied on the left of $\oplus$. Assume that the bottommost rule of a proof of length $k+1$ is of the following form.

$$(\mathcal{C}\{\ T\ \} \oplus V) \parallel W \longrightarrow (\mathcal{C}\{\ U\ \} \oplus V) \parallel W$$

such that $\vdash (\mathcal{C}\{\ U\ \} \oplus V) \parallel W$ has a proof with k rule instances. Furthermore, by Lemma 9, $|(\mathcal{C}\{\ U\ \} \oplus V) \parallel W| \sqsubseteq |(\mathcal{C}\{\ T\ \} \oplus V) \parallel W|$, hence the induction hypothesis is enabled.

Hence by induction, there exist n-ary killing context $\mathcal{T}\{\ \ \}$ and propositions P_i such that either $\vdash \mathcal{C}\{\ U\ \} \parallel P_i$ or $\vdash V \parallel P_i$, for $1 \leq i \leq n$, such that the following holds.

$$W \longrightarrow \mathcal{T}\{\ P_1, \ldots, P_n\ \}$$

Hence either $\vdash V \parallel P_i$ holds, or the following proof of $\mathcal{C}\{\ T\ \} \parallel P_i$ holds, for all i, as required.

$$\mathcal{C}\{\ T\ \} \parallel P_i \longrightarrow \mathcal{C}\{\ U\ \} \parallel P_i \longrightarrow \mathrm{I}$$

A symmetic proof holds for a rule applied in the right branch of $\oplus$.

All cases for the splitting lemma for plus have been considered, thereby the lemma follows by induction on the size of the proof. $\square$

Lemma 14 (Splitting atoms) *The following statements hold.*

- *For any atom a, if $\vdash \overline{a} \parallel T$, then there exist atoms b_1, b_2, $\ldots$, b_n such that $a \leq b_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{T}\{\ \ \}$ such that $T \longrightarrow \mathcal{T}\{\ b_1, b_2, \ldots, b_n\ \}$.*

- *For any atom a, if $\vdash a \parallel T$, then there exist atoms b_1, b_2, $\ldots$, b_n such that $b_i \leq a$, where $1 \leq i \leq n$, and n-ary killing context $\mathcal{T}\{\ \ \}$ such that $T \longrightarrow \mathcal{T}\{\ \overline{b_1}, \overline{b_2}, \ldots, \overline{b_n}\ \}$.*

Proof: Proceed by induction on the size of the proof, as defined in Defn. 3. Consider the base case for atoms. The case for positive and negative atoms are symmetric in the direction of subsorting. Consider the case for negative atoms and suppose that the bottommost rule in a proof is an atomic interaction as follows, where a and b are atoms such that $\vdash a \leq b$.

$$\overline{a} \parallel b \parallel U \longrightarrow U$$

where $\vdash U$. Hence, the derivation $b \parallel U \longrightarrow b$ can be constructed as required.

Consider the commutative case for & when an atom a is the principal proposition. In this case, the bottommost rule in a proof is of the following form.

$$a \parallel (T \mathbin{\&} U) \parallel V \parallel W \longrightarrow (a \parallel T \parallel V \mathbin{\&} a \parallel U \parallel V) \parallel W$$

such that $\vdash (a \parallel T \parallel V \mathbin{\&} a \parallel U \parallel V) \parallel W$ holds. By Lemma 2, $\vdash a \parallel T \parallel V \parallel W$ and $\vdash a \parallel U \parallel V \parallel W$ hold. Furthermore, the following strict multiset inequalities hold, by Lemma 5.

$$|a \parallel T \parallel V \parallel W| \sqsubset |a \parallel (T \mathbin{\&} U) \parallel V \parallel W|$$

$$|a \parallel U \parallel V \parallel W| \sqsubset |a \parallel (T \mathbin{\&} U) \parallel V \parallel W|$$

Hence, by induction, there exists m-ary and n-ary killing contexts $\mathcal{T}^1\{\ \}$ and $\mathcal{T}^2\{\ \}$ respectively and atoms b_i and c_j where $1 \leq i \leq m$ and $1 \leq j \leq n$ such that the following derivations hold:

$$\begin{array}{rl} V \parallel P \parallel Q \longrightarrow & \mathcal{T}^1\{\ \overline{b_1}, \ldots, \overline{b_m}\ \} \\ W \parallel P \parallel Q \longrightarrow & \mathcal{T}^2\{\ \overline{c_1}, \ldots, \overline{c_n}\ \} \end{array}$$

and furthermore $\vdash b_i \leq a$ and $\vdash c_i \leq a$ for all i. Hence the following derivation can be constructed.

$$\begin{array}{rl} (T \mathbin{\&} U) \parallel V \parallel W \longrightarrow & T \parallel V \parallel W \mathbin{\&} U \parallel V \parallel W \\ \longrightarrow & \mathcal{T}^1\{\ \overline{b_1}, \ldots, \overline{b_m}\ \} \mathbin{\&} \mathcal{T}^2\{\ \overline{c_1}, \ldots, \overline{c_n}\ \} \end{array}$$

Notice that $\mathcal{T}^1\{\ \} \mathbin{\&} \mathcal{T}^2\{\ \}$ is an $(m+n)$-ary killing context satisfying the induction invariant. The case for negative atoms is symmetric in the direction of the subsorting relation.

Consider the cases for the multiplicatives commuting with an atom. Firstly, consider the commutative case for seq in the presence of principal proposition a. In this case, the bottommost rule in a proof is of the following form, where $U \not\equiv \mathrm{I}$.

$$a \parallel (T \mathbin{;} U) \parallel V \parallel W \longrightarrow ((a \parallel T \parallel V) \mathbin{;} U) \parallel W$$

such that $\vdash ((a \parallel T \parallel V) \,;\, U) \parallel W$ holds. Furthermore, by Lemma 8, the following strict multiset inequality holds.

$$|((a \parallel T \parallel V) \,;\, U) \parallel W| \sqsubset |a \parallel (T \,;\, U) \parallel V \parallel W|$$

By Lemma 12, there exist P_i and Q_i such that $\vdash a \parallel V \parallel T \parallel P_i$ and $\vdash U \parallel Q_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{T}\{\ \}$ such that the following derivation holds.

$$W \longrightarrow \mathcal{T}\{\ P_1 \,;\, Q_1, \ldots, P_n \,;\, Q_n\ \}$$

Furthermore, $|a \parallel V \parallel T \parallel P_i| \sqsubseteq |((a \parallel T \parallel V) \,;\, U) \parallel W|$, enabling the induction hypothesis.

By the induction hypothesis, for $1 \leq i \leq n$, there exist atoms b^i_j such that $\vdash b^i_j \leq a$, for $1 \leq j \leq m_i$, and m_i-ary killing contexts $\mathcal{T}^i\{\ \}$ such that the following derivation holds.

$$V \parallel T \parallel P_i \longrightarrow \mathcal{T}^i\left\{\ \overline{b^i_1}, \overline{b^i_2}, \ldots, \overline{b^i_{m_i}}\ \right\}$$

Hence the following derivation can be constructed.

$$\begin{array}{ll} (T \,;\, U) \parallel V \parallel W & \\ \qquad \longrightarrow (T \,;\, U) \parallel V \parallel \mathcal{T}\{\ P_1 \,;\, Q_1, \ldots, P_n \,;\, Q_n\ \} \\ \qquad \longrightarrow \mathcal{T}\{\ (T \,;\, U) \parallel V \parallel (P_1 \,;\, Q_1), \ldots, (T \,;\, U) \parallel V \parallel (P_n \,;\, Q_n)\ \} \\ \qquad \longrightarrow \mathcal{T}\{\ (T \parallel V \parallel P_1) \,;\, (U \,;\, Q_1), \ldots, (T \parallel V \parallel P_n) \,;\, (U \,;\, Q_n)\ \} \\ \qquad \longrightarrow \mathcal{T}\{\ T \parallel V \parallel P_1, \ldots, T \parallel V \parallel P_n\ \} \\ \qquad \longrightarrow \mathcal{T}\left\{\ \mathcal{T}^1\left\{\ \overline{b^1_1}, \overline{b^1_2}, \ldots, \overline{b^1_{m_1}}\ \right\}, \ldots, \mathcal{T}^n\{\ \overline{b^n_1}, \overline{b^n_2}, \ldots, \overline{b^n_{m_n}}\ \}\ \right\} \end{array}$$

By construction, $\vdash b^i_j \leq a$ for all i and j and $\mathcal{T}\left\{\ \mathcal{T}^1\{\ \}, \ldots, \mathcal{T}^n\{\ \}\ \right\}$ is a $\sum_i m_i$-ary killing context, as required. The second commutative case for seq and the commutative case for times are similar, and the cases for negative atoms are symmetric.

The remaining deep inference cases are when a rule appears in the context of the proposition. Assume that the following is the bottommost rule in a proof that applies $k + 1$ instances of rules.

$$a \parallel \mathcal{C}\{\ V\ \} \longrightarrow a \parallel \mathcal{C}\{\ W\ \}$$

such that $\vdash a \parallel \mathcal{C}\{\ W\ \}$ holds by applying k instances of rules. By Lemma 9, $|a \parallel \mathcal{C}\{\ W\ \}| \sqsubseteq |a \parallel \mathcal{C}\{\ V\ \}|$, hence the induction hypothesis in enabled.

By the induction hypothesis, there exist atoms b_i such that $\vdash b_i \leq a$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{T}\{\ \}$ such that the following derivation holds.

$$\mathcal{C}\{\ W\ \} \longrightarrow \mathcal{T}\{\ \overline{b_1}, \overline{b_2}, \ldots, \overline{b_n}\ \}$$

Hence clearly, the following derivation holds, satisfying the induction invariant: $\mathcal{C}\{\ V\ \} \longrightarrow \mathcal{C}\{\ W\ \} \longrightarrow \mathcal{T}\{\ \overline{b_1}, \overline{b_2}, \ldots, \overline{b_n}\ \}$.

We have covered all cases for the splitting lemma for atoms, thereby the lemma follows by induction on the size of the proof. □

4.2 From a Shallow Context to a Deep Context

The context reduction lemma enables a implication that holds in a shallow context to be extended such that it holds in any context. Notice that the shallow context, consisting of only the par connective, is analogous to a sequent which is a context defined only by the meta-level connective comma. The proof of the context reduction lemma involves a stronger intermediate induction invariant from which the lemma follows directly.

Lemma 15 (Context reduction) *If* $\vdash T \parallel V$ *implies* $\vdash U \parallel V$*, for any* V*, then* $\vdash \mathcal{C}\{\ T\ \}$ *implies* $\vdash \mathcal{C}\{\ U\ \}$*, for any context* $\mathcal{C}\{\ \}$*.*

Proof: Firstly we establish, by induction on the size of the context, the following stronger property. If $\vdash \mathcal{C}\{\ T\ \}$, then there exist U_i for $1 \leq i \leq n$ and n-ary killing context $\mathcal{T}\{\ \}$ such that $\vdash T \parallel U_i$; and, for any proposition V there exists W_i such that either $W_i = V \parallel U_i$ or $W_i = \text{I}$ and the following holds:

$$\mathcal{C}\{\ V\ \} \longrightarrow \mathcal{T}\{\ W_1, W_2, \ldots, W_n\ \}$$

The base case is when the context is of the from $\{\ \} \parallel P$, where the hole appears directly inside a parallel composition, in which case we are done.

Consider the case for a context of the form $(\mathcal{C}\{\ \} \otimes U) \parallel P$ such that $\vdash (\mathcal{C}\{\ T\ \} \otimes U) \parallel P$. By Lemma 12, there exist n-ary killing context $\mathcal{T}\{\ \}$ and propositions Q_i and R_i, for $1 \leq i \leq n$, such that

$$P \longrightarrow \mathcal{T}\{\ Q_1 \parallel R_1, \ldots, Q_n \parallel R_n\ \}$$

and $\vdash \mathcal{C}\{\ T\ \} \parallel Q_i$ and $\vdash U \parallel R_i$ hold.

By the induction hypothesis, for every i such that $1 \leq i \leq n$, there exist m_i-ary killing context $\mathcal{T}^i\{\ \ \}$ and propositions W^i_j such that $\vdash T \parallel W^i_j$ holds, for $1 \leq j \leq m_i$; and, for any proposition V, for $1 \leq j \leq m_i$, there exists S^i_j such that either $S^i_j = \text{I}$ or $S^i_j = V \parallel W^i_j$ and the following derivation holds:

$$\mathcal{C}\{\ V\ \} \parallel Q_i \longrightarrow \mathcal{T}^i\left\{\ S^i_1, \ldots, S^i_{m_i}\ \right\}$$

Hence we can construct the following derivation for any proposition V.

$$\begin{array}{rl} (\mathcal{C}\{\ V\ \} \otimes U) \parallel P \longrightarrow & (\mathcal{C}\{\ V\ \} \otimes U) \parallel \mathcal{T}\{\ Q_1 \parallel R_1, \ldots, Q_n \parallel R_n\ \} \\ \longrightarrow & \mathcal{T}\{\ (\mathcal{C}\{\ V\ \} \otimes U) \parallel Q_i \parallel R_i \colon 1 \leq i \leq n\ \} \\ \longrightarrow & \mathcal{T}\{\ (\mathcal{C}\{\ V\ \} \parallel Q_i) \otimes (U \parallel R_i) : 1 \leq i \leq n\ \} \\ \longrightarrow & \mathcal{T}\{\ \mathcal{C}\{\ V\ \} \parallel Q_i \colon 1 \leq i \leq n\ \} \\ \longrightarrow & \mathcal{T}\left\{\ \mathcal{T}^i\left\{\ S^i_1, \ldots, S^i_{m_i}\ \right\} : 1 \leq i \leq n\ \right\} \end{array}$$

The final proposition above consists of a $(\sum_i m_i)$-ary killing context and propositions S^i_j such that either $S^i_j = \text{I}$ or $S^i_j = V \parallel W^i_j$ for all i, j. Thereby, the induction invariant is satisfied. The two cases for when the hole appears on the left or right of a sequential composition are similar to the above case for times.

Consider the case for a context of the form $(\mathcal{C}\{\ \ \} \mathbin{\&} U) \parallel P$ such that $\vdash (\mathcal{C}\{\ T\ \} \mathbin{\&} U) \parallel P$. By Lemma 2, $\vdash \mathcal{C}\{\ T\ \} \parallel P$ and $\vdash U \parallel P$ hold.

Hence, by the induction hypothesis, there exist killing context $\mathcal{T}\{\ \ \}$ and propositions V_i for $1 \leq i \leq n$ such that $\vdash T \parallel V_i$; and, for all propositions W, for $1 \leq i \leq n$, there exists S_i such that either $S_i = \text{I}$ or $S_i = W \parallel V_i$ and the following derivation holds:

$$\mathcal{C}\{\ W\ \} \parallel P \longrightarrow \mathcal{T}\{\ S_1, \ldots, S_n\ \}$$

Hence we can construct a derivation as follows for all propositions W.

$$\begin{array}{rl} (\mathcal{C}\{\ W\ \} \mathbin{\&} U) \parallel P \longrightarrow & \mathcal{C}\{\ W\ \} \parallel P \mathbin{\&} U \parallel P \\ \longrightarrow & \mathcal{C}\{\ W\ \} \parallel P \mathbin{\&} \text{I} \\ \longrightarrow & \mathcal{T}\{\ S_1, \ldots, S_n\ \} \mathbin{\&} \text{I} \end{array}$$

where $\mathcal{T}\{\ \ \} \mathbin{\&} \{\ \cdot\ \}$ is a $(n+1)$-ary killing context and $S_{n+1} = \text{I}$, thereby satisfying the induction invariant. The case when the hole appears on the right of an external choice is similar.

Consider the case for a context of the form $(\mathcal{C}\{\ \ \} \oplus U) \parallel P$ where $\vdash (\mathcal{C}\{\ T\ \} \oplus U) \parallel P$. By Lemma 13, there exist killing context $\mathcal{T}\{\ \ \}$ and V_i

for $1 \leq i \leq n$ such that either $\vdash \mathcal{C}\{\ T\ \} \parallel V_i$ or $\vdash U \parallel V_i$ and the following derivation holds:

$$P \longrightarrow \mathcal{T}\{\ V_1, \ldots, V_n\ \}$$

Now, by the induction hypothesis, if $\vdash \mathcal{C}\{\ T\ \} \parallel V_i$ holds, then there exist $\mathcal{T}^i\{\ \ \}$ and propositions W^i_j for $1 \leq j \leq m_i$ such that $\vdash T \parallel W^i_j$; and, for any proposition Q for $1 \leq j \leq m_i$, there exists S^i_j where wither $S^i_j = \text{I}$ or $S^i_j = Q \parallel W^i_j$ and the following derivation holds:

$$\mathcal{C}\{\ Q\ \} \parallel V_i \longrightarrow \mathcal{T}^i\{\ S^i_1, \ldots, S^i_{m_i}\ \}$$

Hence we can construct the following derivation for any proposition Q.

$$\begin{array}{rll} (\mathcal{C}\{\ Q\ \} \oplus U) \parallel P & \longrightarrow & (\mathcal{C}\{\ Q\ \} \oplus U) \parallel \mathcal{T}\{\ V_1, \ldots, V_n\ \} \\ & \longrightarrow & \mathcal{T}\{\ (\mathcal{C}\{\ Q\ \} \oplus U) \parallel V_1, \ldots, (\mathcal{C}\{\ Q\ \} \oplus U) \parallel V_n\ \} \\ & \longrightarrow & \mathcal{T}\{\ R_1, \ldots, R_n\ \} \end{array}$$

where R_i is defined as follows.

$$R_i = \begin{cases} \text{I} & \text{if } \vdash U \parallel V_i \\ \mathcal{T}^i\{\ S^i_1, \ldots, S^i_{m_i}\ \} & \text{otherwise} \end{cases}$$

The above is well-defined since if $\vdash U \parallel V_i$ holds, then

$$(\mathcal{C}\{\ Q\ \} \oplus U) \parallel V_i \longrightarrow U \parallel V_i \longrightarrow \text{I} = R_i$$

and, if $\vdash U \parallel V_i$ does not hold, then $\vdash \mathcal{C}\{\ T\ \} \parallel V_i$ must hold; hence the following derivation can be applied:

$$(\mathcal{C}\{\ Q\ \} \oplus U) \parallel V_i \longrightarrow \ \mathcal{C}\{\ Q\ \} \parallel V_i \longrightarrow \mathcal{T}^i\{\ S^i_1, \ldots, S^i_{m_i}\ \} = R_i$$

Hence the induction invariant is satisfied.

Having established the stronger intermediate lemma, assume that for any local proposition U, $\vdash S \parallel U$ implies $\vdash T \parallel U$, and fix any context $\mathcal{C}\{\ \ \}$ such that $\vdash \mathcal{C}\{\ S\ \}$ holds. By the above intermediate lemma, there exist n-ary killing context $\mathcal{T}\{\ \ \}$ and, for $1 \leq i \leq n$, P_i such that either $P_i = \text{I}$ or there exists W_i where $P_i = T \parallel W_i$ and $\vdash S \parallel W_i$, and furthermore $\mathcal{C}\{\ T\ \} \longrightarrow \mathcal{T}\{\ P_1, \ldots, P_n\ \}$. Since also $\vdash T \parallel W_i$ holds for $1 \leq i \leq n$, the following proof can be constructed.

$$\mathcal{C}\{\ T\ \} \longrightarrow \ \mathcal{T}\{\ P_1, \ldots, P_n\ \} \longrightarrow \mathcal{T}\{\ \text{I}, \ldots, \text{I}\ \} \longrightarrow \text{I}$$

Therefore $\vdash \mathcal{C}\{\ T\ \}$ holds as required. □

Note that the above lemma corrects a flaw present in the corresponding lemma in [9]:Lemma 14. In particular, the possibility that $W_i = \text{I}$ in the induction invarient is required to handle the additives, even if the operator *seq* is removed.

4.3 Co-rule Elmination and Cut Elimination

By a complementary rule, or *co-rule*, we mean a rule where the direction of rewriting is reversed and complementation is applied to both propositions in the rewrite rule. Given a rule of the form $P \longrightarrow Q$, its co-rule is of the form $\overline{Q} \longrightarrow \overline{P}$. The full list of co-rules are presented in Fig. 3. Note that *switch* is its own co-rule.

The following results show that the rules complimentary to those that appear in Fig. 2 are admissible in MAV. The proofs of the following lemmata follow from applying splitting exhaustively and finally applying the context lemma (Lemma 15). Note that admissibility results for two rules — the co-rules for the *left* and *right* rules, *co-left* and *co-right* respectively — were proven directly in Lemma 2.

Lemma 16 (Co-tidy Elimination) *If* $\vdash \mathcal{C}\{\ \mathrm{I} \oplus \mathrm{I}\ \}$, *then* $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$.

Proof: Assume that $\vdash (\mathrm{I} \oplus \mathrm{I}) \parallel T$ holds. By Lemma 13, there exist killing context $\mathcal{T}\{\ \ \}$ and propositions U_i, for $1 \leq i \leq n$, such that $\vdash \mathrm{I} \parallel U_i$ or $\vdash \mathrm{I} \parallel U_i$ hold, hence $\vdash U_i$ holds, and the following derivation can be constructed.

$$T \longrightarrow \mathcal{T}\{\ U_1, U_2, \ldots, U_n\ \}$$

Hence the following proof can be constructed, as required.

$$T \longrightarrow \mathcal{T}\{\ U_1, U_2, \ldots, U_n\ \} \longrightarrow \mathcal{T}\{\ \mathrm{I}, \mathrm{I}, \ldots, \mathrm{I}\ \} \longrightarrow \mathrm{I}$$

Hence $\vdash \mathrm{I} \parallel T$ holds. Therefore, by Lemma 15, for any context $\vdash \mathcal{C}\{\ \mathrm{I} \oplus \mathrm{I}\ \}$ yields $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$, as required. □

Lemma 17 (Co-external Elimination)
If $\vdash \mathcal{C}\{\ T \otimes (U \oplus V)\ \}$, *then* $\vdash \mathcal{C}\{\ (T \otimes U) \oplus (T \otimes V)\ \}$.

Proof: Assume that $\vdash ((T \oplus U) \otimes V) \parallel W$ holds. By Lemma 12, there exist killing context $\mathcal{T}\{\ \ \}$ and propositions P_i and Q_i, for $1 \leq i \leq n$, such that $\vdash (T \oplus U) \parallel P_i$ and $\vdash V \parallel Q_i$ and the following derivation holds:

$$W \longrightarrow \mathcal{T}\{\ P_1 \parallel Q_1, \ldots, P_n \parallel Q_n\ \}$$

Now, by Lemma 13, for every i, there exists killing context $\mathcal{T}^i\{\ \ \}$ and propositions R^i_j, for $1 \leq j \leq m_i$, such that either $\vdash T \parallel R^i_j$ or $\vdash U \parallel R^i_j$ holds and the following derivation holds:

$$P_i \longrightarrow \mathcal{T}^i\{\ R^i_1, R^i_2, \ldots, R^i_{m_i}\ \}$$

$$\mathrm{I} \mathbin{\&} \mathrm{I} \longrightarrow \mathrm{I} \quad \textit{tidy} \qquad \overline{a} \parallel b \longrightarrow \mathrm{I} \text{ only if } a \leq b \quad \textit{atomic interaction}$$

$$(T \otimes U) \parallel V \longrightarrow T \otimes (U \parallel V) \quad \textit{switch}$$

$$(T \mathbin{;} U) \parallel (V \mathbin{;} W) \longrightarrow (T \parallel V) \mathbin{;} (U \parallel W) \quad \textit{sequence}$$

$$T \oplus U \longrightarrow T \quad \textit{left} \qquad T \oplus U \longrightarrow U \quad \textit{right}$$

$$T \parallel (U \mathbin{\&} V) \longrightarrow (T \parallel U) \mathbin{\&} (T \parallel V) \quad \textit{external}$$

$$(T \mathbin{;} U) \mathbin{\&} (V \mathbin{;} W) \longrightarrow (T \mathbin{\&} V) \mathbin{;} (U \mathbin{\&} W) \quad \textit{medial}$$

$$\mathrm{I} \longrightarrow \mathrm{I} \oplus \mathrm{I} \quad \textit{co-tidy} \qquad \mathrm{I} \longrightarrow a \otimes \overline{b} \text{ only if } a \leq b \quad \textit{atomic co-interaction}$$

$$(T \otimes V) \mathbin{;} (U \otimes W) \longrightarrow (T \mathbin{;} U) \otimes (V \mathbin{;} W) \quad \textit{co-sequence}$$

$$T \longrightarrow T \mathbin{\&} U \quad \textit{co-left} \qquad U \longrightarrow T \mathbin{\&} U \quad \textit{co-right}$$

$$(T \otimes U) \oplus (T \otimes V) \longrightarrow T \otimes (U \oplus V) \quad \textit{co-external}$$

$$(T \oplus V) \mathbin{;} (U \oplus W) \longrightarrow (T \mathbin{;} U) \oplus (V \mathbin{;} W) \quad \textit{co-medial}$$

Figure 3: Term rewriting system modulo an equational theory for SMAV.

Notice that if $\vdash T \parallel R^i_j$ holds then the following derivation can be constructed.

$$\begin{array}{rl}(T \otimes V \oplus U \otimes V) \parallel R^i_j \parallel Q_i \longrightarrow & (T \otimes V) \parallel R^i_j \parallel Q_i \\ \longrightarrow & \left(T \parallel R^i_j\right) \otimes (V \parallel Q_i) \\ \longrightarrow & \mathrm{I}\end{array}$$

Otherwise $\vdash U \parallel R^i_j$ holds, hence the following derivation can be constructed.

$$\begin{array}{rl}(T \otimes V \oplus U \otimes V) \parallel R^i_j \parallel Q_i \longrightarrow & (U \otimes V) \parallel R^i_j \parallel Q_i \\ \longrightarrow & \left(U \parallel R^i_j\right) \otimes (V \parallel Q_i) \\ \longrightarrow & \mathrm{I}\end{array}$$

Hence we can construct the following proof, as required.

$$\begin{array}{l}(T \otimes V \oplus U \otimes V) \parallel W \\ \quad\longrightarrow (T \otimes V \oplus U \otimes V) \parallel \mathcal{T}\{\ P_1 \parallel Q_1, \ldots, P_n \parallel Q_n\ \} \\ \quad\longrightarrow (T \otimes V \oplus U \otimes V) \parallel \mathcal{T}\{\ \mathcal{T}^i\{\ R^i_1, R^i_2, \ldots, R^i_{m_i}\ \} \parallel Q_i \colon 1 \leq i \leq n\ \} \\ \quad\longrightarrow (T \otimes V \oplus U \otimes V) \parallel \mathcal{T}\left\{\ \mathcal{T}^i\left\{\ R^i_j \parallel Q_i \colon 1 \leq j \leq m_i\ \right\} \colon 1 \leq i \leq n\ \right\} \\ \quad\longrightarrow \mathcal{T}\left\{\ (T \otimes V \oplus U \otimes V) \parallel \mathcal{T}^i\left\{\ R^i_j \parallel Q_i \colon 1 \leq j \leq m_i\ \right\} \colon 1 \leq i \leq n\ \right\} \\ \quad\longrightarrow \mathcal{T}\left\{\ \mathcal{T}^i\left\{\ (T \otimes V \oplus U \otimes V) \parallel R^i_j \parallel Q_i \colon 1 \leq j \leq m_i\ \right\} \colon 1 \leq i \leq n\ \right\} \\ \quad\longrightarrow \mathcal{T}\left\{\ \mathcal{T}^i\{\ \mathrm{I} \colon 1 \leq j \leq m_i\ \} \colon 1 \leq i \leq n\ \right\} \\ \quad\longrightarrow \mathrm{I}\end{array}$$

Hence $\vdash (T \otimes V \oplus U \otimes V) \parallel W$ holds. Therefore, by Lemma 15, for any context $\vdash \mathcal{C}\{\ (T \oplus U) \otimes V\ \}$ yields $\vdash \mathcal{C}\{\ T \otimes V \oplus U \otimes V\ \}$, as required. $\Box$

Lemma 18 (Co-seqence Elimination) *If* $\vdash \mathcal{C}\{\ (T\ ; U) \otimes (V\ ; W)\ \}$ *then* $\vdash \mathcal{C}\{\ (T \otimes V)\ ; (U \otimes W)\ \}$.

Proof: Assume that $\vdash ((T\ ; U) \otimes (V\ ; W)) \parallel P$ holds. By Lemma 12, there exist n-ary killing context $\mathcal{T}\{\ \ \}$ and Q^0_i and Q^1_i, for $1 \leq i \leq n$, such that $\vdash (T\ ; U) \parallel Q^0_i$ and $\vdash (V\ ; W) \parallel Q^1_i$ and the following derivation holds:

$$P \longrightarrow \mathcal{T}\{\ Q^0_1 \parallel Q^1_1, Q^0_2 \parallel Q^1_2, \ldots, Q^0_n \parallel Q^1_n\ \}$$

Hence by Lemma 12, for $k \in \{0, 1\}$ there exists m^k_i-ary killing context $\mathcal{T}^k_i\{\ \ \}$ and propositions $R^k_{i,j}$ and $S^k_{i,j}$, for $1 \leq j \leq m^k_i$, such that $\vdash T \parallel R^0_{i,j}$ and $\vdash U \parallel S^0_{i,j}$ and $\vdash V \parallel R^1_{i,j}$ and $\vdash W \parallel S^1_{i,j}$ and the following derivation holds:

$$Q^k_i \longrightarrow \mathcal{T}^k_i\left\{\ R^k_{i,1}\ ; S^k_{i,1}, R^k_{i,2}\ ; S^k_{i,2} \ldots, R^k_{i,m_i}\ ; S^k_{i,m_i}\ \right\}$$

Hence we can construct the following proof.

$$
\begin{array}{l}
((T \otimes V) \mathbin{;} (U \otimes W)) \parallel P \\
\quad \longrightarrow ((T \otimes V) \mathbin{;} (U \otimes W)) \parallel \mathcal{T}\left\{\ Q_1^0 \parallel Q_1^1, Q_2^0 \parallel Q_2^1, \ldots, Q_n^0 \parallel Q_n^1\ \right\} \\
\quad \longrightarrow ((T \otimes V) \mathbin{;} (U \otimes W)) \parallel \mathcal{T}\left\{\begin{array}{ll}
 & \mathcal{T}_i^0\left\{\ R_{i,j}^0 \mathbin{;} S_{i,j}^0 : 1 \leq j \leq m_i^0\ \right\} \\
\parallel & \mathcal{T}_i^1\left\{\ R_{i,k}^1 \mathbin{;} S_{i,k}^1 : 1 \leq k \leq m_i^1\ \right\} \\
 & : 1 \leq i \leq n
\end{array}\right\} \\
\quad \longrightarrow ((T \otimes V) \mathbin{;} (U \otimes W)) \parallel \mathcal{T}\left\{\begin{array}{l}
\mathcal{T}_i^1\left\{\begin{array}{l}
\mathcal{T}_i^0\left\{\begin{array}{l} R_{i,j}^0 \mathbin{;} S_{i,j}^0 \\ : 1 \leq j \leq m_i^0 \end{array}\right\} \\
\parallel \left(R_{i,k}^1 \mathbin{;} S_{i,k}^1\right) \\
: 1 \leq k \leq m_i^1
\end{array}\right\} \\
: 1 \leq i \leq n
\end{array}\right\} \\
\quad \longrightarrow ((T \otimes V) \mathbin{;} (U \otimes W)) \parallel \mathcal{T}\left\{\begin{array}{l}
\mathcal{T}_i^1\left\{\begin{array}{l}
\mathcal{T}_i^0\left\{\begin{array}{l} \left(R_{i,j}^0 \mathbin{;} S_{i,j}^0\right) \\ \parallel \left(R_{i,k}^1 \mathbin{;} S_{i,k}^1\right) \\ : 1 \leq j \leq m_i^0 \end{array}\right\} \\
: 1 \leq k \leq m_i^1
\end{array}\right\} \\
: 1 \leq i \leq n
\end{array}\right\} \\
\quad \longrightarrow ((T \otimes V) \mathbin{;} (U \otimes W)) \parallel \mathcal{T}\left\{\begin{array}{l}
\mathcal{T}_i^1\left\{\begin{array}{l}
\mathcal{T}_i^0\left\{\begin{array}{l} \left(R_{i,j}^0 \parallel R_{i,k}^1\right) \mathbin{;} \\ \left(S_{i,j}^0 \parallel S_{i,k}^1\right) \\ : 1 \leq j \leq m_i^0 \end{array}\right\} \\
: 1 \leq k \leq m_i^1
\end{array}\right\} \\
: 1 \leq i \leq n
\end{array}\right\} \\
\quad \longrightarrow \mathcal{T}\left\{\begin{array}{l}
\mathcal{T}_i^1\left\{\begin{array}{l}
\mathcal{T}_i^0\left\{\begin{array}{l} ((T \otimes V) \mathbin{;} (U \otimes W)) \\ \parallel \left(\left(R_{i,j}^0 \parallel R_{i,k}^1\right) \mathbin{;} \left(S_{i,j}^0 \parallel S_{i,k}^1\right)\right) \\ : 1 \leq j \leq m_i^0 \end{array}\right\} \\
: 1 \leq k \leq m_i^1
\end{array}\right\} \\
: 1 \leq i \leq n
\end{array}\right\} \\
\quad \longrightarrow \mathcal{T}\left\{\begin{array}{l}
\mathcal{T}_i^1\left\{\begin{array}{l}
\mathcal{T}_i^0\left\{\begin{array}{l} \left((T \otimes V) \parallel R_{i,j}^0 \parallel R_{i,k}^1\right) \mathbin{;} \\ \left((U \otimes W) \parallel S_{i,j}^0 \parallel S_{i,k}^1\right) \\ : 1 \leq j \leq m_i^0 \end{array}\right\} \\
: 1 \leq k \leq m_i^1
\end{array}\right\} \\
: 1 \leq i \leq n
\end{array}\right\} \\
\quad \longrightarrow \mathcal{T}\left\{\begin{array}{l}
\mathcal{T}_i^1\left\{\begin{array}{l}
\mathcal{T}_i^0\left\{\begin{array}{l} \left(\left(T \parallel R_{i,j}^0\right) \otimes \left(V \parallel R_{i,k}^1\right)\right) \mathbin{;} \\ \left(\left(U \parallel S_{i,j}^0\right) \otimes \left(W \parallel S_{i,k}^1\right)\right) \\ : 1 \leq j \leq m_i^0 \end{array}\right\} \\
: 1 \leq k \leq m_i^1
\end{array}\right\} \\
: 1 \leq i \leq n
\end{array}\right\} \\
\quad \longrightarrow \mathcal{T}\left\{\ \mathcal{T}_i^1\left\{\ \mathcal{T}_i^0\left\{\ \mathrm{I} : 1 \leq j \leq m_i^0\ \right\} : 1 \leq k \leq m_i^1\ \right\} : 1 \leq i \leq n\ \right\} \\
\quad \longrightarrow \mathrm{I}
\end{array}
$$

Hence $\vdash ((T \otimes V) \mathbin{;} (U \otimes W)) \parallel P$ holds. Therefore, by Lemma 15, for any context $\vdash \mathcal{C}\{\ (T \mathbin{;} U) \otimes (V \mathbin{;} W)\ \}$ yields $\vdash \mathcal{C}\{\ (T \otimes V) \mathbin{;} (U \otimes W)\ \}$, as required. □

Lemma 19 (Atomic Co-Interact Elimination) *If* $\vdash \mathcal{C}\left\{\ a \otimes \overline{b}\ \right\}$, *where* $\vdash a \leq b$, *then* $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$.

Proof: Assume for atoms a and b, where $\vdash a \leq b$, $\vdash \left(a \otimes \overline{b}\right)\sigma \parallel T$. By Lemma 12, there exist n-ary killing context $\mathcal{T}\{\ \ \}$ and formulae U_i and V_i such that $\vdash a \parallel U_i$ and $\vdash \overline{b} \parallel V_i$, for $1 \leq i \leq n$, such that $T \longrightarrow \mathcal{T}\{\ U_1 \parallel V_1, U_2 \parallel V_2, \ldots\ \}$. By Lemma 14, for every i, there exist m_i^0-ary killing contexts $\mathcal{T}_i^0\{\ \ \}$ and atoms c_i^j such that $\vdash c_i^j \leq a$ for $1 \leq j \leq m_i^0$ such that $U_i \longrightarrow \mathcal{T}_i^0\left\{\ \overline{c_i^1}, \ldots, \overline{c_i^{m_i^0}}\ \right\}$. By Lemma 14, for every i, there exist m_i^1-ary killing contexts $\mathcal{T}_i^1\{\ \ \}$ and atoms d_i^k such that $\vdash b \leq d_i^k$ for $1 \leq k \leq m_i^1$ such that $V_i \longrightarrow \mathcal{T}_i^1\left\{\ d_i^1, \ldots, d_i^{m_i^1}\ \right\}$. Also, since $\vdash c_i^j \leq a$ and $\vdash a \leq b$ and $\vdash b \leq d_i^k$, by the transitivity of $\leq$ for atoms, $\vdash c_i^j \leq d_i^k$. Thereby the following derivation holds, by repeatedly applying the *external* rule.

$$\begin{array}{rl}
T \longrightarrow & \mathcal{T}\{\ U_1 \parallel V_1, U_2 \parallel V_2, \ldots\ \} \\
\longrightarrow & \mathcal{T}\left\{\ \mathcal{T}_i^0\left\{\ \overline{c_i^j} : 1 \leq j \leq m_i^0\ \right\} \parallel \mathcal{T}_i^1\left\{\ d_i^k : 1 \leq k \leq m_i^1\ \right\} : 1 \leq i \leq n\ \right\} \\
\longrightarrow & \mathcal{T}\left\{\ \mathcal{T}_i^1\left\{\ \mathcal{T}_i^0\left\{\ \overline{c_i^j} : 1 \leq j \leq m_i^0\ \right\} \parallel d_i^k : 1 \leq k \leq m_i^1\ \right\} : 1 \leq i \leq n\ \right\} \\
\longrightarrow & \mathcal{T}\left\{\ \mathcal{T}_i^1\left\{\ \mathcal{T}_i^0\left\{\ \overline{c_i^j} \parallel d_i^k : 1 \leq j \leq m_i^0\ \right\} : 1 \leq k \leq m_i^1\ \right\} : 1 \leq i \leq n\ \right\} \\
\longrightarrow & \mathcal{T}\left\{\ \mathcal{T}_i^1\left\{\ \mathcal{T}_i^0\left\{\ \mathrm{I} : 1 \leq j \leq m_i^0\ \right\} : 1 \leq k \leq m_i^1\ \right\} : 1 \leq i \leq n\ \right\} \longrightarrow \mathrm{I}
\end{array}$$

Hence $\vdash T$ holds. Therefore, by Lemma 15, for any context $\mathcal{C}\{\ \ \}$, if $\vdash \mathcal{C}\left\{\ a \otimes \overline{b}\ \right\}$ holds, then $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$ holds, as required. □

Proof of Theorem 3. Theorem 3 follows from the above co-rule elimination results, by induction on the size of the proposition eliminated. Thereby we establish the consistency of the system MAV. The conclusion of the proof of Theorem 3 is provided below.

Proof: The proof follows by inductively applying co-rule elimination on the structure of a proposition T appearing in a provable proposition of the form $\mathcal{C}\left\{\ T \otimes \overline{T}\ \right\}$.

The base cases for any atom a follows since subsorting over atoms is reflexive hence if $\vdash \mathcal{C}\{\ \overline{a} \otimes a\ \}$ then $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$ by Lemma 19. The base case for the unit is immediate.

As the induction hypothesis in the following cases assume that, for any contexts, $\vdash \mathcal{C}\{\ T \otimes \overline{T}\ \}$ yields $\mathcal{C}\{\ \mathrm{I}\ \}$ and $\vdash \mathcal{D}\{\ U \otimes \overline{U}\ \}$ yields $\mathcal{D}\{\ \mathrm{I}\ \}$.

Consider when the root connective in the formula is the times operator. Assume that $\vdash \mathcal{C}\{\ T \otimes U \otimes \left(\overline{T} \parallel \overline{U}\right)\ \}$ holds. By the *switch* rule, $\vdash \mathcal{C}\{\ \left(T \otimes \overline{T}\right) \parallel \left(U \otimes \overline{U}\right)\ \}$ holds. Hence, by the induction hypothesis twice, $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$ holds. The case for when parallel composition is the root connective is symmetric to the case for times.

Consider when the root connective in the formula is parallel composition operator. Assume that $\vdash \mathcal{C}\{\ (T \mathbin{;} U) \otimes \left(\overline{T} \mathbin{;} \overline{U}\right)\ \}$ holds. By Lemma 18, $\vdash \mathcal{C}\{\ \left(T \otimes \overline{T}\right) \mathbin{;} \left(U \otimes \overline{U}\right)\ \}$ holds. Hence, by the induction hypothesis twice, $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$ holds.

Consider when the root connective in the formula is the & operator. Assume that $\vdash \mathcal{C}\{\ (T \mathbin{\&} U) \otimes \left(\overline{T} \oplus \overline{U}\right)\ \}$ holds. By Lemma 17, it holds that $\vdash \mathcal{C}\{\ (T \mathbin{\&} U) \otimes \overline{T} \oplus (T \mathbin{\&} U) \otimes \overline{U}\ \}$. By Lemma 2 twice, $\vdash \mathcal{C}\{\ T \otimes \overline{T} \oplus U \otimes \overline{U}\ \}$ holds. Hence by the induction hypothesis twice, $\vdash \mathcal{C}\{\ \mathrm{I} \oplus \mathrm{I}\ \}$ holds. Hence by Lemma 16, $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$ holds, as required. The case for when internal choice, $\oplus$, is the root connective is symmetric to the case for external choice.

This completes the case analysis. Therefore, by induction on the size of the proposition T, if $\vdash \mathcal{C}\{\ T \otimes \overline{T}\ \}$ holds, then $\vdash \mathcal{C}\{\ \mathrm{I}\ \}$ holds. □

The above proof follows a similar pattern to Proposition 3, except that a co-rule elimination lemma is applied at each step. The above theorem is constructive, hence a cut elimination algorithm can be extracted from this proof that could be machine checked.

A symmetric term rewriting system. Note that no elimination result for the *co-medial* rules was required to establish cut elimination (Theorem 3). The *co-medial* rule can be eliminated directly using Corollary 1.

Lemma 20 *If* $\vdash \mathcal{C}\{\ (T \mathbin{;} U) \oplus (V \mathbin{;} W)\ \}$ *then* $\vdash \mathcal{C}\{\ (T \oplus V) \mathbin{;} (U \oplus W)\ \}$.

Proof: Assume that $\vdash \mathcal{C}\{\ (T \mathbin{;} U) \oplus (V \mathbin{;} W)\ \}$. The following proof holds in *MAV*.

$$
\begin{array}{ll}
\multicolumn{2}{l}{(T \mathbin{;} U) \oplus (V \mathbin{;} W) \multimap (T \oplus V) \mathbin{;} (U \oplus W)} \\
\longrightarrow & \left(\left(\overline{T} \mathbin{;} \overline{U}\right) \parallel ((T \oplus V) \mathbin{;} (U \oplus W))\right) \mathbin{\&} \left(\left(\overline{V} \mathbin{;} \overline{W}\right) \parallel ((T \oplus V) \mathbin{;} (U \oplus W))\right) \\
\longrightarrow & \left(\left(\overline{T} \mathbin{;} \overline{U}\right) \parallel (T \mathbin{;} U)\right) \mathbin{\&} \left(\left(\overline{V} \mathbin{;} \overline{W}\right) \parallel (V \mathbin{;} W)\right) \\
\longrightarrow & \mathrm{I} \mathbin{\&} \mathrm{I} \longrightarrow \mathrm{I}
\end{array}
$$

Hence, by context closure in Corollary 1, the following is provable.

$$\vdash \mathcal{C}\{\ (T \mathbin{;} U) \oplus (V \mathbin{;} W)\ \} \multimap \mathcal{C}\{\ (T \oplus V) \mathbin{;} (U \oplus W)\ \}$$

Furthermore, by transitivity in Corollary 1, a proof of the following can be constructed in MAV, as required: $\vdash \mathcal{C}\{\ (T \oplus V)\ ;\ (U \oplus W)\ \}$. $\square$

Co-rules are interesting in their own right, since derivations extended with all co-rules coincide with provable linear implications. Suppose that SMAV is the system MAV extended with all co-rules. The following corollary is an immediate consequence of Theorem 3, the proof being standard for related calculi with a cut elimination result.

Corollary 2 *$\vdash V \multimap U$ if and only if $U \longrightarrow V$ in SMAV.*

The advantage of the former definition of linear implication, using provability, is that MAV is in some sense *analytic* [5, 7], hence the length of derivations is bounded. In contrast, in SMAV many co-rules can be applied infinitely.

5 The Complexity of MAV

We explore some immediate consequences of cut elimination. Firstly, we prove that MAV is a conservative extension of MALL with *mix*. Secondly, this observation is used to establish the complexity class of MAV.

5.1 A Conservative Extension with the Operator Seq.

To establish that MAV is a conservative extension of MALL, we must establish that, for any proposition T in MALL, i.e. without the *seq* operator, $\vdash T$ holds in MAV if and only if $\vdash T$ holds in MALL. The proof is divided into the following two lemmas.

Lemma 21 *For any proposition T in MALL, if $\vdash T$ holds in MALL, then $\vdash T$ holds in MAV.*

Proof: The proof is by induction on the depth of the proof tree in MALL. For sequents define the following transformation for proposition T and sequents Γ and Δ.

$$[\![T]\!] = T \qquad [\![\Gamma, \Delta]\!] = [\![\Gamma]\!] \parallel [\![\Delta]\!]$$

Consider the base cases. $\vdash \overline{a}, b$ follows from the atomic interact axiom in MALL only if $a \leq b$ holds, hence $[\![\overline{a}, b]\!] \longrightarrow \text{I}$ by the atomic interact rule in MAV. If $\vdash \text{I}$, then trivially I is provable.

Consider the inductive case for times. If $\vdash \Gamma, \Delta, T \otimes U$ follows from proofs of $\vdash \Gamma, T$ and $\vdash \Delta, U$ in MALL, then by the induction hypothesis

$[\![\Gamma, T]\!]$ and $[\![\Delta, U]\!]$ are provable in MAV. Hence the following proof can be constructed in MAV.

$$[\![\Gamma, \Delta, T \otimes U]\!] \longrightarrow [\![\Gamma, T]\!] \otimes [\![\Delta, U]\!] \longrightarrow \mathrm{I}$$

Consider the inductive case for par. If $\vdash \Gamma, T \parallel U$ follows from $\vdash \Gamma, T, U$, then by the induction hypothesis $[\![\Gamma, T, U]\!]$ is provable in MAV, and furthermore $[\![\Gamma, T, U]\!] \equiv [\![\Gamma, T \parallel U]\!]$, hence we are done.

Consider the inductive case for mix. If $\vdash \Gamma, \Delta$ follows from a proof of $\vdash \Gamma$ and $\vdash \Delta$, then by the induction hypothesis $[\![\Gamma]\!]$ and $[\![\Delta]\!]$ is provable in MAV. Hence the following proof can be constructed in MAV: $[\![\Gamma, \Delta]\!] \longrightarrow \mathrm{I}$.

Consider the inductive case for with. If $\vdash \Gamma, T \mathbin{\&} U$ follows from proof of $\vdash \Gamma, T$ and $\vdash \Gamma, U$ in MALL, then by the induction hypothesis $[\![\Gamma, T]\!]$ and $[\![\Gamma, U]\!]$ are provable. Hence the following proof can be constructed in MAV.

$$[\![\Gamma, T \mathbin{\&} U]\!] \longrightarrow [\![\Gamma, T]\!] \mathbin{\&} [\![\Gamma, U]\!] \longrightarrow \mathrm{I} \mathbin{\&} \mathrm{I} \longrightarrow \mathrm{I}$$

Consider the inductive cases for plus. Without loss of generality consider the left rule. If $\vdash \Gamma, T \oplus U$ follows from a proof of $\vdash \Gamma, T$, then by the induction hypothesis $[\![\Gamma, T]\!]$ is provable in MAV. Hence the following proof can be constructed in MAV.

$$[\![\Gamma, T \oplus U]\!] \longrightarrow [\![\Gamma, T]\!] \longrightarrow \mathrm{I}$$

Hence, by induction on the depth of a proof tree in MALL, if $\vdash \Gamma$, then $[\![\Gamma]\!]$ is provable in MAV. Since $[\![T]\!] = T$, we are done. □

Notice that in a proposition that does not involve seq operator, the seq operator can be introduced in an intermediate state of the proof by a rule of the following form $\mathcal{C}\{\ (T \mathbin{;} \mathrm{I}) \parallel (\mathrm{I} \mathbin{;} U)\ \} \longrightarrow \mathcal{C}\{\ (T \parallel \mathrm{I}) \mathbin{;} (\mathrm{I} \parallel U)\ \}$, where $T \not\equiv \mathrm{I}$ and $U \not\equiv \mathrm{I}$. The proof of the following proposition checks that such scenarios do not increase the number of propositions from MALL that are provable in MAV.

By applying Theorem 1, we can establish the following contrapositive to Lemma 21.

Lemma 22 *For any proposition T in MALL, i.e. without the seq operator, if $\vdash T$ holds in MAV, then $\vdash T$ holds in MALL.*

Proof: The trick is to define a function $s(T)$ over propositions, that transforms every occurrence of seq to par, as follows, where $\odot \in \{\parallel, \otimes, \oplus, \&\}$

is any binary connective.

$$s(T \,;\, U) = l(T) \parallel l(U) \qquad s(T \odot U) = l(T) \odot l(U)$$

$$s(\text{I}) = \text{I} \qquad s(a) = a \qquad s(\overline{a}) = \overline{a}$$

We now aim to establish that if $\vdash T$ holds in MAV, then $\vdash s(T)$ is also provable in MALL. By establishing this stronger property, the lemma follows since for propositions P in MALL, $s(P) = P$ since seq never occurs in MALL.

Firstly, observe that the following equivalences hold.

- $s((T \,;\, U) \,;\, V) \equiv s(T \,;\, (U \,;\, V))$,
- $s(\text{I} \,;\, T) \equiv s(T)$,
- $s(T \,;\, \text{I}) \equiv s(T)$.

Therefore if $T \equiv U$, then $s(T) \equiv s(U)$.

The base case is when $T \equiv \text{I}$ is a proof of length 0 in MAV. In this $s(T) \equiv \text{I}$ hence the following is a proof in MALL.

$$\frac{}{\vdash s(T)}$$

Now consider proofs in MAV of length $n + 1$ of the following form.

$$W \equiv \mathcal{C}\{\ U\ \} \longrightarrow \mathcal{C}\{\ V\ \} \longrightarrow \text{I}$$

where $\mathcal{C}\{\ V\ \}$ has a proof of length n and $U \longrightarrow V$ is one instance of any rule in MAV.

For rules other than *sequence* and *medial*, observe that $s(U) \longrightarrow s(V)$ follows by applying the same rule. For example, for the *switch* rule the following holds.

$$\begin{aligned} s((P \otimes Q) \parallel R) &= (s(P) \otimes s(Q)) \parallel s(R) \\ &\longrightarrow s(P) \otimes (s(Q) \parallel s(R)) = s(P \otimes (Q \parallel R)) \end{aligned}$$

Furthermore, for all such rules, $\vdash V \multimap U$ by Lemma 1.

Consider now the cases of the *sequence* rule. The following follows by applying associativity and commutativity of par.

$$\begin{aligned} s((P \,;\, Q) \parallel (R \,;\, S)) &= (s(P) \parallel s(Q)) \parallel (s(R) \parallel s(S)) \\ &\equiv (s(P) \parallel s(R)) \parallel (s(Q) \parallel s(S)) = s((P \parallel R) \,;\, (Q \parallel S)) \end{aligned}$$

Thereby $\vdash s((P \parallel R) \mathbin{;} (Q \parallel S)) \multimap s((P \mathbin{;} Q) \parallel (R \mathbin{;} S))$ holds in MALL.

Consider also the case of the *medial* rule. In this case, observe that the following holds by definition.

$$
\begin{aligned}
&s((P \mathbin{\&} Q) \mathbin{;} (R \mathbin{\&} S)) \multimap s((P \mathbin{;} R) \mathbin{\&} (Q \mathbin{;} S)) \\
&\quad = \left(\overline{s(P)} \oplus \overline{s(Q)}\right) \otimes \left(\overline{s(R)} \oplus \overline{s(S)}\right) \parallel (s(P) \parallel s(R)) \mathbin{\&} (s(Q) \parallel s(S))
\end{aligned}
$$

Thereby $\vdash s((P \mathbin{\&} Q) \mathbin{;} (R \mathbin{\&} S)) \multimap s((P \mathbin{;} R) \mathbin{\&} (Q \mathbin{;} S))$ holds in MALL by Lemma 1.

Notice that in each case we have established that $\vdash s(V) \multimap s(U)$ holds in MALL and hence $\vdash s(\mathcal{C}\{\ V\ \}) \multimap s(\mathcal{C}\{\ U\ \})$ holds by Proposition 2. Also observe that since $\mathcal{C}\{\ U\ \} \equiv W$ we have that $s(\mathcal{C}\{\ U\ \}) \equiv s(W)$ and hence $\vdash s(\mathcal{C}\{\ U\ \}) \multimap s(W)$ holds in MALL.

Now, by the induction hypothesis, $s(\mathcal{C}\{\ V\ \})$ is provable in MALL, hence the following proof can be constructed for W using the rules of MALL and the cut rule.

$$
\dfrac{\dfrac{s(\mathcal{C}\{\ V\ \}) \qquad \vdash \overline{s(\mathcal{C}\{\ V\ \})}, s(\mathcal{C}\{\ U\ \})}{\vdash s(\mathcal{C}\{\ U\ \})} \qquad \vdash \overline{s(\mathcal{C}\{\ U\ \})}, s(W)}{\vdash s(W)}
$$

Hence, by Theorem 1, we can construct a proof of $s(W)$ in MALL. □

5.2 Seq Preserves the Complexity Bound.

Proof search in MAV, like MALL, is a PSPACE-complete decision problem. Lemmas 21 and 22, establish that provability in MAV is PSPACE-hard. It remains to establish that proof search in MAV is in PSPACE, as sketched in the following proposition.

Proposition 4 *Proof search in MAV is in PSPACE.*

Proof: The trick is to observe that branches of the proof separated by the *with* operators can be evaluated separately, in the sense that we can fix one branch of each *with* operator and never apply any rule inside the context of that branch. The following measure verifies that such derivations that forbid deductions in the context of one branch of a *with* operator are polynomial in length. For any proof, for a formula of MAV that does not involve the $\&$ operator, define the measure $\mu(T)$ to be the sum of the following:

- the number of occurrences of the $\oplus$ operator in T.

- the cardinality of the multiset relation $\not\uparrow$, defined such that for two occurrences of atoms a and b in T, $a \not\uparrow b$ if and only if there is no $\mathcal{C}\{\ \}$, U and V, such that a occurs in U and b occurs in V such that $T = \mathcal{C}\{\ U \,;\, V\ \}$.

- double the cardinality of the multiset relation $\sim$, defined such that for any two occurrences of atoms a and b in T, $a \sim b$ if and only if there is $\mathcal{C}\{\ \}$, U and V, such that a occurs in U and b occurs in V such that $T = \mathcal{C}\{\ U \parallel V\ \}$.

Every rule that is not applied inside a forbidden branch of a *with* operator strictly decreases the above measure. Hence a proof of any proposition T of size n that does not involve the & operator is of length no greater than $\mu(T)$, where $\mu(T) = \mathcal{O}\big(n^2\big)$.

Now suppose that $\vdash T$ is any proof in MAV. There are at most 2^n independent branches in T to check where n is the number of & operators that occur in the formula, obtained by hiding one branch of each *with* operator. Each of these independent branches can be investigated in parallel in a universal fashion by an alternating Turing machine [8]. An accepting state is reached when a proposition is equivalent to the unit. Since the alternating Turing machine finishes in polynomial time, and AP=PSPACE, we are done. □

Note the parallelism induced by independent branches could be illuminated further by the proposed formalisms that are more explicit about concurrent proof search in deep inference, such as formalism B [47]. It may also be interesting to revisit the above problem in the context of the interactive proof class IP [42, 34].

The following is the main complexity result of this paper.

Theorem 4 *Proof search in MAV is PSPACE complete.*

Proof: By Lemma 21 and Lemma 22, the identity embedding of a proposition of MALL in MAV, reduces the problem of provability of a proposition in MALL to provability of the same proposition in MAV. Since by Theorem 2, provability in MALL is PSPACE-complete, provability in MALL is PSPACE-hard. Since, by Lemma 4, provability in MALL is in PSPACE, the problem is PSPACE-complete. □

The suitability of this complexity bound depends on the application, e.g. to verifying protocols or to querying provenance, as discussed in the introduction. Reductions to established PSPACE-complete problems, such as certain decision problems for QBF and relational algebra, suggest a path for the implementation of tools based on MAV.

6 Conclusion and Future Work

This article is a companion paper for a conference paper [11] that observes connections between operators that appear in the proof calculi BV and MALL and operators that appear in session types. These observations lead to the system MAV investigated in this work. Further to the rules directly from BV and MAV, a rule relating *seq* from BV and *with* from MALL called the *medial* rule is required. This paper establishes proof theoretic results that are of primary importance when introducing a new proof calculus.

The main result is the generalised cut elimination result in Theorem 3. By using cut elimination, many results can be established including the transitivity of an internal notion of linear implication (Corollary 1), the completeness of the symmetric extension of MAV (Corollary 2), and several results concerning session types that appear in the companion paper [11]. This main result follows from a technique developed in the calculus of structures called splitting. Novel features include the handling of subsorting for atoms, and the direct splitting of proofs into independent branches to control the size of the proof search (Lemma 2). The most challenging case is the principal case for *seq* in Lemma 12. This particular case is challenging due to interactions between *seq* and *with*, which do not co-exist in any other published proof calculus, although the problem was acknowledged several years previously [45]. A termination measure defined over multisets of multisets of natural numbers is introduced. The preservation of the measure by the problematic case involves the substantial case analysis in Lemma 10.

The secondary result, in Theorem 4, establishes that proof search in MAV is PSPACE-complete. This result is included for a more complete picture, and to suggest an implementation path for a tool that decides provability by using a reduction to an established PSPACE-complete problem.

In the literature, Ruet [41] presents a cut elimination result for a logical system in which the additives and both commutative and non-commutative multiplicatives co-exist, called NL. A distinction between NL and MAV is that NL has a pair of De Morgan dual non-commutative operators and two multiplicative units; whereas MAV has a single self-dual non-commutative operator and a single self-dual multiplicative unit. A stronger difference is that the non-commutative operators in NL are subject to “seesaw” and “entropy” rules that together make these operators cyclic in the sense that propositions can be ordered but the last proposition in a structure is effectively ordered directly before the first, forming a cycle. Such a *cyclic* non-commutative logic has been proposed as an approach to quantum logic [52]. However, the cyclic non-commutative operators of NL do not meet the requirements of explicitly ordering events in a finite session of a protocol, as explained in the companion paper that motivates MAV [11].

The reason for such a thorough proof theoretic treatment of MAV is that we propose MAV for a range of applications in computer science. Applications include the verification of propocols using session types, as proposed in the companion paper [11], and query languages for partially ordered structures such as provenance diagrams [10, 31]. To be able to use MAV in confidence, the fact that it is a consistent logical system in a well understood complexity class, increases confidence that MAV is a "good" model to use in some objective sense.

The consistency of the system suggests that MAV is a solid starting point for future investigations into more expressive proof calculi. We know that the induction measure for splitting presented is not sufficient to handle the additive units, for which the induction measure would need to be revisited. However, we know that the techniques presented here adapt to an extension of MAV with first-order quantifiers. MAV is a finite calculus in which only finite structures can be presented. In future work, we aim to investigate extensions for second-order quantifiers [48] and infinite structures [3] that are likely to be undecidable [46, 32].

Acknowledgements. The author is grateful to Bogdan Aman for assistance with proof reading, to a reviewer who helped identify issues regarding the termination of the splitting proof in the presence of a single multiplicative unit, and careful reading by other reviewers that improved the presentation.

This work is supported by a grant of the Romanian National Authority for Scientific Research, project number PN-II-ID-PCE-2011-3-0919.

References

[1] Samson Abramsky. Computational interpretations of linear logic. *Theoretical computer science*, 111(1):3–57, 1993.

[2] Samson Abramsky and Radha Jagadeesan. Games and full completeness for multiplicative linear logic. *The Journal of Symbolic Logic*, 59(02):543–574, 1994.

[3] David Baelde. Least and greatest fixed points in linear logic. *ACM Transactions on Computational Logic (TOCL)*, 13(1):2, 2012.

[4] Richard Blute, Alessio Guglielmi, Ivan Ivanov, Prakash Panangaden, and Lutz Straßburger. A logical basis for quantum evolution and entanglement. In *Categories and Types in Logic, Language, and Physics*, volume 8222 of *LNCS*, pages 90–107, 2014.

[5] Kai Brünnler. Atomic cut elimination for classical logic. In *CSL*, pages 86–97, 2003.

[6] Paola Bruscoli. A purely logical account of sequentiality in proof search. In *ICLP*, pages 302–316, 2002.

[7] Paola Bruscoli and Alessio Guglielmi. On the proof complexity of deep inference. *ACM Transactions on Computational Logic (TOCL)*, 10(2):14, 2009.

[8] Ashok K. Chandra, Dexter C. Kozen, and Larry J. Stockmeyer. Alternation. *Journal of the ACM*, 28:114133, 1981.

[9] Kaustuv Chaudhuri, Nicolas Guenot, and Lutz Straßburger. The focused calculus of structures. In *EACSL*, volume 12, pages 159–173, 2011.

[10] Gabriel Ciobanu and Ross Horne. A provenance tracking model for data updates. In *FOCLASA*, pages 31–44, 2012.

[11] Gabriel Ciobanu and Ross Horne. Behavioural analysis of sessions using the calculus of structures. In *PSI 2015, 25-27 August, Kazan, Russia*, LNCS, 2015.

[12] J Robin B Cockett and Robert AG Seely. Weakly distributive categories. *Journal of Pure and Applied Algebra*, 114(2):133–173, 1997.

[13] Nachum Dershowitz and Zohar Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, 1979.

[14] Alexandre Frey. Satisfying subtype inequalities in polynomial space. *Theoretical Computer Science*, 277(1):105–117, 2002.

[15] Simon Gay and Malcolm Hole. Subtyping for session types in the pi calculus. *Acta Informatica*, 42(2-3):191–225, 2005.

[16] Gerhard Gentzen. Untersuchungen über das logische Schließen. I. *Mathematische zeitschrift*, 39(1):176–210, 1935.

[17] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50(1):1–112, 1987.

[18] Jean-Yves Girard. Linear logic: its syntax and semantics. *London Mathematical Society Lecture Note Series*, pages 1–42, 1995.

[19] Jay L. Gischer. The equational theory of pomsets. *Theoretical Computer Science*, 61(2-3):199–224, 1988.

[20] Alessio Guglielmi. A system of interaction and structure. *ACM Transactions on Compututational Logic*, 8, 2007.

[21] Alessio Guglielmi and Tom Gundersen. Normalisation control in deep inference via atomic flows. *Logical Methods in Computer Science*, 4(1), 2008.

[22] Alessio Guglielmi and Lutz Straßburger. A system of interaction and structure V: The exponentials and splitting. *Mathematical Structures in Computer Science*, 21(03):563–584, 2011.

[23] Tony Hoare, Bernhard Möller, Georg Struth, and Ian Wehrman. Concurrent Kleene algebra and its foundations. *Journal of Logic and Algebraic Programming*, 80(6):266–296, 2011.

[24] Kohei Honda. Types for dyadic interaction. In *CONCUR'93*, pages 509–523, 1993.

[25] Kohei Honda, Aybek Mukhamedov, Gary Brown, Tzu-Chun Chen, and Nobuko Yoshida. Scribbling interactions with a formal foundation. In *Distributed Computing and Internet Technology*, pages 55–75. 2011.

[26] Kohei Honda, Nobuko Yoshida, and Marco Carbone. Multiparty asynchronous session types. *ACM SIGPLAN Notices*, 43(1):273–284, 2008.

[27] Haruo Hosoya, Jérôme Vouillon, and Benjamin C Pierce. Regular expression types for XML. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 27(1):46–90, 2005.

[28] Raymond Hu, Rumyana Neykova, Nobuko Yoshida, Romain Demangeon, and Kohei Honda. Practical interruptible conversations. In *RV*, pages 130–148, 2013.

[29] Raymond Hu, Nobuko Yoshida, and Kohei Honda. Session-based distributed programming in Java. In *ECOOP*, pages 516–541. 2008.

[30] Ozan Kahramanogullari. System BV is NP-complete. *Ann. Pure Appl. Logic*, 152(1-3):107–121, 2008.

[31] Grigoris Karvounarakis, Zachary G. Ives, and Val Tannen. Querying data provenance. In *Proceedings of SIGMOD'10*, pages 951–962. ACM, 2010.

[32] Yves Lafont and Andre Scedrov. The undecidability of second order multiplicative linear logic. *Information and Computation*, 125(1):46–51, 1996.

[33] Patrick Lincoln, John Mitchell, Andre Scedrov, and Natarajan Shankar. Decision problems for propositional linear logic. *Ann. Pure Appl. Logic*, 56(1):239–311, 1992.

[34] Patrick D Lincoln, J Mitchell, and Andre Scedrov. Stochastic interaction and linear logic. *London Mathematical Society Lecture Note Series*, pages 147–166, 1995.

[35] Jan Łukasiewicz. *Aristotle's syllogistic from the standpoint of modern formal logic.* Oxford Clarendon Press, 1951.

[36] Roger C Lyndon. An interpolation theorem in the predicate calculus. *Pacific Journal of Mathematics*, 9(1):129–142, 1959.

[37] Nicholas Ng, Nobuko Yoshida, and Kohei Honda. Multiparty session C: Safe parallel programming with message optimisation. In *Objects, Models, Components, Patterns*, pages 202–218. 2012.

[38] Frank Pfenning. Structural cut elimination in linear logic. Technical report, DTIC Document, 1994.

[39] Christian Retoré. Pomset logic: a non-commutative extension of classical linear logic. In *Typed Lambda Calculi and Applications*, pages 300–318. 1997.

[40] Luca Roversi. Linear lambda calculus and deep inference. In Luke Ong, editor, *Typed Lambda Calculi and Applications*, volume 6690 of *LNCS*, pages 184–197. 2011.

[41] Paul Ruet. Non-commutative logic II: sequent calculus and phase semantics. *Mathematical Structures in Computer Science*, 10(02):277–312, 2000.

[42] Adi Shamir. IP = PSPACE. *Journal of the ACM (JACM)*, 39(4):869–877, 1992.

[43] Richard Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Computer Science*, 9(1):67–72, 1979.

[44] Lutz Straßburger. A local system for linear logic. In *LPAR*, pages 388–402, 2002.

[45] Lutz Straßburger. *Linear logic and noncommutativity in the calculus of structures*. PhD thesis, TU Dresden, 2003.

[46] Lutz Straßburger. System NEL is undecidable. *Electronic Notes in Theoretical Computer Science*, 84:166–177, 2003.

[47] Lutz Straßburger. From deep inference to proof nets. In *Structures and Deduction*, 2005.

[48] Lutz Straßburger. Some observations on the proof theory of second order propositional multiplicative linear logic. In *Typed Lambda Calculi and Applications*, pages 309–324. 2009.

[49] Lutz Straßburger and Alessio Guglielmi. A system of interaction and structure IV: The exponentials and decomposition. *ACM Trans. Comput. Log.*, 12(4):23, 2011.

[50] Alwen Tiu. A system of interaction and structure II: The need for deep inference. *Logical Methods in Computer Science*, 2(2), 2006.

[51] Moshe Y Vardi. The complexity of relational query languages. In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 137–146. ACM, 1982.

[52] David N. Yetter. Quantales and (noncommutative) linear logic. *Journal of Symbolic Logic*, 55(1):41–64, 1990.