De Morgan Dual Nominal Quantifiers Modelling Private Names in Non-Commutative Logic

ROSS HORNE, Computer Science and Communications, University of Luxembourg
ALWEN TIU, Research School of Computer Science, The Australian National University, Australia
BOGDAN AMAN, Alexandru Ioan Cuza University of Iaşi, Romania
GABRIEL CIOBANU, Alexandru Ioan Cuza University of Iaşi, Romania

This paper explores the proof theory necessary for recommending an expressive but decidable first-order system, named MAV1, featuring a de Morgan dual pair of nominal quantifiers. These nominal quantifiers called 'new' and 'wen' are distinct from the self-dual Gabbay-Pitts and Miller-Tiu nominal quantifiers. The novelty of these nominal quantifiers is they are polarised in the sense that 'new' distributes over positive operators while 'wen' distributes over negative operators. This greater control of bookkeeping enables private names to be modelled in processes embedded as formulae in MAV1. The technical challenge is to establish a cut elimination result, from which essential properties including the transitivity of implication follow. Since the system is defined using the calculus of structures, a generalisation of the sequent calculus, novel techniques are employed. The proof relies on an intricately designed multiset-based measure of the size of a proof, which is used to guide a normalisation technique called *splitting*. The presence of equivariance, which swaps successive quantifiers, induces complex inter-dependencies between nominal quantifiers, additive conjunction and multiplicative operators in the proof of splitting. Every rule is justified by an example demonstrating why the rule is necessary for soundly embedding processes and ensuring that cut elimination holds.

CCS Concepts: • **Theory of computation → Proof theory**; **Process calculi**; **Linear logic**;

Additional Key Words and Phrases: calculus of structures, nominal logic, non-commutative logic

ACM Reference format:
Ross Horne, Alwen Tiu, Bogdan Aman, and Gabriel Ciobanu. 2019. De Morgan Dual Nominal Quantifiers Modelling Private Names in Non-Commutative Logic. *ACM Trans. Comput. Logic* 0, 0, Article 0 (July 2019), 58 pages.
https://doi.org/10.1145/3325821

1 INTRODUCTION

This paper investigates the proof theory of a novel pair of de Morgan dual nominal quantifiers. These quantifiers are motivated by the desire to model private name binders in processes by embedding the processes directly as formulae in a suitable logical system. The logical system in which this investigation is conducted is sufficiently expressive to soundly embed the finite fragment of several process calculi.

R. Horne and A. Tiu acknowledge support from Ministry of Education, Singapore, Tier 2 grant MOE2014-T2-2-076.

Authors' addresses: R. Horne, Faculty of Science, Technology and Communication, 6 avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg, email: ross.horne@uni.lu; A. Tiu, Research School of Computer Science, The Australian National University, Building 108, North Road, Canberra, ACT 2061, Australia; email: alwen.tiu@anu.edu.au; B. Aman and G. Ciobanu, Alexandru Ioan Cuza University of Iaşi, Romania; email: bogdan.aman@iit.academiaromana-is.ro and gabriel@info.uaic.ro.

A requirement of directly embedding processes as formulae is that the logic should be able to capture causal dependencies. To do so, we employ a non-commutative multiplicative operator, which can be used to model the fact that 'a happens before b' is not equivalent to 'b happens before a'. Such non-commutative operators are problematic for traditional proof frameworks such as the sequent calculus; hence we adopt a formalism called the *calculus of structures* [21, 22, 48, 52, 53]. The calculus of structures permits more proofs than the sequent calculus, by allowing inference rules to be applied in any context; while still satisfying proof theoretic properties, notably cut elimination. An advantage of the calculus of structures is that it can express proof systems combining connectives for sequentiality and parallelism. The calculus of structures was motivated by a need for understanding why pomset logic [45] could not be expressed in the sequent calculus. Pomset logic is inspired by pomsets [44] and linear logic [18], the former being a model of concurrency respecting causality, while the latter can be interpreted in various ways as a logic of resources and concurrency [11, 31, 56].

These observations lead to the propositional system MAV [23] and its first-order extension presented in this work, named MAV1. Related work establishes that linear implication in such logical systems is sound with respect to both pomset ideals [25] and weak simulation [26]. These results tighten results in initial investigations concerning a minimal calculus BV and trace inclusion [8]. Hence reasoning using linear implication is sound with respect to most useful (weak) preorders over processes, for a range of languages not limited to CCS [39] and π-calculus [41].

This paper resolves the fundamental logical problem of whether cut elimination holds for MAV1. Cut elimination, the corner stone of a proof system, is essential for confidently recommending a proof system. In the setting of the calculus of structures, cut elimination is formalised quite differently compared to traditional proof frameworks; hence the proof techniques employed in this paper are of considerable novelty. Furthermore, this paper is the first paper to establish cut elimination for a de Morgan dual pair of nominal quantifiers in any proof framework. These nominal quantifiers introduce intricate interdependencies between other operators in the calculus, reflected in the technique of *splitting* (Lemma 4.19) which is the key lemma required to establish cut elimination (Theorem 3.3).

Logically speaking, nominal quantifiers И and Э, pronounced 'new' and 'wen' respectively, sit between $\forall$ and $\exists$ such that $\forall x.P \multimap \text{И} x.P$ and $\text{И} x.P \multimap \text{Э} x.P$ and $\text{Э} x.P \multimap \exists x.P$, where $\multimap$ is linear implication. The quantifier И is similar in some respects to $\forall$, whereas Э is similar to $\exists$. A crucial difference between $\exists x.P$ and $\text{Э} x.P$ is that variable x in the latter cannot be instantiated with arbitrary terms, but only 'fresh' names introduced by И. Our *new* quantifier И, distinct from the Gabbay-Pitts quantifier, addresses limitations of established self-dual nominal quantifiers for modelling private names in embeddings of processes as formulae. In particular, our И quantifier does not distribute over parallel composition in either direction. In MAV1, the formulae $\text{И} x.(\text{event}(x) \parr \text{event}(x))$ and $\text{И} x.\text{event}(x) \parr \text{И} x.\text{event}(x)$ are unrelated by linear implication. This property is essential for soundly modelling private name binders in processes.

Outline. For a new logical system it is necessary to justify correctness, which we approach in proof theoretic style by cut elimination. Section 2 illustrates why an established self-dual nominal quantifier [16, 17, 38, 43] is incapable of soundly modelling name restriction in a processes-as-formulae embedding. Section 3 defines MAV1, explains cut elimination and discusses rules. Section 3.4 presents an explanation of the rules for the nominal quantifiers. Section 4 presents technical lemmas and the *splitting* technique which is key to cut elimination. Section 5 presents a context lemma which is used to eliminate *co-rules* that form a cut; thereby establishing cut elimination. Section 6 explains the complexity classes for various fragments of MAV1.

The cut elimination result in this article was announced at CONCUR 2016 [27], without full proofs. This journal version of the paper explains the cut elimination proof, elaborates on the motivating discussion, and highlights further corollaries of cut elimination. Since И is a Cyrillic vowel, we use another Cyrillic vowel Э for nominal quantifier ’wen’. This Cyrillic vowel is pronounced as the hard e in ‘wen’ and reminds the reader of its existential nature.

Due to the space limitation, some proofs are omitted in the printed version of this article, but are available in the accompanying Electronic Appendix.

2 WHY NOT A SELF-DUAL NOMINAL QUANTIFIER?

Nominal quantifiers in the literature are typically self-dual in the sense of de Morgan dualities. That is, for a nominal quantifier, say ∇, “not ∇x P” is equivalent to “∇x not P.” Such self-dual nominal quantifiers have been successfully introduced in classical and intuitionistic frameworks, typically used to reason about higher-order abstract syntax with name binders. Such nominal frameworks are therefore suited to program analysis, where the semantics of a programming language are encoded as a theory over terms in the logical framework.

Rather surprisingly, when processes themselves are directly embedded as formulae in a logic, where constructs are mapped directly to primitive logical connectives (as opposed to terms inside a logical encoding of the semantics of processes), self-dual quantifiers do not exhibit typical properties expected of name binders. To understand this problem, in this section we recall an established calculus BVQ [46] that can directly embed processes but features a self-dual nominal quantifier. We explain that such a self-dual quantifier provides an unsound semantics for name binders. This motivates the need for a finer polarised nominal quantifier, which leads to the calculus introduced in subsequent sections.

We assume the reader has a basic understanding of the semantics of the π-calculus [41] and CCS [39]. This section provides necessary preliminaries for the calculus of structures.

2.1 An established extension of BV with a self-dual quantifier

An abstract syntax for formulae and the rules of BVQ are defined in Fig 1. In an inference rule, the formula appearing above the horizontal line is the premise and the formula below the horizontal line is the conclusion. The key feature of the calculus of structures is *deep inference*, which is the ability to apply all rules in any context, i.e. formulae with a hole of the following form: $C\{\ \} ::= \{\ \cdot\ \} \mid C\{\ \} \odot P \mid P \odot C\{\ \} \mid \nabla x.C\{\ \}$, where $\odot \in \{\lhd, \parr, \otimes\}$.

Inference rules are defined *modulo a structural congruence*, where a congruence is an equivalence relation that holds in any context. A *derivation* is a sequence of rules from Fig. 1, where the structural congruence can be applied at any point in a derivation. The length of a derivation involving only the structural congruence is zero. The length of a derivation involving one inference rule instance is one. Given a derivation $\frac{P}{Q}$ of length m and another $\frac{Q}{R}$ of length n, the derivation $\frac{P}{R}$ is of length $m + n$. Unless we make it clear in the context that we refer to a specific rule, this horizontal line notation is generally used to represent derivations of any length. For example, since $\nabla x.\circ \equiv \circ$, derivation $\frac{\circ}{\nabla x.\circ}$ of length 0, and derivation $\frac{(P \parr R) \otimes (Q \parr S)}{(P \otimes Q) \parr R \parr S}$ is of length 2, since two instances of *switch* are applied.

The congruence, $\equiv$ in Fig. 1, makes *par* and *times* commutative and *seq* non-commutative in general. For the nominal quantifier ∇, the congruence enables: α-conversion for renaming bound names; *equivariance* which allows names bound by successive nominal quantifiers to be swapped; and *vacuous* that allows the nominal quantifier to be introduced or removed whenever the bound variable does not appear in the formula. As standard, we define a freshness predicate such that a

Structural rules

$(P, \parr, \circ)$ and $(P, \otimes, \circ)$ are commutative monoids

$(P, \lhd, \circ)$ is a monoid $\qquad$ α-conversion for ∇ quantifier

$$\nabla x.\nabla y.P \equiv \nabla y.\nabla x.P \text{ (equivariance)}$$

$$\nabla x.P \equiv P \text{ only if } x \mathrel{\#} P \text{ (vacuous)}$$

Syntax

$$\begin{array}{lll} P ::= & \circ & \text{(unit)} \\ & \alpha & \text{(atom)} \\ & \overline{\alpha} & \text{(co-atom)} \\ & \nabla x.P & \text{(nabla)} \\ & P \parr P & \text{(par)} \\ & P \otimes P & \text{(times)} \\ & P \lhd P & \text{(seq)} \end{array}$$

Inference rules

$$\frac{C\{\ \circ\ \}}{C\{\ \overline{\alpha} \parr \alpha\ \}}\ \text{(atomic interaction)} \qquad \frac{C\{\ (P \parr Q) \otimes S\ \}}{C\{\ P \parr (Q \otimes S)\ \}}\ \text{(switch)}$$

$$\frac{C\{\ (P \parr R) \lhd (Q \parr S)\ \}}{C\{\ (P \lhd Q) \parr (R \lhd S)\ \}}\ \text{(sequence)} \qquad \frac{C\{\ \nabla x.(P \parr Q)\ \}}{C\{\ \nabla x.P \parr \nabla x.Q\ \}}\ \text{(unify)}$$

Fig. 1. Syntax and rules of system BVQ [46]: which is BV extended with a self-dual nominal quantifier.

variable x is fresh for a formulae P, written $x \mathrel{\#} P$, if and only if x is not a member of the set of free variables of P, where $\nabla x.P$ binds occurrences of x in P.

Consider the syntax and rules of BVQ in Figure 1. The three rules *atomic interaction* and *switch* and *sequence* define the basic system BV [21] that also forms the core of the system MAV1 investigated in later sections. The only additional inference rule for ∇ is called *unify*.

Atomic interaction. The atomic interaction rule should remind the reader of the classical tautology $\neg\alpha \vee \alpha$ or intuitionistic axiom $\alpha \implies \alpha$, applied only to the predicates forming the atoms of the calculus. Since there is no contraction rule for $\parr$, once atoms are consumed by *atomic interaction* they cannot be reused. Thus *atomic interaction* is useful for modelling communication in process, where α models a receive action or event and $\overline{\alpha}$ is the complementary send, which cancel each other out.

Switch and sequence. The *atomic interaction* and *switch* rules together provide a model for multiplicative linear logic (with *mix*) [18]. The difference between $\parr$ and $\otimes$ is that $\parr$ allows interaction, but $\otimes$ does not. In this sense the switch rule restricts where which atoms may interact. The *seq* rule also restricts where interactions can take place, but, since *seq* is non-commutative, it can be used to capture causal dependencies between atoms. The *sequence* rule preserves these causal dependencies, while permitting new causal dependencies. In terms of process models, the *sequence* rule appears in the theory of pomsets [19] and can refine parallel composition to its interleavings.

Unify. The novel rule for BVQ is *unify* for nominal quantifier ∇. The *unify* rule should be admissible in a well-designed extension of linear logic with a self-dual quantifier. To see why, consider the following auxiliary definitions. Observe that the following definition of linear implication ensures that ∇ is self-dual in the sense that the de Morgan dual of ∇ is ∇ itself. Similarly, *seq* and the unit are self-dual, while $\otimes$ and $\parr$ are a de Morgan dual pair of operators.

Definition 2.1. Linear negation is defined by the following function over formulae.

$$\overline{\circ} = \circ \qquad \overline{\overline{\alpha}} = \alpha \qquad \overline{P \otimes Q} = \overline{P} \parr \overline{Q} \qquad \overline{P \parr Q} = \overline{P} \otimes \overline{Q} \qquad \overline{P \lhd Q} = \overline{P} \lhd \overline{Q} \qquad \overline{\nabla x.P} = \nabla x.\overline{P}$$

Linear implication, written $P \multimap Q$, is defined as $\overline{P} \parr Q$.

We are particularly interested in special derivations, called proofs.

Definition 2.2. A *proof* is a derivation of any length with conclusion P and premise $\circ$. When such a derivation exists, we say that P is provable, and write $\vdash P$ holds.

As a basic property of linear implication $\vdash P \multimap P$ must hold for any P. Now assume that $\vdash Q \multimap Q$ is provable in BVQ (hence, by the above definitions, there exists a derivation with conclusion $\overline{Q} \parr Q$ and premise $\circ$), and consider formula $\nabla x.Q$. Using the *unify* rule and the definition of linear implication, we can construct the following proof of $\vdash \nabla x.Q \multimap \nabla x.Q$.

$$\dfrac{\dfrac{\dfrac{\circ}{\nabla x.\circ}\ \text{by the \textit{vacuous} rule}}{\nabla x.\left(\overline{Q} \parr Q\right)}\ \text{by the assumption } \vdash \overline{Q} \parr Q}{\nabla x.\overline{Q} \parr \nabla x.Q}\ \text{by the \textit{unify} rule}$$

The above illustrates why *unify* should be admissible in order to guarantee *reflexivity* — the most basic property of implication — for an extension of BV with a self-dual nominal quantifier. In the next section, we explain why the *unify* rule is problematic for modelling processes as formulae.

2.2 Fundamental problems with a self-dual nominal for embeddings of processes

Initially, it seems that desirable properties of name binding, typical of process calculi, are achieved in BVQ. For example, we expect that if $x \mathrel{\#} Q$ then $\vdash \nabla x. (P \parr Q) \multimap \nabla x.P \parr Q$, indicating that the scope of a name can be *extruded* as long as another name is not captured, which is provable using the *vacuous* and *unify* rules. The *equivariance* rule that swaps name binders is also a property preserved by most equivalences over processes.

Another strong property of BVQ, expected of all nominal quantifiers, is that we avoid the *diagonalisation* property. Diagonalisation $\vdash \forall x.\forall y.P(x, y) \multimap \forall z.P(z, z)$ holds in any system with universal quantifiers, as does the converse for existential quantifiers. However, for nominals such at ∇, **neither** $\nabla x.\nabla y.P(x, y) \multimap \nabla z.P(z, z)$ **nor** its converse $\nabla z.P(z, z) \multimap \nabla x.\nabla y.P(x, y)$ hold. This is a critical feature of all nominal quantifiers that ensures that distinct fresh names in the same scope never collapse to the same name, and explains why universal and existential quantifiers are not suited modelling fresh name binders. It is precisely the absence of diagonalisation for nominals that is used in classical [16, 43] and intuitionistic frameworks [17, 38] to logically manage the bookkeeping of fresh name in, so called, *deep embeddings* of processes as terms in a theory. Avoiding diagonalisation is sufficient in such deep embeddings since nominal quantifiers cannot appear inside a term representation of a process, so are always pushed to the outermost level where formulae are used to define the operational semantics of processes as a theory over process terms.

Soundness criterion. The problem with BVQ is that when processes are directly embedded as formulae ∇ quantifiers may appear inside embeddings of processes, which can result in unsound behaviours. To see why the *unify* rule induces unsound behaviours consider the following π-calculus terms. $\nu x.(\overline{z}x \mid \overline{y}x)$ is a π-calculus process that can output a fresh name twice, once on channel z and once on channel y; but cannot output two distinct names in any execution. In contrast, observe that $\nu x.\overline{z}x \mid \nu x.\overline{y}x$ is a π-calculus process that outputs two distinct fresh names before terminating, but cannot output the same name twice in any execution. As a soundness criterion, since the processes $\nu x.(\overline{z}x \mid \overline{y}x)$ and $\nu x.\overline{z}x \mid \nu x.\overline{y}x$ do not have any complete traces in common, these processes must not be related by any sound preorder over processes.

Now consider an embedding of these processes in BVQ, where the parallel composition operator of the π-calculus is encoded as *par* and ν is encoded as ∇. This gives us the formulae $\nabla x.\left(\overline{\mathrm{act}(z, x)} \parr \overline{\mathrm{act}(y, x)}\right)$ and $\nabla x.\overline{\mathrm{act}(z, x)} \parr \nabla x.\overline{\mathrm{act}(y, x)}$. Note that output action prefixes are encoded as negated predicates, e.g., $\overline{z}x$ is encoded $\overline{\mathrm{act}(z, x)}$.

Observe that $\vdash \nabla x.\left(\overline{\text{act}(z,x)} \parr \overline{\text{act}(y,x)}\right) \multimap \nabla x.\overline{\text{act}(z,x)} \parr \nabla x.\overline{\text{act}(y,x)}$ is provable, as follows.

$$\begin{array}{cl}
\circ & \\ \hline
\nabla x.\circ & \text{by } \textit{vacuous} \\ \hline
\nabla x.\left(\text{act}(y,x) \parr \overline{\text{act}(y,x)}\right) & \text{by } \textit{atomic interaction} \\ \hline
\nabla x.\left(\left(\text{act}(z,x) \parr \overline{\text{act}(z,x)}\right) \otimes \left(\text{act}(y,x) \parr \overline{\text{act}(y,x)}\right)\right) & \text{by } \textit{atomic interaction} \\ \hline
\nabla x.\left(\left(\left(\text{act}(z,x) \parr \overline{\text{act}(z,x)}\right) \otimes \text{act}(y,x)\right) \parr \overline{\text{act}(y,x)}\right) & \text{by } \textit{switch} \\ \hline
\nabla x.\left((\text{act}(z,x) \otimes \text{act}(y,x)) \parr \overline{\text{act}(z,x)} \parr \overline{\text{act}(y,x)}\right) & \text{by } \textit{switch} \\ \hline
\nabla x.(\text{act}(z,x) \otimes \text{act}(y,x)) \parr \nabla x.\left(\overline{\text{act}(z,x)} \parr \overline{\text{act}(y,x)}\right) & \text{by } \textit{unify} \\ \hline
\nabla x.(\text{act}(z,x) \otimes \text{act}(y,x)) \parr \nabla x.\overline{\text{act}(z,x)} \parr \nabla x.\overline{\text{act}(y,x)} & \text{by } \textit{unify}
\end{array}$$

The above implication is **unsound** with respect to trace inclusion for the π-calculus. The implication wrongly suggests that the process $\nu x.\bar{z}x \mid \nu x.\bar{y}x$, that cannot output the same names twice, can be refined to a process $\nu x.(\bar{z}x \mid \bar{y}x)$, that outputs the same name twice. This is exactly the contradiction that we avoid by using polarised nominal quantifiers investigated in subsequent sections.

As a further example of unsoundness issues for a self-dual nominal, consider the following criterion: an embedding of a process is provable if and only if there is a series of internal transitions leading to a successful termination state. A successful termination state is a state without any unconsumed actions. Now consider the process $\nu x.(x.y) \mid \nu z.\bar{z} \mid \bar{y}$ in process calculus **CCS** [39]. We can attempt to embed this process in BVQ as $\nabla x.(\text{event}(x) \triangleleft \text{event}(y)) \parr \nabla z.\overline{\text{event}(z)} \parr \overline{\text{event}(y)}$, where $\text{event}(x)$ is a unary predicate representing an event identified by variable x. This embedding **violates** our soundness criterion. Under the semantics of CCS the process is immediately deadlocked; hence none of the four actions are consumed. However, the embedding is a provable formula, by the following derivation.

$$\begin{array}{cl}
\circ & \\ \hline
\nabla x.\left(\text{event}(y) \parr \overline{\text{event}(y)}\right) & \text{by } \textit{atomic interaction} \text{ and } \textit{vacuous} \\ \hline
\nabla x.\left(\left(\text{event}(x) \parr \overline{\text{event}(x)}\right) \triangleleft \left(\text{event}(y) \parr \overline{\text{event}(y)}\right)\right) & \text{by } \textit{atomic interaction} \\ \hline
\nabla x.\left((\text{event}(x) \triangleleft \text{event}(y)) \parr \left(\overline{\text{event}(x)} \triangleleft \overline{\text{event}(y)}\right)\right) & \text{by } \textit{sequence} \\ \hline
\nabla x.\left((\text{event}(x) \triangleleft \text{event}(y)) \parr \overline{\text{event}(x)} \parr \overline{\text{event}(y)}\right) & \text{by } \textit{sequence} \\ \hline
\nabla x.\left((\text{event}(x) \triangleleft \text{event}(y)) \parr \overline{\text{event}(x)}\right) \parr \overline{\text{event}(y)} & \text{by } \textit{vacuous} \text{ and } \textit{unify} \\ \hline
\nabla x.(\text{event}(x) \triangleleft \text{event}(y)) \parr \nabla z.\overline{\text{event}(z)} \parr \overline{\text{event}(y)} & \text{by } \textit{unify} \text{ and } \alpha\text{-conversion}
\end{array}$$

The above observations lead to a specification of the properties desired for a nominal quantifier suitable for direct embeddings of processes as formulae. We desire a nominal quantifier, say И, such that properties such as *no diagonalisation*, *equivariance* and *extrusion* hold except that also **neither** $\text{И}x.(P \parr Q) \multimap \text{И}x.P \parr \text{И}x.Q$ **nor** $\text{И}x.P \parr \text{И}x.Q \multimap \text{И}x.(P \parr Q)$ hold in general. Also, by the arguments above the quantifier cannot be self-dual; and hence, as a side effect, we expose another nominal quantifier, called “wen”, denoted Э, that is de Morgan dual to И. The rest of this paper is devoted to establishing that indeed there does exist a logical system with such a pair of nominal quantifiers.

$$
\begin{array}{c}
x \text{ a variable} \\[1ex]
c \text{ a constant} \\[1ex]
f \text{ a function symbol} \\[1ex]
\mathrm{p} \text{ a predicate symbol}
\end{array}
\qquad
\begin{array}{rcll}
P & ::= & \circ & \text{(unit)} \\
 & & \alpha & \text{(atom)} \\
 & & \overline{\alpha} & \text{(co-atom)} \\
 & & \forall x.P & \text{(all)} \\
 & & \exists x.P & \text{(some)} \\
 & & \text{И}x.P & \text{(new)} \\
 & & \text{Э}x.P & \text{(wen)} \\
 & & P \mathbin{\&} P & \text{(with)} \\
 & & P \oplus P & \text{(plus)} \\
 & & P \parr P & \text{(par)} \\
 & & P \otimes P & \text{(times)} \\
 & & P \triangleleft P & \text{(seq)}
\end{array}
$$

$$
\begin{array}{rcll}
t & ::= & x & \text{(variable)} \\
 & & c & \text{(constant)} \\
 & & f(t, \ldots t) & (n\text{-ary function)} \\[1ex]
\alpha & ::= & \mathrm{p}(t, \ldots t) & (n\text{-ary predicate)}
\end{array}
$$

Fig. 2. Syntax for MAV1 formulae.

$$(P, \parr, \circ) \text{ and } (P, \otimes, \circ) \text{ are commutative monoids and } (P, \triangleleft, \circ) \text{ is a monoid.}$$

$$\text{И}x.\text{И}y.P \equiv \text{И}y.\text{И}x.P \qquad \text{Э}x.\text{Э}y.P \equiv \text{Э}y.\text{Э}x.P \qquad \text{(equivariance)}$$

Fig. 3. Structural congruence ($\equiv$) for MAV1 formulae, plus α-conversion for all quantifiers.

3 INTRODUCING A PROOF SYSTEM WITH A PAIR OF NOMINAL QUANTIFIERS

Soundness issues associated with a self-dual nominal quantifier in embeddings of processes as formulae, can be resolved by instead using a pair of de Morgan dual nominal quantifiers. This section introduces a proof system for such a pair of nominal quantifiers, building on the core system BV, further extended with: additives useful for expressing non-deterministic choice; and first-order quantifiers which range over terms not only fresh names. Investigating the pair of nominal quantifiers in the presence of these operators is essential for understanding the interplay between nominal quantifiers and other operators, showing that this pair of nominal quantifiers can exist in a system sufficiently expressive to embed rich process models. This section also summarises the main proof theoretic result, although lemmas are postponed until later sections.

3.1 The inference rules and structural rules

We present the syntax and rules of a first-order system expressed in the calculus of structures, with the technical name MAV1. The derivations of the system are defined by the *abstract syntax* in Fig. 2, *structural congruence* in Fig. 3, and the *inference rules*, in Fig 4. We emphasise that, in contrast to the sequent calculus, rules can be applied in any context, i.e. MAV1 formulae from Fig. 2 with a hole of the form

$$C\{\ \} ::= \{\ \cdot\ \} \mid C\{\ \} \odot P \mid P \odot C\{\ \} \mid \text{Ꝺ}x.C\{\ \}\,, \text{ where } \odot \in \{\triangleleft, \parr, \otimes, \&, \oplus\} \text{ and } \text{Ꝺ} \in \{\exists, \forall, \text{И}, \text{Э}\}.$$

We also assume the standard notion of capture avoiding substitution of a variable for a term. Terms may be constructed from variables, constants and function symbols.

To explore the theory of proofs, two auxiliary definitions are introduced: linear negation and linear implication. Notice in the syntax in Fig. 2 linear negation applies only to atoms.

$$\frac{C\{\, \circ \,\}}{C\{\, \overline{\alpha} \parr \alpha \,\}}\ \text{(atomic interaction)} \qquad \frac{C\{\, (P \parr Q) \otimes S \,\}}{C\{\, P \parr (Q \otimes S) \,\}}\ \text{(switch)}$$

$$\frac{C\{\, (P \parr U) \lhd (Q \parr V) \,\}}{C\{\, (P \lhd Q) \parr (U \lhd V) \,\}}\ \text{(sequence)}$$

$$\frac{C\{\, (P \parr S) \mathbin{\&} (Q \parr S) \,\}}{C\{\, (P \mathbin{\&} Q) \parr S \,\}}\ \text{(external)} \qquad \frac{C\{\, (P \mathbin{\&} U) \lhd (Q \mathbin{\&} V) \,\}}{C\{\, (P \lhd Q) \mathbin{\&} (U \lhd V) \,\}}\ \text{(medial)}$$

$$\frac{C\{\, \circ \,\}}{C\{\, \circ \mathbin{\&} \circ \,\}}\ \text{(tidy)} \qquad \frac{C\{\, P \,\}}{C\{\, P \oplus Q \,\}}\ \text{(left)} \qquad \frac{C\{\, Q \,\}}{C\{\, P \oplus Q \,\}}\ \text{(right)}$$

$$\frac{C\{\, \forall x.(P \parr R) \,\}}{C\{\, \forall x.P \parr R \,\}}\ \text{(extrude1)} \qquad \frac{C\{\, \forall x.P \lhd \forall x.S \,\}}{C\{\, \forall x.(P \lhd S) \,\}}\ \text{(medial1)}$$

$$\frac{C\{\, \circ \,\}}{C\{\, \forall x.\circ \,\}}\ \text{(tidy1)} \qquad \frac{C\{\, P\{{}^{t}\!/\!{}_{x}\} \,\}}{C\{\, \exists x.P \,\}}\ \text{(select1)}$$

$$\frac{C\{\, \text{И}x.(P \parr R) \,\}}{C\{\, \text{И}x.P \parr R \,\}}\ \text{(extrude new)} \qquad \frac{C\{\, \text{И}x.P \lhd \text{И}x.S \,\}}{C\{\, \text{И}x.(P \lhd S) \,\}}\ \text{(medial new)}$$

$$\frac{C\{\, \circ \,\}}{C\{\, \text{И}x.\circ \,\}}\ \text{(tidy name)} \qquad \frac{C\{\, \text{И}x.(P \parr Q) \,\}}{C\{\, \text{И}x.P \parr \text{Э}x.Q \,\}}\ \text{(close)}$$

$$\frac{C\{\, \text{И}x.P \,\}}{C\{\, \text{Э}x.P \,\}}\ \text{(fresh)} \qquad \frac{C\{\, \text{Э}y.\text{И}x.P \,\}}{C\{\, \text{И}x.\text{Э}y.P \,\}}\ \text{(new wen)} \qquad \frac{C\{\, \text{Ꝺ}y.\forall x.P \,\}}{C\{\, \forall x.\text{Ꝺ}y.P \,\}}\ \text{(all name)}$$

$$\frac{C\{\, \text{Э}x.(P \odot S) \,\}}{C\{\, \text{Э}x.P \odot \text{Э}x.S \,\}}\ \text{(suspend)} \qquad \frac{C\{\, \text{Э}x.(P \odot R) \,\}}{C\{\, \text{Э}x.P \odot R \,\}}\ \text{(left wen)} \qquad \frac{C\{\, \text{Э}x.(R \odot Q) \,\}}{C\{\, R \odot \text{Э}x.Q \,\}}\ \text{(right wen)}$$

$$\frac{C\{\, \text{Ꝺ}x.(P \mathbin{\&} S) \,\}}{C\{\, \text{Ꝺ}x.P \mathbin{\&} \text{Ꝺ}x.S \,\}}\ \text{(with name)} \qquad \frac{C\{\, \text{Ꝺ}x.(P \mathbin{\&} R) \,\}}{C\{\, \text{Ꝺ}x.P \mathbin{\&} R \,\}}\ \text{(left name)} \qquad \frac{C\{\, \text{Ꝺ}x.(R \mathbin{\&} Q) \,\}}{C\{\, R \mathbin{\&} \text{Ꝺ}x.Q \,\}}\ \text{(right name)}$$

where $\text{Ꝺ} \in \{\text{И}, \text{Э}\}$, $\odot \in \{\parr, \lhd\}$ and $x \# R$, in all rules containing R

Fig. 4. Rules for formulae in system MAV1. Notice the figure is divided into four parts. The first part defines sub-system BV [21]. The first and second parts define sub-system MAV [23].

Definition 3.1. *Linear negation* is defined by the following function from formulae to formulae.

$$\overline{\overline{\alpha}} = \alpha \qquad \overline{P \otimes Q} = \overline{P} \parr \overline{Q} \qquad \overline{P \parr Q} = \overline{P} \otimes \overline{Q} \qquad \overline{P \oplus Q} = \overline{P} \mathbin{\&} \overline{Q} \qquad \overline{P \mathbin{\&} Q} = \overline{P} \oplus \overline{Q}$$

$$\overline{\circ} = \circ \qquad \overline{P \lhd Q} = \overline{P} \lhd \overline{Q} \qquad \overline{\forall x.P} = \exists x.\overline{P} \qquad \overline{\exists x.P} = \forall x.\overline{P} \qquad \overline{\text{И}x.P} = \text{Э}x.\overline{P} \qquad \overline{\text{Э}x.P} = \text{И}x.\overline{P}$$

Linear implication, written $P \multimap Q$, is defined as $\overline{P} \parr Q$.

Linear negation defines de Morgan dualities. As in linear logic, the multiplicatives $\otimes$ and $\parr$ are de Morgan dual; as are the additives $\&$ and $\oplus$, the first-order quantifiers $\exists$ and $\forall$, and the nominal quantifiers И and Э. As in BV, *seq* and the unit are self-dual.

A basic, but essential, property of implication can be established immediately. The following proposition is simply a reflexivity property of linear implication in MAV1.

Proposition 3.2 (Reflexivity). *For any formula P, $\vdash \overline{P} \parr P$ holds, i.e., $\vdash P \multimap P$.*

The proof of the above follows by a straightforward induction over the structure of P.

3.2 Intuitive explanations for the rules of MAV1.

We briefly recall the established system MAV, before explaining the rules for quantifiers. This paper focuses on necessary proof theoretical prerequisites, and hints at result for process embeddings in MAV1. Details on the soundness of process embeddings appear in a companion paper [26].

The additives. The rules of the basic system BV in the top part of Fig. 4 are as described previously in Section 2. The first and second parts of Fig. 4 define multiplicative-additive system MAV [23]. The additives are useful for modelling non-deterministic choice in processes [1]: the *left* rule $\dfrac{P}{P \oplus Q}$ suggests we chose the left branch P **or** alternatively the right branch Q by using the *right* rule; the *external* rule $\dfrac{(P \parr R) \& (Q \parr R)}{(P \& Q) \parr R}$ suggests that we try both branches $P \parr R$ **and** $Q \parr R$ separately; and the *tidy* rule indicates a derivation is successfully only if both branches explored are successful. The *medial* rule is a partial distributivity property between the additives and *seq* (in concurrency theory, this is a property expected of most preorders over processes). The role of the additives as a form of *internal* and *external* choice has been investigated in related work [13].

The first-order quantifiers. The rules for the first-order quantifiers in the third part of Fig. 4 follow a similar pattern to the additives. The *select1* rule allows a variable to be replaced by any term. Notice we stick to the first-order case, since variables only appear in atomic formulae and may only be replaced by terms. The *extrude1*, *tidy1* and *medial1* rules follow a similar pattern to the rules for the additives *external*, *tidy* and *medial* respectively. In process embeddings, first-order quantifiers are useful as input binders. For example we can soundly embed the π-calculus process $\overline{y}z \mid y(x).\overline{x}w \mid z(x)$ as the following provable formula:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\overline{\mathsf{act}(z, w)} \parr \mathsf{act}(z, w)}\ \text{by } \textit{atomic interaction}}{\overline{\mathsf{act}(z, w)} \parr \exists v.\mathsf{act}(z, v)}\ \text{by } \textit{select1}}{\left(\left(\overline{\mathsf{act}(y, z)} \parr \mathsf{act}(y, z)\right) \triangleleft \overline{\mathsf{act}(z, w)}\right) \parr \exists v.\mathsf{act}(z, v)}\ \text{by } \textit{atomic interaction}}{\overline{\mathsf{act}(y, z)} \parr \left(\mathsf{act}(y, z) \triangleleft \overline{\mathsf{act}(z, w)}\right) \parr \exists v.\mathsf{act}(z, v)}\ \text{by } \textit{sequence}}{\overline{\mathsf{act}(y, z)} \parr \exists x.\left(\mathsf{act}(y, x) \triangleleft \overline{\mathsf{act}(x, w)}\right) \parr \exists v.\mathsf{act}(z, v)}\ \text{by } \textit{select1}
$$

Notice, that the above process can also reach a successfully terminated state using τ transitions in the π-calculus semantics. Indeed the cut elimination result established in this paper is a prerequisite in order to prove this soundness criterion holds for finite π-calculus processes.

The polarised nominal quantifiers. The rules for the de Morgan dual pair of nominal quantifiers are more intricate. For first-order quantifiers many properties are derivable, e.g., the following implications hold (appealing to Prop. 3.2): $\vdash \forall x.\forall y.P \multimap \forall y.\forall x.P$, $\vdash \exists x.\forall y.P \multimap \forall y.\exists x.P$ and

$\vdash \forall x.(P \parr Q) \multimap \forall x.P \parr \exists x.Q$. The three proofs proceed as follows.

$$\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\forall y.\forall x.\circ}}{\forall y.\forall x.\left(\overline{P} \parr P\right)}}{\forall y.\forall x.\left(\exists x.\exists y.\overline{P} \parr P\right)}}{\exists x.\exists y.\overline{P} \parr \forall y.\forall x.P} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\circ}{\forall x.\forall y.\circ}}{\forall x.\forall y.\left(\overline{P} \parr P\right)}}{\forall x.\forall y.\left(\exists y.\overline{P} \parr \exists x.P\right)}}{\forall x.\exists y.\overline{P} \parr \forall y.\exists x.P} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\circ}{\forall x.\circ}}{\forall x.\left(\overline{P \parr Q} \parr P \parr Q\right)}}{\forall x.\left(\exists x.\left(\overline{P} \otimes \overline{Q}\right) \parr P \parr \exists x.Q\right)}}{\exists x.\left(\overline{P} \otimes \overline{Q}\right) \parr \forall x.P \parr \exists x.Q}$$

We desire analogous properties for the nominals И and Э. However, in contrast to first-order quantifiers, these properties must be induced for our pair of nominals. The first property is induced for И and Э by *equivariance* in the structural congruence. The other rules analogous to the above derived implications are induced by the rules: *new wen*, which allow a weaker quantifier Э to commute over a stronger quantifier И; and *close* which models that Э can select a name as long as it is fresh as indicated by И.

We avoid *new* distributing over ⅋, i.e., in general **neither** $\text{И}x.(P \parr Q) \multimap \text{И}x.P \parr \text{И}x.Q$ **nor** $\text{И}x.P \parr \text{И}x.Q \multimap \text{И}x.(P \parr Q)$ hold. Hence И is suitable for embedding the name binder ν of the π-calculus. Interestingly, the dual quantifier Э is also useful for embedding a variant of the π-calculus called the πI-calculus, where every communication creates a new fresh name. For example, πI-calculus process $\overline{v}[x].x[y] \mid v[z].\overline{z}[w]$ can be embedded as the following provable formula.[1]

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\text{И}x.\text{И}w.\circ}\;\text{by } \textit{tidy name}}{\text{И}x.\text{И}w.\left(\text{act}(x,w) \parr \overline{\text{act}(x,w)}\right)}\;\text{by } \textit{atomic interaction}}{\text{И}x.\left(\text{Э}y.\text{act}(x,y) \parr \text{И}w.\overline{\text{act}(x,w)}\right)}\;\text{by } \textit{close}}{\text{И}x.\left(\left(\overline{\text{act}(v,x)} \parr \text{act}(v,x)\right) \triangleleft \left(\text{Э}y.\text{act}(x,y) \parr \text{И}w.\overline{\text{act}(x,w)}\right)\right)}\;\text{by } \textit{atomic interaction}}{\text{И}x.\left(\left(\overline{\text{act}(v,x)} \triangleleft \text{Э}y.\text{act}(x,y)\right) \parr \left(\text{act}(v,x) \triangleleft \text{И}w.\overline{\text{act}(x,w)}\right)\right)}\;\text{by } \textit{sequence}}{\text{И}x.\left(\overline{\text{act}(v,x)} \triangleleft \text{Э}y.\text{act}(x,y)\right) \parr \text{Э}z.\left(\text{act}(v,z) \triangleleft \text{И}w.\overline{\text{act}(z,w)}\right)}\;\text{by } \textit{close} \text{ and } \alpha\text{-conversion}$$

Note that α-renaming is implicitly applied in the derivation above.

There is no *vacuous* rule in Fig. 2, in contrast to the presentation of BVQ in Fig. 1. This is because the *vacuous* rule creates problems for proof search, since arbitrarily many nominal quantifiers can be introduced at any point in the proof leading to unnecessary infinite search paths. Instead we build the introduction and elimination of fresh names into rules only where required. For example, *extrude new* is like *close* with a vacuous Э implicitly introduced; similarly, for *left wen*, *right wen*, *left name* and *right name* a vacuous Э is implicitly introduced. Also the *tidy name* allows vacuous И operators to be removed from a successful proof in order to terminate with ∘ only. The reason why the rules *medial new*, *suspend*, *all name* and *with name* are required are in order to make cut elimination work; hence we postpone their explanation until after the statement of the cut elimination result.

In addition to forbidding the *vacuous* rule, the following restrictions are placed on the rules to avoid meaningless infinite paths in proof search.

- For the *switch*, *sequence*, *medial1*, *medial new* and *extrude new* rules, $P \not\equiv \circ$ and $S \not\equiv \circ$.

[1] To disambiguate from the π-calculus we use square brackets as binders for the πI-calculus. So $\overline{v}[x].P$ denotes a process that outputs a fresh name x and $v[x].P$ denotes a process that receives a name x only if it is fresh.

- The *medial* rule is such that either $P \not\equiv \circ$ or $R \not\equiv \circ$ and also either $Q \not\equiv \circ$ or $S \not\equiv \circ$.
- The rules *external*, *extrude1*, *extrude new*, *left wen* and *right wen* are such that $R \not\equiv \circ$.

Avoiding infinite search paths is important for the termination of our cut elimination procedure. Essentially, we desire that our system for MAV1 is in a sense *analytic* [9].

Note on term "medial". Medials were introduced, historically, to make contraction local (reducing contraction to a rule acting only over atoms) [7]. Although the rules in Fig. 4 do not define such a local system, we discovered these rules by first defining a local system, and then designing a more controlled system retaining only the medials of the local system that are not admissible. Related work [54] shows that medials are a ubiquitous recipe underlying the rules of proof systems.

3.3 Cut elimination and its consequences

This section confirms that the rules of MAV1 indeed define a logical system, as established by a cut elimination theorem. Surprisingly, prior to this work, the only direct proof of cut elimination involving quantifiers in the calculus of structures was for BVQ [46]. Related cut elimination results involving first-order quantifiers in the calculus of structures relied on a correspondence with the sequent calculus [6, 50]. However, due to the presence of the non-commutative operator *seq* there is no sequent calculus presentation [53] for MAV1; hence we pursue here a direct proof.

The main result of this paper is the following, which is a generalisation of *cut elimination* to the setting of the calculus of structures.

Theorem 3.3 (Cut elimination). *For any formula P, if $\vdash C\left\{\, P \otimes \overline{P} \,\right\}$ holds, then $\vdash C\{\, \circ \,\}$ holds.*

The above theorem can be stated alternatively by supposing that there is a proof in MAV1 extended with the extra inference rule: $\dfrac{C\left\{\, P \otimes \overline{P} \,\right\}}{C\{\, \circ \,\}}\ (\text{cut})$. Given such a proof, a new proof can be constructed that uses only the rules of MAV1. In this formulation, we say that *cut* is *admissible*.

Cut elimination for the propositional sub-system MAV has been previously established [23]. The current paper advances cut-elimination techniques to tackle first-order system MAV1, as achieved by the lemmas in later sections. Before proceeding with the necessary lemmas, we provide a corollary that demonstrates that one of many consequences of cut elimination is indeed that linear implication defines a precongruence — a reflexive transitive relation that holds in any context.

Corollary 3.4. *Linear implication defines a precongruence.*

Proof. For transitivity, if $\vdash P \multimap Q$ and $\vdash Q \multimap R$ hold, we have the following.

$$\cfrac{\cfrac{\circ}{\left(\overline{P} \parr Q\right) \otimes \left(\overline{Q} \parr R\right)}\ \text{by the assumptions } \vdash \overline{P} \parr Q \text{ and } \vdash \overline{Q} \parr R}{\left(\overline{P} \parr \left(Q \otimes \overline{Q}\right) \parr R\right)}\ \text{by the } \textit{switch} \text{ rule}$$

Hence, by Theorem 3.3, $\vdash P \multimap R$ as required.

For contextual closure, if $\vdash P \multimap Q$ holds, we have the following.

$$\cfrac{\cfrac{\cfrac{\circ}{\overline{C\{\, P \,\}} \parr C\{\, P \,\}}\ \text{by Proposition 3.2}}{\overline{C\{\, P \,\}} \parr C\left\{\, P \otimes \left(\overline{P} \parr Q\right) \,\right\}}\ \text{by the assumption } \vdash P \multimap Q}{\overline{C\{\, P \,\}} \parr C\left\{\, \left(P \otimes \overline{P}\right) \parr Q \,\right\}}\ \text{by the } \textit{switch} \text{ rule}$$

Hence by Theorem 3.3, $\vdash C\{\, P \,\} \multimap C\{\, Q \,\}$ as required. Reflexivity holds by Proposition 3.2. □

3.4 Discussion on logical properties of the rules for nominal quantifiers

The rules for the nominal quantifiers *new* and *wen* require justification. The *close* and *tidy name* rules ensure the reflexivity of implication for nominal quantifiers. Using the *extrude new* rule (and Proposition 3.2) we can establish the following proof of $\vdash \text{Э}x.P \multimap \exists x.P$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\text{И}x.\circ}\;\text{by the \textit{tidy name} rule}}{\text{И}x.\left(P \parr \overline{P}\right)}\;\text{by Proposition 3.2}}{\text{И}x.\left(\exists x.P \parr \overline{P}\right)}\;\text{by the \textit{select1} rule}}{\exists x.P \parr \text{И}x.\overline{P}}\;\text{by the \textit{extrude new} rule}$$

The above also serves as a proof of the dual statement $\vdash \forall x.P \multimap \text{И}x.P$.

Using the *fresh* rule we can establish the following implication $\vdash \text{И}x.P \multimap \text{Э}x.P$, as follows.

$$\dfrac{\dfrac{\circ}{\text{И}x.\overline{P} \parr \text{Э}x.P}\;\text{by Proposition 3.2}}{\text{Э}x.\overline{P} \parr \text{Э}x.P}\;\text{by the \textit{fresh} rule}$$

This completes the chain $\vdash \forall x.P \multimap \text{И}x.P$, $\vdash \text{И}x.P \multimap \text{Э}x.P$ and $\vdash \text{Э}x.P \multimap \exists x.P$. These linear implications are strict unless $x \mathrel{\#} P$, in which case, for $\mho \in \{\forall, \exists, \text{И}, \text{Э}\}$, $\mho x.P$ is logically equivalent to P. For example, using the *fresh* rule followed by the *extrude new* and *tidy name* rules, $\vdash \text{И}x.P \multimap P$ holds, whenever $x \mathrel{\#} P$. Thus the implication corresponding to the *vacuous* rule as in Fig. 1 is provable for any quantifier.

The medial rules for nominals. The *medial new* rule is particular to handling nominals in the presence of the self-dual non-commutative operator *seq*. To see why this medial rule cannot be excluded, consider the following formulae, where x is free for atoms β, γ, ε and ζ.

$$\begin{aligned}(\alpha \lhd \text{Э}x.(\beta \lhd \gamma)) \otimes (\delta \lhd \text{Э}x.(\varepsilon \lhd \zeta)) &\multimap (\alpha \lhd \exists x.\beta \lhd \exists x.\gamma) \otimes (\delta \lhd \exists x.\varepsilon \lhd \exists x.\zeta)\\ (\alpha \lhd \exists x.\beta \lhd \exists x.\gamma) \otimes (\delta \lhd \exists x.\varepsilon \lhd \exists x.\zeta) &\multimap ((\alpha \lhd \exists x.\beta) \otimes (\delta \lhd \exists x.\varepsilon)) \lhd (\exists x.\gamma \otimes \exists x.\zeta)\end{aligned}$$

Without using the *medial new* rule, the above formulae are provable. The first is as follows.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\circ}{(\text{И}x.\circ) \otimes (\text{И}x.\circ)}\;\text{by \textit{tidy name}}}{\left((\overline{\alpha} \parr \alpha) \lhd \text{И}x.\left(\left(\overline{\beta \lhd \gamma}\right) \parr (\beta \lhd \gamma)\right)\right) \otimes \left(\left(\overline{\delta} \parr \delta\right) \lhd \text{И}x.\left(\overline{\varepsilon \lhd \zeta} \parr (\varepsilon \lhd \zeta)\right)\right)}\;\text{by Proposition 3.2}}{\left((\overline{\alpha} \parr \alpha) \lhd \text{И}x.\left(\left(\overline{\beta} \lhd \overline{\gamma}\right) \parr (\exists x.\beta \lhd \exists x.\gamma)\right)\right) \otimes \left(\left(\overline{\delta} \parr \delta\right) \lhd \text{И}x.\left(\left(\overline{\varepsilon} \lhd \overline{\zeta}\right) \parr (\exists x.\varepsilon \lhd \exists x.\zeta)\right)\right)}\;\textit{select1}}{\left((\overline{\alpha} \parr \alpha) \lhd \left(\text{И}x.\left(\overline{\beta} \lhd \overline{\gamma}\right) \parr (\exists x.\beta \lhd \exists x.\gamma)\right)\right) \otimes \left(\left(\overline{\delta} \parr \delta\right) \lhd \left(\text{И}x.\left(\overline{\varepsilon} \lhd \overline{\zeta}\right) \parr (\exists x.\varepsilon \lhd \exists x.\zeta)\right)\right)}\;\textit{extrude}}{\left(\left(\overline{\alpha} \lhd \text{И}x.\left(\overline{\beta} \lhd \overline{\gamma}\right)\right) \parr (\alpha \lhd \exists x.\beta \lhd \exists x.\gamma)\right) \otimes \left(\left(\overline{\delta} \lhd \text{И}x.\left(\overline{\varepsilon} \lhd \overline{\zeta}\right)\right) \parr (\delta \lhd \exists x.\varepsilon \lhd \exists x.\zeta)\right)}\;\textit{sequence}}{\left(\overline{\alpha} \lhd \text{И}x.\left(\overline{\beta} \lhd \overline{\gamma}\right)\right) \parr \left(\overline{\delta} \lhd \text{И}x.\left(\overline{\varepsilon} \lhd \overline{\zeta}\right)\right) \parr (\alpha \lhd \exists x.\beta \lhd \exists x.\gamma) \otimes (\delta \lhd \exists x.\varepsilon \lhd \exists x.\zeta)}\;\textit{switch}$$

The proof of the second formula above is as follows.

$$\dfrac{\dfrac{\dfrac{\circ}{\left(\overline{(\alpha \lhd \exists x.\beta) \otimes (\delta \lhd \exists x.\varepsilon)} \parr ((\alpha \lhd \exists x.\beta) \otimes (\delta \lhd \exists x.\varepsilon))\right) \lhd \left(\overline{\exists x.\gamma \otimes \exists x.\zeta} \parr (\exists x.\gamma \otimes \exists x.\zeta)\right)}\;\text{by Prop. 3.2}}{\left(\left(\overline{\alpha} \lhd \forall x.\overline{\beta}\right) \parr \left(\overline{\delta} \lhd \forall x.\overline{\varepsilon}\right)\right) \lhd \left(\forall x.\overline{\gamma} \parr \forall x.\overline{\zeta}\right) \parr ((\alpha \lhd \exists x.\beta) \otimes (\delta \lhd \exists x.\varepsilon)) \lhd (\exists x.\gamma \otimes \exists x.\zeta)}\;\text{by \textit{sequence}}}{\left(\overline{\alpha} \lhd \forall x.\overline{\beta} \lhd \forall x.\overline{\gamma}\right) \parr \left(\overline{\delta} \lhd \forall x.\overline{\varepsilon} \lhd \forall x.\overline{\zeta}\right) \parr ((\alpha \lhd \exists x.\beta) \otimes (\delta \lhd \exists x.\varepsilon)) \lhd (\exists x.\gamma \otimes \exists x.\zeta)}\;\text{by \textit{sequence}}$$

However, the issue is that the following formula would not be provable without using the *medial new* rule; hence cut elimination cannot hold without the *medial new* rule.

$$(\alpha \triangleleft \text{Э}x.(\beta \triangleleft \gamma)) \otimes (\delta \triangleleft \text{Э}x.(\varepsilon \triangleleft \zeta)) \multimap ((\alpha \triangleleft \exists x.\beta) \otimes (\delta \triangleleft \exists x.\varepsilon)) \triangleleft (\exists x.\gamma \otimes \exists x.\zeta)$$

In contrast, with the *medial new* rule the above formula is provable, as verified by the proof in Figure 5. Notice the above proofs use only the *medial new*, *extrude new* and *tidy name* rules for nominals. These rules are of the same form as rules *medial1*, *extrude1* and *tidy1* for universal quantifiers, hence the same argument holds for the necessity of the *medial1* rule by replacing И with ∀.

$$\begin{array}{c}
\circ \\ \hline
(\text{И}x.\circ \otimes \text{И}x.\circ) \triangleleft (\text{И}x.\circ \otimes \text{И}x.\circ) \\ \hline
\left(\left((\overline{\alpha} \parr \alpha) \triangleleft \text{И}x.\left(\overline{\beta} \parr \beta\right)\right) \otimes \left(\left(\overline{\delta} \parr \delta\right) \triangleleft \text{И}x.(\overline{\varepsilon} \parr \varepsilon)\right)\right) \triangleleft \left(\text{И}x.(\overline{\gamma} \parr \gamma) \otimes \text{И}x.\left(\overline{\zeta} \parr \zeta\right)\right) \\ \hline
\left(\left((\overline{\alpha} \parr \alpha) \triangleleft \text{И}x.\left(\overline{\beta} \parr \exists x.\beta\right)\right) \otimes \left(\left(\overline{\delta} \parr \delta\right) \triangleleft \text{И}x.(\overline{\varepsilon} \parr \exists x.\varepsilon)\right)\right) \triangleleft \left(\text{И}x.(\overline{\gamma} \parr \exists x.\gamma) \otimes \text{И}x.\left(\overline{\zeta} \parr \exists x.\zeta\right)\right) \\ \hline
\left(\left((\overline{\alpha} \parr \alpha) \triangleleft \left(\text{И}x.\overline{\beta} \parr \exists x.\beta\right)\right) \otimes \left(\left(\overline{\delta} \parr \delta\right) \triangleleft (\text{И}x.\overline{\varepsilon} \parr \exists x.\varepsilon)\right)\right) \triangleleft \left((\text{И}x.\overline{\gamma} \parr \exists x.\gamma) \otimes \left(\text{И}x.\overline{\zeta} \parr \exists x.\zeta\right)\right) \\ \hline
\left(\left(\left(\overline{\alpha} \triangleleft \text{И}x.\overline{\beta}\right) \parr (\alpha \triangleleft \exists x.\beta)\right) \otimes \left(\left(\overline{\delta} \triangleleft \text{И}x.\overline{\varepsilon}\right) \parr (\delta \triangleleft \exists x.\varepsilon)\right)\right) \triangleleft \left((\text{И}x.\overline{\gamma} \parr \exists x.\gamma) \otimes \left(\text{И}x.\overline{\zeta} \parr \exists x.\zeta\right)\right) \\ \hline
\left(\left(\overline{\alpha} \triangleleft \text{И}x.\overline{\beta}\right) \parr \left(\overline{\delta} \triangleleft \text{И}x.\overline{\varepsilon}\right) \parr ((\alpha \triangleleft \exists x.\beta) \otimes (\delta \triangleleft \exists x.\varepsilon))\right) \triangleleft \left(\text{И}x.\overline{\gamma} \parr \text{И}x.\overline{\zeta} \parr (\exists x.\gamma \otimes \exists x.\zeta)\right) \\ \hline
\left(\left(\overline{\alpha} \triangleleft \text{И}x.\overline{\beta}\right) \parr \left(\overline{\delta} \triangleleft \text{И}x.\overline{\varepsilon}\right)\right) \triangleleft \left(\text{И}x.\overline{\gamma} \parr \text{И}x.\overline{\zeta}\right) \parr ((\alpha \triangleleft \exists x.\beta) \otimes (\delta \triangleleft \exists x.\varepsilon)) \triangleleft (\exists x.\gamma \otimes \exists x.\zeta) \\ \hline
\left(\overline{\alpha} \triangleleft \text{И}x.\overline{\beta} \triangleleft \text{И}x.\overline{\gamma}\right) \parr \left(\overline{\delta} \triangleleft \text{И}x.\overline{\varepsilon} \triangleleft \text{И}x.\overline{\zeta}\right) \parr ((\alpha \triangleleft \exists x.\beta) \otimes (\delta \triangleleft \exists x.\varepsilon)) \triangleleft (\exists x.\gamma \otimes \exists x.\zeta) \\ \hline
\left(\overline{\alpha} \triangleleft \text{И}x.\left(\overline{\beta} \triangleleft \overline{\gamma}\right)\right) \parr \left(\overline{\delta} \triangleleft \text{И}x.\left(\overline{\varepsilon} \triangleleft \overline{\zeta}\right)\right) \parr ((\alpha \triangleleft \exists x.\beta) \otimes (\delta \triangleleft \exists x.\varepsilon)) \triangleleft (\exists x.\gamma \otimes \exists x.\zeta)
\end{array}$$

Fig. 5. A proof of $(\alpha \triangleleft \text{Э}x.(\beta \triangleleft \gamma)) \otimes (\delta \triangleleft \text{Э}x.(\varepsilon \triangleleft \zeta)) \multimap ((\alpha \triangleleft \exists x.\beta) \otimes (\delta \triangleleft \exists x.\varepsilon)) \triangleleft (\exists x.\gamma \otimes \exists x.\zeta)$

Including the *medial new* rule forces the *suspend* rule to be included. To see why, observe that the following linear implications are provable.

$$\begin{array}{c}
(\text{И}x.\alpha \triangleleft \text{И}x.\beta) \otimes (\text{И}x.\gamma \triangleleft \text{И}x.\delta) \multimap \text{И}x.(\alpha \triangleleft \beta) \otimes \text{И}x.(\gamma \triangleleft \delta) \\
\text{И}x.(\alpha \triangleleft \beta) \otimes \text{И}x.(\gamma \triangleleft \delta) \multimap \text{И}x.((\alpha \triangleleft \beta) \otimes (\gamma \triangleleft \delta))
\end{array}$$

However, without the *suspend* rule the following implication is not provable, which would contradict the cut elimination result of this paper.

$$(\text{И}x.\alpha \triangleleft \text{И}x.\beta) \otimes (\text{И}x.\gamma \triangleleft \text{И}x.\delta) \multimap \text{И}x.((\alpha \triangleleft \beta) \otimes (\gamma \triangleleft \delta))$$

Fortunately, including the *suspend* rule ensures that the above implication is provable as follows.

$$\begin{array}{cl}
\circ & \\ \hline
\text{Э}x.\left(\left(\overline{\alpha} \triangleleft \overline{\beta}\right) \parr \left(\overline{\gamma} \triangleleft \overline{\delta}\right)\right) \parr \text{И}x.((\alpha \triangleleft \beta) \otimes (\gamma \triangleleft \delta)) & \text{by Proposition 3.2} \\ \hline
\text{Э}x.\left(\overline{\alpha} \triangleleft \overline{\beta}\right) \parr \text{Э}x.\left(\overline{\gamma} \triangleleft \overline{\delta}\right) \parr \text{И}x.((\alpha \triangleleft \beta) \otimes (\gamma \triangleleft \delta)) & \text{by } \textit{suspend} \\ \hline
\left(\text{Э}x.\overline{\alpha} \triangleleft \text{Э}x.\overline{\beta}\right) \parr \left(\text{Э}x.\overline{\gamma} \triangleleft \text{Э}x.\overline{\delta}\right) \parr \text{И}x.((\alpha \triangleleft \beta) \otimes (\gamma \triangleleft \delta)) & \text{by } \textit{suspend}
\end{array}$$

A similar argument justifies the inclusion of the *left wen* and *right wen* rules.

Rules induced by equivariance. Interestingly, *equivariance* is a design decision in the sense that cut elimination still holds if we drop the *equivariance* rule from the structural congruence. For such a system without *equivariance*, also the rules *all name*, *with name*, *left name* and *right name* could also be dropped. Perhaps there may be interesting applications for a non-equivariant nominal quantifiers; however, for embedding of process such as ν in the π-calculus, *equivariance* is an essential property for scope extrusion. For example, *equivariance* is used when proving the embedding of labelled transition $\nu x.\nu y.\overline{z}y.p \xrightarrow{\overline{z}(y)} \nu x.p$, assuming $z \neq x$ and $z \neq y$.

In our embedding of the π-calculus in MAV1, addressed thoroughly in a companion paper [26], we assume process p is embedded as formula P. In this case, process $\nu x.\nu y.\overline{z}y.p$ maps to $Q = \text{И}x.\text{И}y.\left(\overline{\mathrm{act}(z,y)} \triangleleft P\right)$, process $\nu x.p$ maps to $R = \text{И}x.P$. In this embedding of processes as formulae, we can prove that whenever the above labelled transition is enabled, we can prove the following implication $\text{И}y.\left(\overline{\mathrm{act}(z,y)} \triangleleft R\right) \multimap Q$, where the binder $\text{И}y$ and atom $\mathrm{act}(z,y)$ indicate that the process can commit to a bound output. Indeed this formula is provable, as follows, by using *equivariance*.

$$
\begin{array}{cl}
\circ & \\
\hline
\text{И}y.\text{И}x.\circ & \text{by } \textit{tidy name} \\
\hline
\text{И}y.\left(\text{И}x.\left(\mathrm{act}(z,y) \parr \overline{\mathrm{act}(z,y)}\right) \triangleleft \left(\overline{\text{И}x.P} \parr \text{И}x.P\right)\right) & \text{by Proposition 3.2} \\
\hline
\text{И}y.\left(\left(\mathrm{act}(z,y) \parr \text{И}x.\overline{\mathrm{act}(z,y)}\right) \triangleleft \left(\text{Э}x.\overline{P} \parr \text{И}x.P\right)\right) & \text{by } \textit{extrude new} \\
\hline
\text{И}y.\left(\left(\mathrm{act}(z,y) \triangleleft \text{Э}x.\overline{P}\right) \parr \left(\text{И}x.\overline{\mathrm{act}(z,y)} \triangleleft \text{И}x.P\right)\right) & \text{by } \textit{sequence} \\
\hline
\text{И}y.\left(\left(\mathrm{act}(z,y) \triangleleft \text{Э}x.\overline{P}\right) \parr \text{И}x.\left(\overline{\mathrm{act}(z,y)} \triangleleft P\right)\right) & \text{by } \textit{medial new} \\
\hline
\text{Э}y.\left(\mathrm{act}(z,y) \triangleleft \text{Э}x.\overline{P}\right) \parr \text{И}y.\text{И}x.\left(\overline{\mathrm{act}(z,y)} \triangleleft P\right) & \text{by } \textit{close} \\
\hline
\text{Э}y.\left(\mathrm{act}(z,y) \triangleleft \text{Э}x.\overline{P}\right) \parr \text{И}x.\text{И}y.\left(\overline{\mathrm{act}(z,y)} \triangleleft P\right) & \text{by } \textit{equivariance}
\end{array}
$$

In response to the above problem, modelling the π-calculus, MAV1 includes equivariance.

The *equivariance* rule forces additional distributivity properties for И and Э over & and ∀, given by the *all name*, *with name*, *left name*, *right name* rules. These rules allow И and Э quantifiers to propagate to the front of certain contexts. To see why these rules are necessary consider the following implications, with matching formulae, respectively, after and before the implication.

$$\vdash \text{И}x.(\text{И}y.\forall z.\alpha \parr \text{Э}y.(\beta \mathbin{\&} \gamma)) \multimap \text{И}x.\text{И}y.\forall z.\alpha \parr \text{Э}x.\text{Э}y.(\beta \mathbin{\&} \gamma)$$

$$\vdash \text{И}x.\text{И}y.\forall z.\alpha \parr \text{Э}x.\text{Э}y.(\beta \mathbin{\&} \gamma) \multimap \text{И}y.\forall z.\text{И}x.\alpha \parr \text{Э}y.(\text{Э}x.\beta \mathbin{\&} \text{Э}x.\gamma)$$

Any proof of the second implication does involve *equivariance*; but neither proof requires *all name* or *with name*. A proof of the first implication above is as follows.

$$
\begin{array}{cl}
\circ & \\
\hline
\text{Э}x.\left(\text{Э}y.\exists z.\overline{\alpha} \otimes \text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right)\right) \parr \text{И}x.(\text{И}y.\forall z.\alpha \parr \text{Э}y.(\beta \mathbin{\&} \gamma)) & \text{by Proposition 3.2} \\
\hline
\text{Э}x.\left(\text{Э}y.\exists z.\overline{\alpha} \otimes \text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right)\right) \parr \text{И}x.\text{И}y.\forall z.\alpha \parr \text{Э}x.\text{Э}y.(\beta \mathbin{\&} \gamma) & \text{by } \textit{close}
\end{array}
$$

A proof of the second implication above is given in Figure 6.

By the implications above, if cut elimination holds, it must be the case that the following is provable.

$$\text{И}x.(\text{И}y.\forall z.\alpha \parr \text{Э}y.(\beta \mathbin{\&} \gamma)) \multimap \text{И}y.\forall z.\text{И}x.\alpha \parr \text{Э}y.(\text{Э}x.\beta \mathbin{\&} \text{Э}x.\gamma)$$

$$
\begin{array}{cl}
\circ & \\ \hline
\text{И}y.\forall z.\text{И}x.\circ \otimes \text{И}y.(\text{И}x.\circ \with \text{И}x.\circ) & \text{by \textit{tidy name} and \textit{tidy1}} \\ \hline
\text{И}y.\forall z.\text{И}x.(\overline{\alpha} \parr \alpha) \otimes \text{И}y.\left(\text{И}x.\left(\overline{\beta} \parr \beta\right) \with \text{И}x.(\overline{\gamma} \parr \gamma)\right) & \text{by \textit{atomic interaction}} \\ \hline
\text{И}y.\forall z.\text{И}x.(\overline{\alpha} \parr \alpha) \otimes \text{И}y.\left(\text{И}x.\left(\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \beta\right) \with \text{И}x.\left(\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \gamma\right)\right) & \text{by \textit{left} and \textit{right}} \\ \hline
\text{И}y.\forall z.\text{И}x.(\overline{\alpha} \parr \alpha) \otimes \text{И}y.\left(\left(\text{И}x.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \text{Э}x.\beta\right) \with \left(\text{И}x.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \text{Э}x.\gamma\right)\right) & \text{by \textit{close}} \\ \hline
\text{И}y.\forall z.\text{И}x.(\overline{\alpha} \parr \alpha) \otimes \text{И}y.\left(\text{И}x.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr (\text{Э}x.\beta \with \text{Э}x.\gamma)\right) & \text{by \textit{external}} \\ \hline
\text{И}y.\forall z.\text{И}x.(\overline{\alpha} \parr \alpha) \otimes \left(\text{И}x.\text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma)\right) & \text{by \textit{equivariance} and \textit{close}} \\ \hline
\text{И}y.\forall z.\text{И}x.(\exists z.\overline{\alpha} \parr \alpha) \otimes \left(\text{И}x.\text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma)\right) & \text{by \textit{select1}} \\ \hline
\text{И}y.\forall z.(\text{Э}x.\exists z.\overline{\alpha} \parr \text{И}x.\alpha) \otimes \left(\text{И}x.\text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma)\right) & \text{by \textit{close}} \\ \hline
\text{И}y.(\text{Э}x.\exists z.\overline{\alpha} \parr \forall z.\text{И}x.\alpha) \otimes \left(\text{И}x.\text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma)\right) & \text{by \textit{extrude1}} \\ \hline
(\text{Э}x.\text{Э}y.\exists z.\overline{\alpha} \parr \text{И}y.\forall z.\text{И}x.\alpha) \otimes \left(\text{И}x.\text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right) \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma)\right) & \text{by \textit{equivariance} and \textit{close}} \\ \hline
\left(\text{Э}x.\text{Э}y.\exists z.\overline{\alpha} \otimes \text{И}x.\text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right)\right) \parr \text{И}y.\forall z.\text{И}x.\alpha \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma) & \text{by \textit{switch}}
\end{array}
$$

Fig. 6. A proof of $\text{И}x.\text{И}y.\forall z.\alpha \parr \text{Э}x.\text{Э}y.(\beta \with \gamma) \multimap \text{И}y.\forall z.\text{И}x.\alpha \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma)$

However, without the *all name* and *with name* rules, the above implication is not provable and hence cut elimination would not hold in the presence of *equivariance*. Fortunately, using both the *all name* and *with name* rules the above implication is provable, as follows.

$$
\begin{array}{cl}
\circ & \\ \hline
\text{Э}x.\left(\text{Э}y.\exists z.\overline{\alpha} \otimes \text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right)\right) \parr \text{И}x.(\text{И}y.\forall z.\alpha \parr \text{Э}y.(\beta \with \gamma)) & \text{by Proposition 3.2} \\ \hline
\text{Э}x.\left(\text{Э}y.\exists z.\overline{\alpha} \otimes \text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right)\right) \parr \text{И}x.\text{И}y.\forall z.\alpha \parr \text{Э}x.\text{Э}y.(\beta \with \gamma) & \text{by \textit{close}} \\ \hline
\text{Э}x.\left(\text{Э}y.\exists z.\overline{\alpha} \otimes \text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right)\right) \parr \text{И}x.\text{И}y.\forall z.\alpha \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma) & \text{\textit{with name} and \textit{equivariance}} \\ \hline
\text{Э}x.\left(\text{Э}y.\exists z.\overline{\alpha} \otimes \text{И}y.\left(\overline{\beta} \oplus \overline{\gamma}\right)\right) \parr \text{И}y.\forall z.\text{И}x.\alpha \parr \text{Э}y.(\text{Э}x.\beta \with \text{Э}x.\gamma) & \text{\textit{all name} and \textit{equivariance}}
\end{array}
$$

A similar argument justifies the necessity of the *left name* and *right name* rules.

Polarities of the nominals. As with focussed proof search [2, 12], assigning a positive or negative polarity to operators explains certain distributivity properties. Consider $\parr$, $\with$, $\forall$ and И to be negative operators, and $\otimes$, $\oplus$, $\exists$ and Э to be positive operators, where *seq* is both positive and negative. The negative quantifier И distributes over all positive operators. Considering positive operator *tensor* for example, $\vdash \text{И}x.\alpha \otimes \text{И}x.\beta \multimap \text{И}x.\,(\alpha \otimes \beta)$ holds but the converse implication does not hold. Furthermore, $\text{Э}x.\alpha \otimes \text{Э}x.\beta$ and $\text{Э}x.\,(\alpha \otimes \beta)$ are unrelated by linear implication in general. Dually, for the negative operator *par* the only distributivity property that holds for nominal quantifiers is $\vdash \text{Э}x.\,(\alpha \parr \beta) \multimap \text{Э}x.\alpha \parr \text{Э}x.\beta$. The *new wen* rule completes this picture of *new* distributing over positive operators and *wen* distributing over negative operators. From the perspective of embedding name-passing process calculi in logic, the above distributivity properties of *new* and *wen* suggest that processes should be encoded using negative operators И and ⅋ for private names and parallel composition (or perhaps dually, using positive operators Э and ⊗), so as to avoid private names distributing over parallel composition, which we have shown to be problematic in Section 2.

The control of distributivity exercised by *new* and *wen* contrasts with the situation for universal and existential quantifiers, where ∃ commutes in one direction over all operators and ∀ commutes with all operators in the opposite direction, similarly to the additive ⊕ and & which are also insensitive to the polarity of operators with which they commute. In the sense of control of distributivity [4], *new* and *wen* behave more like multiplicatives than additives, but are unrelated to multiplicative quantifiers in the logic of bunched implications [42].

4 THE SPLITTING TECHNIQUE FOR RENORMALISING PROOFS

This section presents the *splitting* technique that is central to the cut elimination proof for MAV1. Splitting is used to recover a syntax directed approach for sequent-like contexts. Recall that in the sequent calculus rules are always applied to the root connective of a formula in a sequent, whereas deep inference rules can be applied deep within any context. The technique is used to guide proof normalisation leading to the cut elimination result at the end of Section 5.

There are complex inter-dependencies between the nominals *new* and *wen* and other operators, particularly the multiplicatives *times* and *seq* and additive *with*. As such, the splitting proof is tackled as follows, as illustrated in Fig. 7:

- Splitting for the first-order universal quantifier ∀ can be treated independently of the other operators; hence a direct proof of splitting for this operator is provided first as a simple induction over the length of a derivation in Lemma 4.2. Splitting for all other operators are dependent on this lemma.
- Due to inter-dependencies between И, Э, ⊗, ◁ and &, splitting for these operators are proven simultaneously by a (huge) mutual induction in Lemma 4.19. The induction is guided by an intricately designed multiset-based measure of the size of a proof in Definition 4.15. The balance of dependencies between operators in this lemma is, by far, the most challenging aspect of this paper.
- Having established Lemma 4.2 and Lemma 4.19, splitting for the remaining operators ∃ and ⊕ and the atoms can each be established independently of each other in Lemmas 4.20, 4.21 and 4.22 respectively.

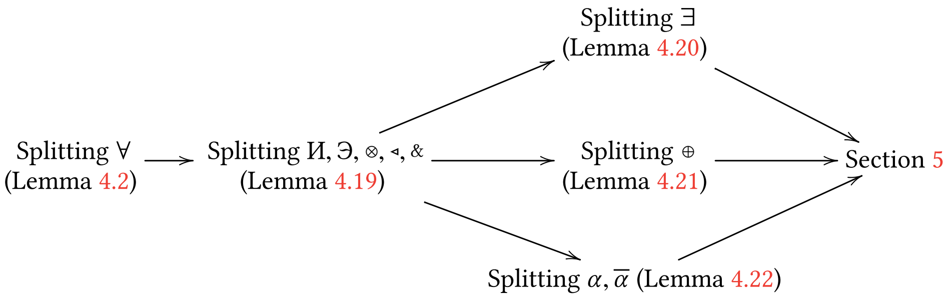

Fig. 7. The proof strategy: dependencies between splitting lemmas leading to cut elimination.

4.1 Elimination of universal quantifiers from a proof

We employ a trick where universal quantification $\forall$ receives a more direct treatment than other operators. The proof requires closure of rules under substitution of terms for variables, established as follows directly by induction over the length of a derivation using a function over formulae.

Lemma 4.1 (Substitution). *If we have derivation* $\dfrac{P}{Q}$*, then we have derivation* $\dfrac{P\{{}^{v}\!/_{x}\}}{Q\{{}^{v}\!/_{x}\}}$.

We can now establish, the following lemma directly, which is a *co-rule* elimination lemma. By a co-rule, we mean that, for *select* rule $\dfrac{C\{\ P\{{}^{v}\!/_{x}\}\ \}}{C\{\ \exists x.P\ \}}$, there is complementary rule $\dfrac{C\{\ \forall x.P\ \}}{C\{\ P\{{}^{v}\!/_{x}\}\ \}}$ where the direction of inference is reversed and the formulae are complemented. Such a co-rule can always be eliminated from a proof, in which case we say *co-select1* is *admissible*, as established by the following lemma.

Lemma 4.2 (Universal). *If* $\vdash C\{\ \forall x.P\ \}$ *holds then, for all terms* v*,* $\vdash C\{\ P\{{}^{v}\!/_{x}\}\ \}$ *holds.*

A corollary of Lemma 4.2 is: if $\vdash \forall x.P \parr Q$ then $\vdash P\{{}^{y}\!/_{x}\} \parr Q$, where $y \mathrel{\#} (\forall x.P \parr Q)$. This corollary is in the form of a *splitting* lemma, where we have a principal connective $\forall$ at the root of a formula inside a context of the form $\{\ \cdot\ \} \parr Q$. This corollary of the above lemma should remind the reader of the (invertible) sequent calculus rule for universal quantifiers:

$$\frac{\vdash P\{{}^{y}\!/_{x}\}, \Gamma}{\vdash \forall x.P, \Gamma} \text{ where } y \text{ is fresh for } \forall x.P \text{ and all formulae in } \Gamma$$

We discuss, the significance of splitting lemmas after some preliminary lemmas required for the main splitting result.

4.2 Killing contexts and technical lemmas required for splitting

We require a restricted form of context called a killing context (terminology is from [12]). A killing context is a context with one or more holes, defined as follows.

Definition 4.3. A *killing context* is a context defined by the following grammar.

$$\mathcal{K}\{\ \ \} ::= \{\ \cdot\ \} \mid \mathcal{K}\{\ \ \} \mathbin{\&} \mathcal{K}\{\ \ \} \mid \forall x.\mathcal{K}\{\ \ \} \mid \text{И}x.\mathcal{K}\{\ \ \}$$

In the above, $\{\ \cdot\ \}$ is a hole into which any formula can be plugged. An n-ary killing context is a killing context in which n holes appear.

For readability of large formulae involving an n-ary killing context, for $n > 1$, we represent the holes using a comma-separated list, so for example, instead of writing $\mathcal{K}\{\cdot\}\{\cdot\}$, we write $\mathcal{K}\{\ \cdot, \cdot\ \}$ for a binary context. Given an n-ary killing context $\mathcal{K}\{\ \ldots\ \}$, we write $\mathcal{K}\{\ Q_1, \ldots, Q_n\ \}$ to denote the formula obtained by filling the holes in the context with formulas $Q_1, \ldots, Q_n$. We also introduce the notation $\mathcal{K}\{\ Q_i \colon 1 \leq i \leq n\ \}$ as shorthand for $\mathcal{K}\{\ Q_1, Q_2, \ldots, Q_n\ \}$; and $\mathcal{K}\{\ Q_i \colon i \in I\ \}$ for a family of formulae indexed by finite subset of natural numbers I.

A killing context represents a context that cannot in general be removed until all other rules in a proof have been applied, hence the corresponding *tidy* rules are suspended until the end of a proof. A killing context has properties that are applied frequently in proofs, characterised by the following lemma.

Lemma 4.4. *For any killing context* $\mathcal{K}\{\ \ \}$*,* $\vdash \mathcal{K}\{\ \circ, \ldots, \circ\ \}$ *holds; and, assuming the free variables of* P *are not bound by* $\mathcal{K}\{\ \ \}$*, we have derivation*

$$\frac{\mathcal{K}\{\ P \parr Q_1, P \parr Q_2, \ldots P \parr Q_n\ \}}{P \parr \mathcal{K}\{\ Q_1, Q_2, \ldots Q_n\ \}} \ .$$

Killing contexts also satisfy the following property that is necessary for handling the *seq* operator, which interacts subtly with killing contexts.

Lemma 4.5. *Assume that I is a finite subset of natural numbers, P_i and Q_i are formulae, for $i \in I$, and $\mathcal{K}\{\ \}$ is a killing context. There exist killing contexts $\mathcal{K}^0\{\ \}$ and $\mathcal{K}^1\{\ \}$ and sets of natural numbers $J \subseteq I$ and $K \subseteq I$ such that the following derivation holds:*

$$\frac{\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \lhd \mathcal{K}^1\{\ Q_k : k \in K\ \}}{\mathcal{K}\{\ P_i \lhd Q_i : i \in I\ \}}\ .$$

The following lemma checks that *wen* quantifiers can propagate to the front of a killing context. Similarly, to the proof of the lemma above, the proof is by induction on the structure of a killing context, applying the *all name*, *new wen*, *with name*, *left name* or *right name* rule, as appropriate.

Lemma 4.6. *Consider an n-ary killing context $\mathcal{K}\{\ \}$ and formulae such that $x \mathrel{\#} P_i$ and either $P_i = \text{Э}x.Q_i$ or $P_i = Q_i$, for $1 \leq i \leq n$. If for some i such that $1 \leq i \leq n$, $P_i = \text{Э}x.Q_i$, then we have derivation $\dfrac{\text{Э}x.\mathcal{K}\{\ Q_1, Q_2, \ldots, Q_n\ \}}{\mathcal{K}\{\ P_1, P_2, \ldots P_n\ \}}$.*

To handle certain cases in splitting the following definitions and property is helpful. Assume $\vec{y}$ defines a possibly empty list of variables $y_1, y_2, \ldots, y_n$ and $\text{Ꝺ}\vec{y}.P$ abbreviates $\text{Ꝺ}y_1.\text{Ꝺ}y_2.\ldots\text{Ꝺ}y_n.P$. Let $\vec{y} \mathrel{\#} P$ hold only if $y \mathrel{\#} P$ for every $y \in \vec{y}$. By induction over the length of $\vec{z}$ we can establish the following lemma, by repeatedly applying the *close*, *fresh* and *extrude new* rules.

Lemma 4.7. *If $\vec{y} \subseteq \vec{z}$ and $\vec{z} \mathrel{\#} \text{Э}\vec{y}.P$, then we have derivations $\dfrac{\text{И}\vec{z}.(P \parr Q)}{\text{Э}\vec{y}.P \parr \text{И}\vec{z}.Q}$ and $\dfrac{\text{И}\vec{z}.(P \parr Q)}{\text{И}\vec{y}.P \parr \text{Э}\vec{z}.Q}$.*

4.3 An Affine Measure for the Size of a Proof.

As an induction measure in the splitting lemmas, we employ a multiset-based measure [14] of the size of a proof. An *occurrence count* is defined in terms of a multiset of multisets. To give weight to nominals, a *wen* and *new* count is employed. The measure of the size of a proof, Definition 4.15, is then given by the lexicographical order induced by the occurrence count, wen count and new count for the formula in the conclusion of a proof, and the derivation length of the proof itself.

In the sub-system BV [21], the occurrence count is simply the number of atom and co-atom occurrences. For the sub-system corresponding to MALL (multiplicative-additive linear logic) [48], i.e. without *seq*, a multiset of atom occurrences such that $|(P \mathbin{\&} Q) \parr R|_{occ} = |(P \parr R) \mathbin{\&} (Q \parr R)|_{occ}$ is sufficient, to ensure that the *external* rule does not increase the size of the measure. The reason why a multiset of multisets is employed for extensions of MAV [23] is to handle subtle interactions between the unit, *seq* and *with* operators. In particular, by applying the structural rules for units, such that $C\{\ P \mathbin{\&} Q\ \} \equiv C\{\ (P \lhd \circ) \mathbin{\&} (\circ \lhd Q)\ \}$ and the *medial* rule, we obtain the following inference.

$$\frac{C\{\ (P \mathbin{\&} \circ) \lhd (\circ \mathbin{\&} Q)\ \}}{C\{\ P \mathbin{\&} Q\ \}}\ \text{by the } \textit{medial} \text{ rule}$$

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

Definition 4.8. We denote the standard multiset disjoint union operator as $\uplus$, a multiset sum operator defined such that $M + N = \{m + n\colon m \in M \text{ and } n \in N\}$. We also define pointwise plus and pointwise union over multisets of multisets of natural numbers, where $\mathcal{M}$ and $\mathcal{N}$ are multisets of multisets. $\mathcal{M} \boxplus \mathcal{N} = \{M + N, M \in \mathcal{M} \text{ and } N \in \mathcal{N}\}$ and $\mathcal{M} \sqcup \mathcal{N} = \{M \uplus N, M \in \mathcal{M} \text{ and } N \in \mathcal{N}\}$.

We employ two distinct multiset orderings over multisets and over multisets of multisets.

Definition 4.9. For multisets of natural numbers M and N, define a multiset ordering $M \leq N$ if and only if there exists an injective multiset function $f\colon M \longrightarrow N$ such that, for all $m \in M$, $m \leq f(m)$. Strict multiset ordering $M < N$ is defined such that $M \leq N$ but $M \neq N$.

Definition 4.10. Given two multisets of multisets of natural numbers $\mathcal{M}$ 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 $M_i < N$. $\mathcal{M} \sqsubset \mathcal{N}$ is defined when $\mathcal{M} \sqsubseteq \mathcal{N}$ but $\mathcal{M} \neq \mathcal{N}$.

Definition 4.11. The occurrence count is the following function from formulae to multiset of multisets of natural numbers.

$$|\circ|_{occ} = \{\{0\}\} \qquad |\alpha|_{occ} = |\overline{\alpha}|_{occ} = \{\{1\}\} \qquad |\text{И}x.P|_{occ} = |\text{Э}x.P|_{occ} = \begin{cases} \{\{0,0\}\} & \text{if } P \equiv \circ \\ |P|_{occ} & \text{otherwise} \end{cases}$$

$$|P \mathbin{\&} Q|_{occ} = |P \oplus Q|_{occ} = |P|_{occ} \sqcup |Q|_{occ}$$

$$|P \parr Q|_{occ} = |P|_{occ} \boxplus |Q|_{occ} \qquad |P \otimes Q|_{occ} = |P \mathbin{\triangleleft} Q|_{occ} = \begin{cases} |P|_{occ} & \text{if } Q \equiv \circ \\ |Q|_{occ} & \text{if } P \equiv \circ \\ |P|_{occ} \uplus |Q|_{occ} & \text{otherwise} \end{cases}$$

$$|\forall x.P|_{occ} = |\exists x.P|_{occ} = \{\{0\}\} \sqcup |P|_{occ}$$

Definition 4.12. The wen count is the following function from formulae to natural numbers.

$$|\text{Э}x.P|_{\text{э}} = 1 + |P|_{\text{э}} \qquad |\exists x.P|_{\text{э}} = |\forall x.P|_{\text{э}} = |\text{И}x.P|_{\text{э}} = |P|_{\text{э}} \qquad |\alpha|_{\text{э}} = |\overline{\alpha}|_{\text{э}} = |\circ|_{\text{э}} = 1$$

$$|P \mathbin{\triangleleft} Q|_{\text{э}} = |P \otimes Q|_{\text{э}} = |P \parr Q|_{\text{э}} = |P|_{\text{э}}|Q|_{\text{э}} \qquad |P \oplus Q|_{\text{э}} = |P \mathbin{\&} Q|_{\text{э}} = |P|_{\text{э}} + |Q|_{\text{э}}$$

Definition 4.13. The new count is the following function from formulae to natural numbers.

$$|\text{И}x.P|_{\text{и}} = 1 + |P|_{\text{и}} \qquad |\exists x.P|_{\text{и}} = |\forall x.P|_{\text{и}} = |\text{Э}x.P|_{\text{и}} = |P|_{\text{и}} \qquad |\alpha|_{\text{и}} = |\overline{\alpha}|_{\text{и}} = |\circ|_{\text{и}} = 1$$

$$|P \parr Q|_{\text{и}} = |P|_{\text{и}}|Q|_{\text{и}} \quad |P \oplus Q|_{\text{и}} = |P \mathbin{\&} Q|_{\text{и}} = |P|_{\text{и}} + |Q|_{\text{и}} \quad |P \mathbin{\triangleleft} Q|_{\text{и}} = |P \otimes Q|_{\text{и}} = \max\bigl(|P|_{\text{и}}, |Q|_{\text{и}}\bigr)$$

Definition 4.14. The size of a formula $|P|$ is defined as the triple $(|P|_{occ}, |P|_{\text{э}}, |P|_{\text{и}})$ lexicographically ordered by $\prec$. $\phi \preceq \psi$ is defined such that $\phi \prec \psi$ or $\phi = \psi$ pointwise.

Definition 4.15. The size of a proof of P with derivation of length n is given by the tuple of the form $(|P|\,, n)$, subject to lexicographical ordering.

Lemma 4.16. *For any formula P and term t, $|P| = \left|P\left\{{}^{t}\!/\!_{x}\right\}\right|$.*

Lemma 4.17. *If $P \equiv Q$ then $|P| = |Q|$.*

The following lemma we will appeal to regularly in the splitting proofs in subsequent sections to bound the size of a derivation.

Lemma 4.18 (affine). *Any derivation $\dfrac{P}{Q}$, is bound such that $|P| \preceq |Q|$.*

4.4 The splitting technique for simulating sequent-like rules

The technique called splitting [21, 22] generalises the application of rules in the sequent calculus. In the sequent calculus, any root connective in a sequent can be selected and some rule for that connective can be applied. For example, consider the following rules in linear logic forming part of a proof in the sequent calculus, where $x \mathrel{\#} P, Q, U, V, W$.

$$\dfrac{\dfrac{\dfrac{\vdash P, U \qquad \vdash Q, R}{\vdash P \otimes Q, R, U} \qquad \dfrac{\dfrac{\vdash P, R, V \qquad \vdash Q, W}{\vdash P \otimes Q, R, V, W}}{\vdash P \otimes Q, R, V \parr W}}{\vdash P \otimes Q, R, U \mathbin{\&} (V \parr W)}}{\vdash P \otimes Q, \forall x.R, U \mathbin{\&} (V \parr W)}$$

In the setting of the calculus of structures, the sequent at the conclusion of the above proof corresponds to a *shallow context* of the form $\{\ \cdot\ \} \parr \forall x.R \parr (U \with (V \parr W))$ where the *times* operator at the root of $P \otimes Q$ is a *principal formula* that is plugged into the shallow context. Splitting proves that there is always a derivation reorganising a shallow context into a form such that a rule for the root connective of the principal formula may be applied. In the above example, this would correspond to the following derivation over contexts:

$$\dfrac{\dfrac{\{\ \cdot\ \} \parr \forall x.((R \parr U) \with (R \parr V \parr W))}{\{\ \cdot\ \} \parr \forall x.(R \parr (U \with (V \parr W)))}\ \text{by the } \textit{external} \text{ rule}}{\{\ \cdot\ \} \parr \forall x.R \parr (U \with (V \parr W))}\ \text{by the } \textit{extrude1} \text{ rule}$$

By plugging in the principal formula, $P \otimes Q$, into the hole in the premise of the above derivation and applying distributivity properties of a killing context (Lemma 4.4), the *switch* rule involving the principal connective can be applied as follows.

$$\dfrac{\dfrac{\forall x.(((P \parr U) \otimes (Q \parr R)) \with ((P \parr R \parr V) \otimes (Q \parr W)))}{\forall x.(((P \otimes Q) \parr R \parr U) \with ((P \otimes Q) \parr R \parr V \parr W))}\ \text{by the } \textit{switch} \text{ rule}}{(P \otimes Q) \parr \forall x.((R \parr U) \with (R \parr V \parr W))}\ \text{by Lemma 4.4}$$

Notice that the final formula above holds when all of the following hold: $\vdash P \parr U$, $\vdash Q \parr R$, $\vdash P \parr R \parr V$ and $\vdash Q \parr W$. Notice that these correspond to the leaves of the example sequent above.

Splitting is sufficiently general that the technique can be applied to operators such as *seq* that have no sequent calculus presentation [53]. The technique also extends to the pair of nominals *new* and *wen*, for which a sequent calculus presentation is an open problem.

The operators *times*, *seq*, *new* and *wen* are treated together in Lemma 4.19. These operators give rise to *commutative cases*, where rules for these operators can permute with any principal formula, swapping the order of rules in a proof. *Principal cases* are where the root connective of the principal formula is directly involved in the bottommost rule of a proof. As with MAV [23], the *principal cases* for *seq* are challenging, demanding Lemma 4.5. The principal case induced by *medial new* demands Lemma 4.6. The cases where two nominal quantifiers commute are also interesting, particularly where the case arrises due to *equivariance*.

Lemma 4.19 (Core Splitting). *The following statements hold.*

1. *If $\vdash (P \otimes Q) \parr R$, then there exist formulae V_i and W_i such that $\vdash P \parr V_i$ and $\vdash Q \parr W_i$, where $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\ V_1 \parr W_1, V_2 \parr W_2, \ldots, V_n \parr W_n\ \}}{R}$ and if $\mathcal{K}\{\ \}$ binds x then $x \# (P \otimes Q)$.*
2. *If $\vdash (P \lhd Q) \parr R$, then there exist formulae V_i and W_i such that $\vdash P \parr V_i$ and $\vdash Q \parr W_i$, where $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\ V_1 \lhd W_1, V_2 \lhd W_2, \ldots, V_n \lhd W_n\ \}}{R}$ and if $\mathcal{K}\{\ \}$ binds x then $x \# (P \lhd Q)$.*
3. *If $\vdash \text{И}x.P \parr Q$, then there exist formulae V and W where $x \# V$ and $\vdash P \parr W$ and either $V = W$ or $V = \text{Э}x.W$, such that there is a derivation $\dfrac{V}{Q}$.*
4. *If $\vdash \text{Э}x.P \parr Q$, then there exist formulae V and W where $x \# V$ and $\vdash P \parr W$ and either $V = W$ or $V = \text{И}x.W$, such that there is a derivation $\dfrac{V}{Q}$.*
5. *If $\vdash (P \with Q) \parr R$, then $\vdash P \parr R$ and $\vdash Q \parr R$.*

Furthermore, for all $1 \leq i \leq n$, in the first two cases the size of the proofs of $P \parr V_i$ and $Q \parr W_i$ are strictly bounded above by the size of the proofs of $(P \otimes Q) \parr R$ and $(P \lhd Q) \parr R$. In the third and fourth *cases, the size of the proof* $P \parr W$ *is strictly bounded above by the size of the proofs of* $\text{И}x.P \parr Q$ *and* $\text{Э}x.P \parr Q$. *The size of a proof is measured according to Definition 4.15.*

Proof. The proof proceeds by induction on the size of the proof, as in Defn. 4.15. In each of the following base cases, the conditions for splitting are immediately satisfied. For the base case for the *tidy name* rule, the bottommost rule of a proof is of the form $\dfrac{\text{И}\vec{y}.\circ \parr P}{\text{И}x.\text{И}\vec{y}.\circ \parr P}$, where $\vec{y} \# P$. For the base case for the *tidy* rule, the bottommost rule is of the form $\dfrac{\circ \parr P}{(\circ \& \circ) \parr P}$, such that $\vdash \circ \parr P$. For the base case for *times* and *seq*, $\vdash (\circ \otimes \circ) \parr \circ$ and $\vdash (\circ \triangleleft \circ) \parr \circ$ hold.

A Principal cases for wen. There are principal cases for *wen* where the rules *close*, *suspend*, *left wen*, *right wen* and *fresh* interfere directly with *wen* at the root of a principal formula. Three representative cases are presented.

A.1 The first principal case for *wen* is when the bottommost rule of a proof is an instance of the *close* rule of the form $\dfrac{\text{И}x.(P \parr Q) \parr R}{\text{Э}x.P \parr \text{И}x.Q \parr R}$, where $\vdash \text{И}x.(P \parr Q) \parr R$ and $x \# R$. By the induction hypothesis, there exist S and T such that $\vdash P \parr Q \parr T$ and $x \# S$ and either $S = T$ or $S = \text{Э}x.T$, and also we have derivation $\dfrac{S}{R}$. Since $x \# S$, if $S = T$ then $\dfrac{\text{И}x.(Q \parr T)}{\text{И}x.Q \parr S}$. Furthermore, the size of the proof of $P \parr Q \parr T$ is no larger than the size of the proof of $\text{И}x.(P \parr Q) \parr R$; hence strictly bounded by the size of the proof of $\text{Э}x.P \parr \text{И}x.Q \parr R$. If $S = \text{Э}x.T$ then by the *close* rule $\dfrac{\text{И}x.(Q \parr T)}{\text{И}x.Q \parr \text{Э}x.T}$. If $S = T$ then, since $x \# S$, by the *extrude new* rule, $\dfrac{\text{И}x.(Q \parr T)}{\text{И}x.Q \parr T}$. Hence in either case $\dfrac{\text{И}x.(Q \parr T)}{\text{И}x.Q \parr S}$ and thereby the derivation $\dfrac{\dfrac{\text{И}x.(Q \parr T)}{\text{И}x.Q \parr S}}{\text{И}x.Q \parr R}$ can be constructed, meeting the conditions for splitting for *wen.*

A.2 Consider the second principal case for *wen* where the bottommost rule of a proof is an instance of the *suspend* rule of the form $\dfrac{\text{Э}x.(P \parr Q) \parr R}{\text{Э}x.P \parr \text{Э}x.Q \parr R}$, where $\vdash \text{Э}x.(P \parr Q) \parr R$ and $x \# R$. By the induction hypothesis, there exist S and T such that and $\vdash P \parr Q \parr T$ and $x \# S$ and either $S = T$ or $S = \text{И}x.T$, and also $\dfrac{S}{R}$. Furthermore, the size of the proof of $P \parr Q \parr T$ is no larger than the size of the proof of $\text{Э}x.(P \parr Q) \parr R$; hence strictly bounded by the size of the proof of $\text{Э}x.P \parr \text{Э}x.Q \parr R$. Since $x \# S$, if $S = T$ then, by the *new wen* and *extrude new* rules, $\dfrac{\dfrac{\text{И}x.(Q \parr T)}{\text{И}x.Q \parr T}}{\text{Э}x.Q \parr T}$. If $S = \text{И}x.T$ then, by the *close* rule, $\dfrac{\text{И}x.(Q \parr T)}{\text{Э}x.Q \parr \text{И}x.T}$. So in either case, $\dfrac{\text{И}x.(Q \parr T)}{\text{Э}x.Q \parr S}$, and hence the derivation $\dfrac{\dfrac{\text{И}x.(Q \parr T)}{\text{Э}x.Q \parr S}}{\text{Э}x.Q \parr R}$ can be constructed, as required. The principal cases for *left wen* and *right wen* are similar.

A.3 Consider the principal case for *wen* when the bottommost rule of a proof is an instance of the *fresh* rule of the form $\dfrac{\text{Э}\vec{y}.\text{И}x.P \parr Q}{\text{Э}x.\text{Э}\vec{y}.P \parr Q}$, where $\vdash \text{Э}\vec{y}.\text{И}x.P \parr Q$. Notice that $\vec{y}$ is required to handle the effect of *equivariance*. By applying the induction hypothesis inductively on the length of $\vec{y}$, there exist $\vec{z}$ and $\hat{Q}$ such that $\vec{z} \subseteq \vec{y}$ and $\vec{y} \# \text{И}\vec{z}\hat{Q}$ and $\vdash \text{И}x.P \parr \hat{Q}$, and also $\dfrac{\text{И}\vec{z}.\hat{Q}}{Q}$. Furthermore, the size of the proof of $\text{И}x.P \parr \hat{Q}$ is bounded above by the size of the proof of $\text{Э}\vec{y}.\text{И}x.P \parr Q$. By the induction hypothesis, there exist R and S such that $x \mathrel{\#} R$, $\vdash P \parr S$ and either $R = S$ or $R = \text{Э}x.S$, and also $\dfrac{R}{\hat{Q}}$. There are two cases to consider. If $R = S$ then let $T = \text{И}\vec{z}.S$; and if $R = \text{Э}x.S$ then let $T = \text{И}x.\text{И}\vec{z}.S$, in which case, since $\text{И}\vec{z}.\text{И}x.S \equiv \text{И}x.\text{И}\vec{z}.S$ we have $\dfrac{T}{\text{И}\vec{z}.R}$. In either case $x \mathrel{\#} T$. Thereby we can construct the derivation $\dfrac{\dfrac{\dfrac{T}{\text{И}\vec{z}.R}}{\text{И}\vec{z}.\hat{Q}}}{Q}$. Furthermore, appealing to Lemma 4.7, the proof $\dfrac{\dfrac{\dfrac{}{\circ}}{\text{И}\vec{y}.\circ}}{\dfrac{\text{И}\vec{y}.(P \parr S)}{\text{Э}\vec{y}.P \parr \text{И}\vec{z}.S}}$ can be constructed and, furthermore, $|\text{Э}\vec{y}.P \parr \text{И}\vec{z}.S| \prec |\text{Э}x.\text{Э}\vec{y}.P \parr Q|$, since by Lemma 4.18 $|\text{И}\vec{z}.S| \leq |Q|$ and the *wen* count strictly decreases.

B Principal cases for new. The principal cases for *new* are where the rules *close*, *extrude new*, *medial new* and *new wen* rules interfere directly with the *new* quantifier at the root of the principal formula. Three cases are presented.

B.1 The first principal case for *new* is when the bottommost rule of a proof is an instance of the *close* rules of the form $\dfrac{\text{И}x.(P \parr Q) \parr R}{\text{И}x.P \parr \text{Э}x.Q \parr R}$, where $\vdash \text{И}x.(P \parr Q) \parr R$. By the induction hypothesis, there exist formulae U and V such that $\vdash P \parr Q \parr V$ and $x \mathrel{\#} U$ and either $U = V$ or $U = \text{Э}x.V$, and also we have derivation $\dfrac{U}{R}$. Furthermore, the size of the proof of $P \parr Q \parr V$ is no larger than the size of the proof of $\text{И}x.(P \parr Q) \parr R$; hence strictly bounded by the size of the proof of $\text{И}x.P \parr \text{Э}x.Q \parr R$. In the case $U = V$, we have $\dfrac{\text{Э}x.(Q \parr V)}{\text{Э}x.Q \parr V}$, since $x \mathrel{\#} U$. In the case $U = \text{Э}x.V$, we have $\dfrac{\text{Э}x.(Q \parr V)}{\text{Э}x.Q \parr \text{Э}x.V}$. Hence, by applying one of the above cases the following derivation $\dfrac{\dfrac{\text{Э}x.(Q \parr V)}{\text{Э}x.Q \parr U}}{\text{Э}x.Q \parr R}$ can be constructed as required. The principal case where the bottommost rule in a proof is the *extrude new* rule follows a similar pattern.

B.2 Consider the second principal case for *new* where the *medial new* rule is the bottommost rule of a proof of the form

$$\dfrac{\text{И}\vec{y}.(\text{И}x.P \triangleleft \text{И}x.Q) \parr R}{\text{И}x.\text{И}\vec{y}.(P \triangleleft Q) \parr R} \quad \text{such that } \vdash \text{И}\vec{y}.(\text{И}x.P \triangleleft \text{И}x.Q) \parr R.$$

The $\vec{y}$ is required to handle cases induced by equivariance. By applying the induction hypothesis repeatedly, there exists $\vec{z}$ and $\hat{R}$ such that $\vec{z} \subseteq \vec{y}$ and $\vec{y} \mathrel{\#} \text{Э}\vec{z}.\hat{R}$ and $\vdash (\text{И}x.P \triangleleft \text{И}x.Q) \parr \hat{R}$, and also $\dfrac{\hat{R}}{R}$. Furthermore, the size of the proof of $(\text{И}x.P \triangleleft \text{И}x.Q) \parr \hat{R}$ is bounded above by the size of the proof of $\text{И}\vec{y}.(\text{И}x.P \triangleleft \text{И}x.Q) \parr R$. By the induction hypothesis, there exist S_i and T_i such that $\vdash \text{И}x.P \parr S_i$ and $\vdash \text{И}x.Q \parr T_i$, for $1 \leq i \leq n$, and n-ary killing context such that $\dfrac{\mathcal{K}\{\, S_1 \triangleleft T_1, S_2 \triangleleft T_2, \ldots, S_n \triangleleft T_n \,\}}{\hat{R}}$. Furthermore, the size of the proofs of $\text{И}x.P \parr S_i$ and $\text{И}x.Q \parr T_i$ are bounded above by the size of the proof of $(\text{И}x.P \triangleleft \text{И}x.Q) \parr R$. By the induction hypothesis again, there exist U^i and $\hat{U}^i$ such that $\vdash P \parr \hat{U}^i$ and $x \mathrel{\#} U^i$ and either $U^i = \hat{U}^i$ or $U^i = \text{Э}x.\hat{U}^i$, and also $\dfrac{U^i}{S_i}$. Also by the induction hypothesis, there exist V^i and $\hat{V}^i$ such that $\vdash Q \parr \hat{V}^i$ and $x \mathrel{\#} V^i$ and either $V^i = \hat{V}^i$ or $V^i = \text{Э}x.\hat{V}^i$, and also $\dfrac{V^i}{T_i}$. Now define W and $\hat{W}$ such that $\hat{W} = \text{Э}\vec{z}.\mathcal{K}\left\{\, \hat{U}^i \triangleleft \hat{V}^i : 1 \leq i \leq n \,\right\}$ and, if for all $1 \leq i \leq n$,

$U^i = \hat{U}^i$ and $V^i = \hat{V}^i$, then $W = \hat{W}$; otherwise $W = \text{Э}x.\hat{W}$. Hence for each i, one of the following derivations holds.

- $U^i = \hat{U}^i$ and $V^i = \hat{V}^i$ hence $U^i \triangleleft V^i = \hat{U}^i \triangleleft \hat{V}^i$.
- If $U^i = \text{Э}x.\hat{U}^i$ and $V^i = \hat{V}^i$, hence $x \# V^i$, by the *left wen* rule $\dfrac{\text{Э}x.\left(\hat{U}^i \triangleleft \hat{V}^i\right)}{\text{Э}x.\hat{U}^i \triangleleft \hat{V}^i}$.
- If $U^i = \hat{U}^i$, hence $x \# \hat{U}^i$, and $V^i = \text{Э}x.\hat{V}^i$, by the *right wen* rule $\dfrac{\text{Э}x.\left(\hat{U}^i \triangleleft \hat{V}^i\right)}{U^i \triangleleft \text{Э}x.\hat{V}^i}$.
- Otherwise by the *suspend* rule $\dfrac{\text{Э}x.\left(\hat{U}^i \triangleleft \hat{V}^i\right)}{\text{Э}x.\hat{U}^i \triangleleft \text{Э}x.\hat{V}^i}$

If for all i such that $1 \leq i \leq n$, $U^i = \hat{U}^i$ and $V^i = \hat{V}^i$ then $W = \hat{W}$. Otherwise, by Lemma 4.6, $\dfrac{\text{Э}\vec{z}.\text{Э}x.\mathcal{K}\left\{\, \hat{U}^i \triangleleft \hat{V}^i : 1 \leq i \leq n \,\right\}}{\text{Э}\vec{z}.\mathcal{K}\left\{\, U^i \triangleleft V^i : 1 \leq i \leq n \,\right\}}$, where the premise is equialent to W. Thereby the derivation below left can be constructed, and furthermore, using Lemma 4.7, the proof below right can also be constructed.

$$\cfrac{\cfrac{\cfrac{\cfrac{W}{\text{Э}\vec{z}.\mathcal{K}\left\{\, U^i \triangleleft V^i : 1 \leq i \leq n \,\right\}}}{\text{Э}\vec{z}.\mathcal{K}\{\, S_i \triangleleft T_i : 1 \leq i \leq n \,\}}}{\text{Э}\vec{z}.\hat{R}}}{R} \qquad \cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\circ}{\text{И}\vec{y}.\mathcal{K}\{\, \circ : 1 \leq i \leq n \,\}}}{\text{И}\vec{y}.\mathcal{K}\left\{\, \left(P \parr \hat{U}^i\right) \triangleleft \left(Q \parr \hat{V}^i\right) : 1 \leq i \leq n \,\right\}}}{\text{И}\vec{y}.\mathcal{K}\left\{\, (P \triangleleft Q) \parr \left(\hat{U}^i \triangleleft \hat{V}^i\right) : 1 \leq i \leq n \,\right\}}}{\text{И}\vec{y}.\left((P \triangleleft Q) \parr \mathcal{K}\left\{\, \hat{U}^i \triangleleft \hat{V}^i : 1 \leq i \leq n \,\right\}\right)}}{\text{И}\vec{y}.(P \triangleleft Q) \parr \hat{W}}$$

By Lemma 4.18, $\left|\hat{W}\right| \leq |R|$; hence $\left|\text{И}\vec{y}.(P \triangleleft Q) \parr \hat{W}\right| \prec |\text{И}x.\text{И}\vec{y}.(P \triangleleft Q) \parr R|$ since the *new count* strictly decreases, as required.

B.3 Consider the third principal case for *new* where the bottommost rule of a proof is the *new wen* rule of the form

$$\frac{\text{И}\vec{z}.\text{Э}y.\text{И}x.P \parr Q}{\text{И}x.\text{И}\vec{z}.\text{Э}y.P \parr Q} \text{ , where } \vdash \text{И}\vec{z}.\text{Э}y.\text{И}x.P \parr Q.$$

By applying the induction hypothesis repeatedly, there exist $\vec{w}$ and $\hat{Q}$ such that $\vec{w} \subseteq \vec{z}$ and $\vec{z} \# \text{Э}\vec{w}.\hat{Q}$ and $\vdash \text{Э}y.\text{И}x.P \parr \hat{Q}$, and also $\dfrac{\text{Э}\vec{w}.\hat{Q}}{Q}$. Furthermore, the size of the proof of $\text{Э}y.\text{И}x.P \parr \hat{Q}$ is bounded above by the size of the proof of $\text{И}\vec{z}.\text{Э}y.\text{И}x.P \parr Q$. By the induction hypothesis, there exist R and S such that $x \# R$ and $\vdash \text{И}x.P \parr S$ and either $R = S$ or $R = \text{И}y.S$, and also $\dfrac{R}{\hat{Q}}$. Furthermore, the size of the proof of $\text{И}x.P \parr S$ is bounded above by the size of the proof of $\text{Э}y.\text{И}x.P \parr Q$, hence strictly bounded above by the size of the proof of $\text{И}x.\text{Э}y.P \parr Q$ enabling the induction hypothesis. By the induction hypothesis again, there exist U and V such that $x \# U$ and $\vdash P \parr V$ and either $U = V$ or $U = \text{Э}x.V$, and also $\dfrac{U}{S}$. Let W and $\hat{W}$ be defined such that, if $R = \text{И}y.S$, then $\hat{W} = \text{И}y.V$; or, if $R = S$, then $\hat{W} = V$. If $V = U$ then define $W = \text{Э}\vec{w}.\hat{W}$. If $U = \text{Э}x.V$, then define $W = \text{Э}x.\text{Э}\vec{w}.\hat{W}$. There are four scenarios for constructing a derivation with premise W and conclusion $\text{Э}\vec{w}.R$.

- In the case $V = U$ and $R = \text{И}y.S$ then $\text{Э}\vec{w}.\text{И}y.U = W$.

- If $V = U$ and $R = S$ then $Э\vec{w}.U = W$.
- If both $U = Эx.V$ and $R = Иy.S$ hold, then we have

$$\begin{array}{c} Эx.Э\vec{w}.Иy.V \\ \hline Э\vec{w}.Иy.Эx.V \\ \hline Э\vec{w}.R \end{array}\text{, where the premise is } W.$$

- If both $U = Эx.V$ and $R = S$ then $\dfrac{Э\vec{w}.U}{Э\vec{w}.R}$, where the premise is equivalent to W.

Thereby, by applying one of the above cases, we have $\begin{array}{c} W \\ \hline Э\vec{w}.R \\ \hline Э\vec{w}.Q \\ \hline \hat{Q} \end{array}$.

In the case that $\hat{W} = Иy.V$, the left most derivation below holds. In the case, $\hat{W} = V$ and $y \# V$ the middle derivation below holds. Hence in either case, appealing to Lemma 4.7, the proof below right can be constructed:

$$\begin{array}{c} Иy.(P ⅋ V) \\ \hline Эy.P ⅋ Иy.V \end{array} \qquad \begin{array}{c} Иy.(P ⅋ V) \\ \hline Эy.(P ⅋ V) \\ \hline Эy.P ⅋ \hat{W} \end{array} \qquad \begin{array}{c} \circ \\ \hline И\vec{z}.Иy.\circ \\ \hline И\vec{z}.Иy.(P ⅋ V) \\ \hline И\vec{z}.\left(Эy.P ⅋ \hat{W}\right) \\ \hline И\vec{z}.Эy.P ⅋ Э\vec{w}.\hat{W} \end{array}$$

Furthermore, by Lemma 4.18, $\left|Э\vec{w}.\hat{W}\right| \leq |Q|$. Hence $\left|Эy.P ⅋ Э\vec{w}.\hat{W}\right| \prec |Иx.И\vec{z}.Эy.P ⅋ Q|$ since the *new* count strictly decreases.

C Principal cases for seq. There are two forms of principal cases for *seq*. The first case, induced by the *sequence* rule, is the case that forces the *medial*, *medial1* and *medial new* rules. The other cases are induced by the *suspend*, *left wen* and *right wen* rules (which are forced as a knock on effect of the *medial new* rule).

C.1 Consider the first principal case for *seq*. The difficulty in this case is that, due to associativity of *seq*, the *sequence* rule may be applied in several ways when there are multiple occurrences of *seq*. Consider a principal formula of the form $(T_0 \triangleleft T_1) \triangleleft T_2$, where we aim to split the formula around the second *seq* operator. The difficulty is that the bottommost rule may be an instance of the *sequence* rule applied between T_0 and $T_1 \triangleleft T_2$. Symmetrically, the principal formula may be of the form $T_0 \triangleleft (T_1 \triangleleft T_2)$ but the bottommost rule may be an instance of the *sequence* rule applied between $T_0 \triangleleft T_1$ and T_2. In the following analysis, only the former case is considered; the symmetric case follows a similar pattern. The principal formula is $(T_0 \triangleleft T_1) \triangleleft T_2$ and the bottommost rule is an instance of the *sequence* rule of the form

$$\dfrac{((T_0 ⅋ U) \triangleleft ((T_1 \triangleleft T_2) ⅋ V)) ⅋ W}{(T_0 \triangleleft T_1 \triangleleft T_2) ⅋ (U \triangleleft V) ⅋ W}$$

where $T_0 \not\equiv \circ$, $T_2 \not\equiv \circ$ (otherwise splitting is trivial), and either $U \not\equiv \circ$ or $V \not\equiv \circ$ (otherwise the *sequence* rule cannot be applied); and also $\vdash ((T_0 ⅋ U) \triangleleft ((T_1 \triangleleft T_2) ⅋ V)) ⅋ W$. By the induction hypothesis, there exist P_i and Q_i such that $\vdash T_0 ⅋ U ⅋ P_i$ and $\vdash (T_1 \triangleleft T_2) ⅋ V ⅋ Q_i$ hold, for $1 \leq i \leq n$, and an n-ary killing context $\mathcal{K}\{\ \}$ such that

$$\dfrac{\mathcal{K}\{\, P_1 \triangleleft Q_1, \ldots, P_n \triangleleft Q_n \,\}}{W} \ .$$

Furthermore, the size of the proof of formula $(T_1 \triangleleft T_2) \parr V \parr Q_i$ is bounded above by the size of the proof of $((T_0 \parr U) \triangleleft ((T_1 \triangleleft T_2) \parr V)) \parr W$, hence the induction hypothesis is enabled. By the induction hypothesis, there exists R^i_j and S^i_j such that $\vdash T_1 \parr R^i_j$ and $\vdash T_2 \parr S^i_j$, for $1 \leq j \leq m_i$, and m_i-ary killing context $\mathcal{K}^i\{\ \}$ such that

$$\frac{\mathcal{K}^i\{\, R^i_1 \triangleleft S^i_1, \ldots, R^i_{m_i} \triangleleft S^i_{m_i} \,\}}{V \parr Q_i} \,.$$

Furthermore, by Lemma 4.5 there exist killing contexts $\mathcal{K}^i_0\{\ \}$ and $\mathcal{K}^i_1\{\ \}$ and sets of integers $J^i \subseteq \{1, \ldots, n\}$, $K^i \subseteq \{1, \ldots, n\}$ such that

$$\frac{\mathcal{K}^i_0\left\{\, R^i_j \colon j \in J^i \,\right\} \triangleleft \mathcal{K}^i_1\{\, S^i_k \colon k \in K^i \,\}}{\mathcal{K}^i\{\, R^i_1 \triangleleft S^i_1, \ldots, R^i_{m_i} \triangleleft S^i_{m_i} \,\}} \,.$$

Thereby, the following derivation can be constructed.

$$\begin{array}{c}
\mathcal{K}\left\{\, (U \parr P_i) \triangleleft \mathcal{K}^i_0\left\{\, R^i_j \colon j \in J^i \,\right\} \triangleleft \mathcal{K}^i_1\{\, S^i_k \colon k \in K^i \,\} \,:\, 1 \leq i \leq n \,\right\} \\
\hline
\mathcal{K}\left\{\, (U \parr P_i) \triangleleft \mathcal{K}^i\left\{\, R^i_j \triangleleft S^i_j \colon 1 \leq j \leq m_i \,\right\} \,:\, 1 \leq i \leq n \,\right\} \\
\hline
\mathcal{K}\{\, (U \parr P_1) \triangleleft (V \parr Q_1), \ldots, (U \parr P_n) \triangleleft (V \parr Q_n) \,\} \\
\hline
\mathcal{K}\{\, (U \triangleleft V) \parr (P_1 \triangleleft Q_1), \ldots, (U \triangleleft V) \parr (P_n \triangleleft Q_n) \,\} \\
\hline
(U \triangleleft V) \parr \mathcal{K}\{\, P_1 \triangleleft Q_1, \ldots, P_n \triangleleft Q_n \,\} \\
\hline
(U \triangleleft V) \parr W
\end{array}$$

Furthermore, the following two proofs can be constructed.

$$\begin{array}{c}
\circ \\
\hline
\mathcal{K}^i\{\, \circ \colon 1 \leq j \leq m_i \,\} \\
\hline
\mathcal{K}^i\left\{\, T_2 \parr S^i_j \colon 1 \leq j \leq m_i \,\right\} \\
\hline
T_2 \parr \mathcal{K}^i\left\{\, S^i_j \colon 1 \leq j \leq m_i \,\right\}
\end{array}
\qquad
\begin{array}{c}
\circ \\
\hline
\mathcal{K}^i\{\, \circ \colon 1 \leq j \leq m_i \,\} \\
\hline
\mathcal{K}^i\left\{\, T_1 \parr R^i_j \colon 1 \leq j \leq m_i \,\right\} \\
\hline
T_1 \parr \mathcal{K}^i\left\{\, R^i_j \colon 1 \leq j \leq m_i \,\right\} \\
\hline
(T_0 \parr U \parr P_i) \triangleleft \left(T_1 \parr \mathcal{K}^i\left\{\, R^i_j \colon 1 \leq j \leq m_i \,\right\}\right) \\
\hline
(T_0 \triangleleft T_1) \parr \left((U \parr P_i) \triangleleft \mathcal{K}^i\left\{\, R^i_j \colon 1 \leq j \leq m_i \,\right\}\right)
\end{array}$$

By Lemma 4.18,

$$\left|\mathcal{K}\{\, (U \parr P_1) \triangleleft \mathcal{K}^i_0\{\, R^i_j \colon j \in J^i \,\} \triangleleft \mathcal{K}^i_1\{\, S^i_k \colon k \in K^i \,\} \,:\, 1 \leq i \leq n \,\}\right| \leq |(U \triangleleft V) \parr W|$$

which are also upper bounds for $\left|\mathcal{K}^i_0\left\{\, R^i_j \colon j \in J^i \,\right\}\right|$ and $\left|\mathcal{K}^i_1\{\, S^i_k \colon k \in K^i \,\}\right|$. Furthermore, $T_0 \not\equiv \circ$ and $T_2 \not\equiv \circ$ both $|T_0|_{occ} \sqsubset |T_0 \triangleleft T_1 \triangleleft T_2|_{occ}$ and $|T_2|_{occ} \sqsubset |T_0 \triangleleft T_1 \triangleleft T_2|_{occ}$ Hence the sizes of the above proofs of $T_2 \parr \mathcal{K}^i\left\{\, S^i_j \colon 1 \leq j \leq m_i \,\right\}$ and

$$(T_0 \triangleleft T_1) \parr \left((U \parr P_i) \triangleleft \mathcal{K}^i\{\, R^i_j \colon 1 \leq j \leq m_i \,\}\right)$$

are strictly less than the size of the proof of $(T_0 \triangleleft T_1 \triangleleft T_2) \parr (U \triangleleft V) \parr W$.

C.2 Consider the principal case for *seq* where the bottommost rule of a proof is an instance of the *suspend* rule of the form

$$\frac{(P_0 \triangleleft \exists x.(P_1 \triangleleft P_2) \triangleleft P_3) \parr Q}{(P_0 \triangleleft \exists x.P_1 \triangleleft \exists x.P_2 \triangleleft P_3) \parr Q}\ \text{, where} \vdash (P_0 \triangleleft \exists x.(P_1 \triangleleft P_2) \triangleleft P_3) \parr Q \text{ holds.}$$

By induction, there exist U_i^0 and U_i^1 such that $\vdash P_0 \parr U_i^0$ and $\vdash (\exists x.(P_1 \triangleleft P_2) \triangleleft P_3) \parr U_i^1$ hold, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\, U_i^0 \triangleleft U_i^1 : 1 \leq i \leq n \,\}}{Q}$. Furthermore the size of the proof of $(\exists x.(P_1 \triangleleft P_2) \triangleleft P_3) \parr U_i^1$ is bounded above by the size of the proof of $(P_0 \triangleleft \exists x.P_1 \triangleleft \exists x.P_2 \triangleleft P_3) \parr Q$. By induction again, there exist V_j^i and W_j^i such that $\vdash \exists x.(P_1 \triangleleft P_2) \parr V_j^i$ and $\vdash P_3 \parr W_j^i$, for $1 \leq j \leq m_i$, and m_i-ary killing context $\mathcal{K}^i\{\ \}$ such that the following derivation holds. $\dfrac{\mathcal{K}^i\left\{\, V_j^i \triangleleft W_j^i : 1 \leq j \leq m_i \,\right\}}{U_i^1}$. Furthermore, the size of the proof of $\exists x.(P_1 \triangleleft P_2) \parr V_j^i$ is bounded by the size of the proof of $(\exists x.(P_1 \triangleleft P_2) \triangleleft P_3) \parr U_i^1$. By applying the induction hypothesis again, there exist R_j^i and $\hat{R}_j^i$ such that $x \mathrel{\#} R_j^i$ and $\vdash (P_1 \triangleleft P_2) \parr \hat{R}_j^i$ and either $R_j^i = \hat{R}_j^i$ or $R_j^i = \text{И}x.\hat{R}_j^i$, and also $\dfrac{R_j^i}{V_j^i}$. Furthermore, the size of the proof of $(P_1 \triangleleft P_2) \parr \hat{R}_j^i$ is bounded above by the size of the proof of $(\exists x.(P_1 \triangleleft P_2) \triangleleft P_3) \parr U_i^1$. By a fourth induction, there exist $S_k^{i,j}$ and $T_k^{i,j}$ such that both $\vdash P_1 \parr S_k^{i,j}$ and $\vdash P_2 \parr T_k^{i,j}$ hold, for $1 \leq k \leq \ell^{i,j}$, and $\ell^{i,j}$-ary killing context $\mathcal{K}^{i,j}\{\ \}$ such that the following derivation holds:

$$\frac{\mathcal{K}^{i,j}\left\{\, S_1^{i,j} \triangleleft T_1^{i,j}, S_2^{i,j} \triangleleft T_2^{i,j}, \ldots, S_{\ell^{i,j}}^{i,j} \triangleleft T_{\ell^{i,j}}^{i,j} \,\right\}}{\hat{R}_j^i}\ .$$

By Lemma 4.5, there exists some $I_j^i \subseteq \left\{1 \ldots \ell^{i,j}\right\}$ and $J_j^i \subseteq \left\{1 \ldots \ell^{i,j}\right\}$ and killing contexts $\mathcal{K}_0^{i,j}\{\ \}$ and $\mathcal{K}_1^{i,j}\{\ \}$ such that

$$\cfrac{\cfrac{\mathcal{K}_0^{i,j}\left\{\, S_k^{i,j} : k \in I_j^i \,\right\} \triangleleft \mathcal{K}_1^{i,j}\left\{\, T_k^{i,j} : k \in J_j^i \,\right\}}{\mathcal{K}^{i,j}\left\{\, S_k^{i,j} \triangleleft T_k^{i,j} : 1 \leq k \leq \ell^{i,j} \,\right\}}}{\hat{R}_j^i}\ .$$

Define $\hat{S}_j^i$ and $\hat{T}_j^i$ as follows. If $R_j^i = \hat{R}_j^i$, then

$$\hat{S}_j^i = \mathcal{K}_0^{i,j}\left\{\, S_k^{i,j} : k \in I_j^i \,\right\} \text{ and } \hat{T}_j^i = \mathcal{K}_1^{i,j}\left\{\, T_k^{i,j} : k \in J_j^i \,\right\};$$

and hence, we can construct the derivation

$$\frac{\mathcal{K}_0^{i,j}\left\{\, S_k^{i,j} : k \in I_j^i \,\right\} \triangleleft \mathcal{K}_1^{i,j}\left\{\, T_k^{i,j} : k \in J_j^i \,\right\}}{R_j^i}$$

where the premise equals $\hat{S}_j^i \triangleleft \hat{T}_j^i$. If however $R_j^i = \text{И}x.\hat{R}_j^i$, then define

$$\hat{S}_j^i = \text{И}x.\mathcal{K}_0^{i,j}\left\{\, S_k^{i,j} : k \in I_j^i \,\right\} \text{ and } \hat{T}_j^i = \text{И}x.\mathcal{K}_1^{i,j}\left\{\, T_k^{i,j} : k \in J_j^i \,\right\};$$

and hence, the derivation

$$\begin{array}{c} \hat{S}^i_j \triangleleft \hat{T}^i_j \\ \hline \text{И}x.\left(\mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\} \triangleleft \mathcal{K}^{i,j}_1\left\{\, T^{i,j}_k : k \in J^i_j \,\right\}\right) \\ \hline R^i_j \end{array}$$

can be constructed. By Lemma 4.5, for some $K^i \subseteq \{1 \ldots m_i\}$, $L^i \subseteq \{1 \ldots m_i\}$ and killing contexts $\mathcal{K}^i_0\{\ \}$ and $\mathcal{K}^i_1\{\ \}$, we obtain the following derivation:

$$\begin{array}{c} \mathcal{K}^i_0\left\{\, \hat{S}^i_j : j \in K^i \,\right\} \triangleleft \mathcal{K}^i_1\left\{\, \hat{T}^i_j \triangleleft W^i_j : j \in L^i \,\right\} \\ \hline \mathcal{K}^i\left\{\, \hat{S}^i_j \triangleleft \hat{T}^i_j \triangleleft W^i_j : 1 \leq j \leq m_i \,\right\} \end{array}$$

By using the above derivations we can construct the following derivation:

$$\begin{array}{c} \mathcal{K}\left\{\, U^0_i \triangleleft \mathcal{K}^i_0\left\{\, \hat{S}^i_j : j \in K^i \,\right\} \triangleleft \mathcal{K}^i_1\left\{\, \hat{T}^i_j \triangleleft W^i_j : j \in L^i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline \mathcal{K}\left\{\, U^0_i \triangleleft \mathcal{K}^i\left\{\, \hat{S}^i_j \triangleleft \hat{T}^i_j \triangleleft W^i_j : 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline \mathcal{K}\left\{\, U^0_i \triangleleft \mathcal{K}^i\left\{\, R^i_j \triangleleft W^i_j : 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline \mathcal{K}\left\{\, U^0_i \triangleleft \mathcal{K}^i\left\{\, V^i_j \triangleleft W^i_j : 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline \mathcal{K}\left\{\, U^0_i \triangleleft U^1_i : 1 \leq i \leq n \,\right\} \\ \hline Q \end{array}$$

Consider whether the judgement $\vdash \text{Э}x.P_1 \mathbin{⅋} \hat{S}^i_j$ holds. We have two cases: in the first, $\hat{S}^i_j = \mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\}$ and $x \mathbin{\#} \hat{S}^i_j$; in the second $\hat{S}^i_j = \text{И}x.\mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\}$. In each case, one of the following derivations can be respectively constructed.

$$\begin{array}{c} \text{И}x.\left(P_1 \mathbin{⅋} \mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\}\right) \\ \hline \text{И}x.P_1 \mathbin{⅋} \mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\} \\ \hline \text{Э}x.P_1 \mathbin{⅋} \mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\} \end{array} \qquad \begin{array}{c} \text{И}x.\left(P_1 \mathbin{⅋} \mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\}\right) \\ \hline \text{Э}x.P_1 \mathbin{⅋} \text{И}x.\mathcal{K}^{i,j}_0\left\{\, S^{i,j}_k : k \in I^i_j \,\right\} \end{array}$$

Similarly, consider whether judgement $\vdash \text{Э}x.P_2 \mathbin{⅋} \hat{T}^i_j$ holds. Either we have

$$\hat{T}^i_j = \mathcal{K}^{i,j}_1\left\{\, T^{i,j}_k : k \in J^i_j \,\right\} \text{ and } x \mathbin{\#} \hat{T}^i_j;$$

or we have $\hat{T}^i_j = \text{И}x.\mathcal{K}^{i,j}_1\left\{\, T^{i,j}_k : k \in J^i_j \,\right\}$. In each case, one of the following derivations holds, respectively.

$$\begin{array}{c} \text{И}x.\left(P_2 \mathbin{⅋} \mathcal{K}^{i,j}_1\left\{\, T^{i,j}_k : k \in J^i_j \,\right\}\right) \\ \hline \text{И}x.P_2 \mathbin{⅋} \mathcal{K}^{i,j}_1\left\{\, T^{i,j}_k : k \in J^i_j \,\right\} \\ \hline \text{Э}x.P_2 \mathbin{⅋} \mathcal{K}^{i,j}_1\left\{\, T^{i,j}_k : k \in J^i_j \,\right\} \end{array} \qquad \begin{array}{c} \text{И}x.\left(P_2 \mathbin{⅋} \mathcal{K}^{i,j}_1\left\{\, T^{i,j}_k : k \in J^i_j \,\right\}\right) \\ \hline \text{Э}x.P_2 \mathbin{⅋} \hat{T}^i_j \end{array}$$

Thereby, by applying one of the above cases for each i and j, the following two proofs exist.

$$
\begin{array}{c}
\circ \\ \hline
\mathcal{K}^{i}_{0}\left\{\, \text{И}x.\mathcal{K}^{i,j}_{0}\left\{\, \circ \colon k \in I^{i}_{j} \,\right\} : j \in K^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{0}\left\{\, \text{И}x.\mathcal{K}^{i,j}_{0}\left\{\, P_1 \parr S^{i,j}_{k} : k \in I^{i}_{j} \,\right\} : j \in K^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{0}\left\{\, \text{И}x.\left(P_1 \parr \mathcal{K}^{i,j}_{0}\left\{\, S^{i,j}_{k} : k \in I^{i}_{j} \,\right\}\right) : j \in K^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{0}\left\{\, \text{Э}x.P_1 \parr \hat{S}^{i}_{j} : j \in K^{i} \,\right\} \\ \hline
\text{Э}x.P_1 \parr \mathcal{K}^{i}_{0}\left\{\, \hat{S}^{i}_{j} : j \in K^{i} \,\right\} \\ \hline
\left(P_0 \parr U^{0}_{i}\right) \lhd \left(\text{Э}x.P_1 \parr \mathcal{K}^{i}_{0}\left\{\, \hat{S}^{i}_{j} : j \in K^{i} \,\right\}\right) \\ \hline
\left(P_0 \lhd \text{Э}x.P_1\right) \parr \left(U^{0}_{i} \lhd \mathcal{K}^{i}_{0}\left\{\, \hat{S}^{i}_{j} : j \in K^{i} \,\right\}\right)
\end{array}
\qquad
\begin{array}{c}
\circ \\ \hline
\mathcal{K}^{i}_{1}\left\{\, \text{И}x.\mathcal{K}^{i,j}_{1}\left\{\, \circ \colon k \in J^{i}_{j} \,\right\} : j \in L^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{1}\left\{\, \text{И}x.\mathcal{K}^{i,j}_{1}\left\{\, P_2 \parr T^{i,j}_{k} : k \in J^{i}_{j} \,\right\} : j \in L^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{1}\left\{\, \text{И}x.\left(P_2 \parr \mathcal{K}^{i,j}_{1}\left\{\, T^{i,j}_{k} : k \in J^{i}_{j} \,\right\}\right) : j \in L^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{1}\left\{\, \text{Э}x.P_2 \parr \hat{T}^{i}_{j} : j \in L^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{1}\left\{\, \left(\text{Э}x.P_2 \parr \hat{T}^{i}_{j}\right) \lhd \left(P_3 \parr W^{i}_{j}\right) : j \in L^{i} \,\right\} \\ \hline
\mathcal{K}^{i}_{1}\left\{\, \left(\text{Э}x.P_2 \lhd P_3\right) \parr \left(\hat{T}^{i}_{j} \lhd W^{i}_{j}\right) : j \in L^{i} \,\right\} \\ \hline
\left(\text{Э}x.P_2 \lhd P_3\right) \parr \left(\mathcal{K}^{i}_{1}\left\{\, \hat{T}^{i}_{j} \lhd W^{i}_{j} : j \in L^{i} \,\right\}\right)
\end{array}
$$

Furthermore, by Lemma 4.18,

$$\left|U^{0}_{i} \lhd \mathcal{K}^{i}_{0}\{\, \hat{S}^{i}_{j} : j \in K^{i} \,\}\right| \leq |Q| \text{ and } \left|\mathcal{K}^{i}_{1}\{\, \hat{T}^{i}_{j} \lhd W^{i}_{j} : j \in L^{i} \,\}\right| \leq |Q| \,.$$

Hence, sizes

$$\left|\left(P_0 \lhd \text{Э}x.P_1\right) \parr \left(U^{0}_{i} \lhd \mathcal{K}^{i}_{0}\{\, \hat{S}^{i}_{j} : j \in K^{i} \,\}\right)\right| \text{ and } \left|\left(\text{Э}x.P_2 \lhd P_3\right) \parr \left(\mathcal{K}^{i}_{1}\{\, \hat{T}^{i}_{j} \lhd W^{i}_{j} : j \in L^{i} \,\}\right)\right|$$

are strictly bounded above by $|(P_0 \lhd \text{Э}x.P_1 \lhd \text{Э}x.P_2 \lhd P_3) \parr Q|$, as required. Cases for *left wen* and *right wen* rules are similar.

D Principal case for times. There is only one principal case for *times*, which does not differ significantly from the corresponding case in BV and its extensions. A proof may begin with an instance of the *switch* rule of the form

$$\frac{(T_0 \otimes U_0 \otimes ((T_1 \otimes U_1) \parr V)) \parr W}{(T_0 \otimes T_1 \otimes U_0 \otimes U_1) \parr V \parr W} \quad \text{where} \vdash (T_0 \otimes U_0 \otimes ((T_1 \otimes U_1) \parr V)) \parr W,$$

such that $T_0 \otimes U_0 \not\equiv \circ$ and $V \not\equiv \circ$ (otherwise the *switch* rule cannot be applied), and also $T_0 \otimes T_1 \not\equiv \circ$ and $U_0 \otimes U_1 \not\equiv \circ$ (otherwise splitting holds trivially). By the induction hypothesis, there exist R_i and S_i such that $\vdash (T_0 \otimes U_0) \parr R_i$ and $\vdash (T_1 \otimes U_1) \parr V \parr S_i$ hold, for $1 \leq i \leq n$, and an n-ary killing context $\mathcal{K}\{\ \}$ such that derivation $\dfrac{\mathcal{K}\{\, R_1 \parr S_1, \ldots, R_n \parr S_n \,\}}{W}$ holds. Furthermore $|(T_0 \otimes U_0) \parr R_i|$ and $|(T_1 \otimes U_1) \parr V \parr S_i|$ are bounded above by $|(T_0 \otimes U_0 \otimes ((T_1 \otimes U_1) \parr V)) \parr W|$. Hence, by the induction hypothesis twice there exist formulae $P^{i,0}_{j}$, $Q^{i,0}_{j}$, $P^{i,1}_{k}$ and $Q^{i,1}_{k}$ such that $\vdash T_0 \parr P^{i,0}_{j}$, $\vdash U_0 \parr Q^{i,0}_{j}$, $\vdash T_1 \parr P^{i,1}_{k}$ and $\vdash U_1 \parr Q^{i,1}_{k}$, for $1 \leq j \leq m^{0}_{i}$ and $1 \leq k \leq m^{1}_{i}$, and m^{0}_{i}-ary killing context $\mathcal{K}^{0}_{i}\{\ \}$ and m^{1}_{i}-ary killing context $\mathcal{K}^{1}_{i}\{\ \}$ such that derivations

$$\frac{\mathcal{K}^{0}_{i}\left\{\, P^{i,0}_{j} \parr Q^{i,0}_{j} : 1 \leq j \leq m^{0}_{i} \,\right\}}{R_i} \quad \text{and} \quad \frac{\mathcal{K}^{1}_{i}\{\, P^{i,1}_{k} \parr Q^{i,1}_{k} : 1 \leq k \leq m^{1}_{i} \,\}}{V \parr S_i}$$

can be constructed. Thereby the following derivation can be constructed.

$$\begin{array}{c}
\mathcal{K}\left\{\, \mathcal{K}_i^1\left\{\, \mathcal{K}_i^0\left\{\, P_j^{i,0} \parr P_k^{i,1} \parr Q_j^{i,0} \parr Q_k^{i,1} \colon 1 \leq j \leq m_i^0 \,\right\} \colon 1 \leq k \leq m_i^1 \,\right\} \colon 1 \leq i \leq n \,\right\} \\ \hline
\mathcal{K}\left\{\, \mathcal{K}_i^1\left\{\, \mathcal{K}_i^0\left\{\, P_j^{i,0} \parr Q_j^{i,0} \colon 1 \leq j \leq m_i^0 \,\right\} \parr P_k^{i,1} \parr Q_k^{i,1} \colon 1 \leq k \leq m_i^1 \,\right\} \colon 1 \leq i \leq n \,\right\} \\ \hline
\mathcal{K}\left\{\, \mathcal{K}_i^0\left\{\, P_j^{i,0} \parr Q_j^{i,0} \colon 1 \leq j \leq m_i^0 \,\right\} \parr \mathcal{K}_i^1\left\{\, P_k^{i,1} \parr Q_k^{i,1} \colon 1 \leq k \leq m_i^1 \,\right\} \colon 1 \leq i \leq n \,\right\} \\ \hline
\mathcal{K}\{\, R_i \parr V \parr S_i \colon 1 \leq i \leq n \,\} \\ \hline
V \parr \mathcal{K}\{\, R_i \parr S_i \colon 1 \leq i \leq n \,\} \\ \hline
V \parr W
\end{array}$$

Now observe that the following two proofs can be constructed.

$$\begin{array}{c}
\circ \\ \hline
\left(T_0 \parr P_j^{i,0}\right) \otimes \left(T_1 \parr P_k^{i,1}\right) \\ \hline
(T_0 \otimes T_1) \parr P_j^{i,0} \parr P_k^{i,1}
\end{array}
\qquad\qquad
\begin{array}{c}
\circ \\ \hline
\left(U_0 \parr Q_j^{i,0}\right) \otimes \left(U_1 \parr Q_k^{i,1}\right) \\ \hline
(U_0 \otimes U_1) \parr Q_j^{i,0} \parr Q_k^{i,1}
\end{array}$$

Furthermore, $|T_0 \otimes T_1|_{occ} \sqsubset |T_0 \otimes T_1 \otimes U_0 \otimes U_1|_{occ}$ and $|U_0 \otimes U_1|_{occ} \sqsubset |T_0 \otimes T_1 \otimes U_0 \otimes U_1|_{occ}$, since $T_0 \otimes T_1 \not\equiv \circ$ and $U_0 \otimes U_1 \not\equiv \circ$. Also, by Lemma 4.18, the following inequality holds.

$$\left|\mathcal{K}\left\{\, \mathcal{K}_i^1\left\{\, \mathcal{K}_i^0\left\{\, P_j^{i,0} \parr P_k^{i,1} \parr Q_j^{i,0} \parr Q_k^{i,1} \colon 1 \leq j \leq m_i^0 \,\right\} \colon 1 \leq k \leq m_i^1 \,\right\} \colon 1 \leq i \leq n \,\right\}\right| \leq |V \parr W|$$

Hence both $\left|P_j^{i,0} \parr P_k^{i,1}\right| \leq |V \parr W|$ and $\left|Q_j^{i,0} \parr Q_k^{i,1}\right| \leq |V \parr W|$ hold. Thereby the size of each of the above proofs is strictly bounded above by the size of the proof of $(T_0 \otimes T_1 \otimes U_0 \otimes U_1) \parr V \parr W$.

E Principal cases for with. There are three forms of principal case where the *with* operator is directly involved in the bottommost rules. Note that in MAV the *with* operator is separated from the core splitting lemma, much like universal quantification in this paper. However, in the case of MAV1 the *left name* and *right name* rules introduce inter-dependencies between nominals and *with*, forcing cases for *with* to be checked in this lemma.

E.1 Consider the principal case involving the *extrude* rule. In this case, the bottommost rule is of the form

$$\frac{(P \parr R) \with (Q \parr R) \parr S}{(P \with Q) \parr R \parr S} \quad \text{where } \vdash (P \parr R) \with (Q \parr R) \parr S \text{ holds.}$$

Now, by the induction hypothesis, since $\vdash (P \parr R) \with (Q \parr R) \parr S$ holds, we have that $\vdash P \parr R \parr S$ and $\vdash Q \parr R \parr S$ hold, as required.

E.2 Consider the principal case involving the *left name* rule. In this case, the bottommost rule is of the form

$$\frac{\text{Ǝ}x.(P \with Q) \parr R}{(\text{Ǝ}x.P \with Q) \parr R} \text{ , where } x \mathrel{\#} Q \text{, such that } \vdash \text{Ǝ}x.(P \with Q) \parr R.$$

By the induction hypothesis, there exist S and $\hat{S}$ such that $\dfrac{S}{R}$ and $x \mathrel{\#} S$ and $\vdash (P \with Q) \parr \hat{S}$ and either $S = \hat{S}$ or $S = \text{И}x.\hat{S}$. Furthermore, the size of the proof of $(P \with Q) \parr \hat{S}$ is strictly less than the size of the proof of $(\text{Ǝ}x.P \with Q) \parr R$, since the *wen* count strictly decreases, and by Lemma 4.18, $\left|\hat{S}\right| \leq |R|$. By the induction hypothesis again, $\vdash P \parr \hat{S}$ and $\vdash Q \parr \hat{S}$ hold. Now if $S = \hat{S}$ then $x \mathrel{\#} \hat{S}$ and $\vdash Q \parr S$ holds immediately, whereas $\vdash \text{Ǝ}x.P \parr R$ is proved as below left. Otherwise, $S = \text{И}x.\hat{S}$ and $\vdash \text{Ǝ}x.P \parr R$ is proved in the middle derivation below, whereas $\vdash Q \parr S$ is proved in the right derivation below.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\text{И}x.\circ}}{\text{И}x.\left(P \parr \hat{S}\right)}}{\text{Э}x.\left(P \parr \hat{S}\right)}}{\text{Э}x.P \parr \hat{S}}}{\text{Э}x.P \parr R} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\circ}{\text{И}x.\circ}}{\text{И}x.\left(P \parr \hat{S}\right)}}{\text{Э}x.P \parr \text{И}x.\hat{S}}}{\text{Э}x.P \parr R} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\circ}{\text{И}x.\circ}}{\text{И}x.\left(Q \parr \hat{S}\right)}}{\text{Э}x.\left(Q \parr \hat{S}\right)}}{Q \parr \text{Э}x.\hat{S}} \ .$$

Hence, in either case, $\vdash Q \parr S$ and since $\dfrac{Q \parr S}{Q \parr R}$, we have that $\vdash Q \parr R$ holds. Thereby $\vdash \text{Э}x.P \parr R$ and $\vdash Q \parr R$ hold, as required. The case for the *left name* rule, where И replaces Э is similar; as are the cases for the *right name* and *with name* rules.

E.3 Consider the principal case involving the *medial* rule. In this case, the bottommost rule of a proof is of the form

$$\dfrac{((P \,\&\, R) \triangleleft (Q \,\&\, S)) \parr W}{((P \triangleleft Q) \,\&\, (R \triangleleft S)) \parr W} \quad \text{such that} \vdash ((P \,\&\, R) \triangleleft (Q \,\&\, S)) \parr W \text{ holds.}$$

By the induction hypothesis, for $1 \leq i \leq n$ there exists U_i and V_i such that $\vdash (P \,\&\, R) \parr U_i$ and $\vdash (Q \,\&\, S) \parr V_i$ hold, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\, U_i \triangleleft V_i : 1 \leq i \leq n \,\}}{W}$. Furthermore, the size of the proofs of $(P \,\&\, R) \parr U_i$ and $(Q \,\&\, S) \parr V_i$ are strictly less than the size of the proof of $((P \,\&\, R) \triangleleft (Q \,\&\, S)) \parr W$. Hence by the induction hypothesis again, $\vdash P \parr U_i$, $\vdash R \parr U_i$, $\vdash Q \parr V_i$ and $\vdash S \parr V_i$. Hence we can construct the following two proofs, as required.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\mathcal{K}\{\, \circ : 1 \leq i \leq n \,\}}}{\mathcal{K}\{\, (P \parr U_i) \triangleleft (Q \parr V_i) : 1 \leq i \leq n \,\}}}{\mathcal{K}\{\, (P \triangleleft Q) \parr (U_i \triangleleft V_i) : 1 \leq i \leq n \,\}}}{(P \triangleleft Q) \parr \mathcal{K}\{\, U_i \triangleleft V_i : 1 \leq i \leq n \,\}}}{(P \triangleleft Q) \parr W} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\mathcal{K}\{\, \circ : 1 \leq i \leq n \,\}}}{\mathcal{K}\{\, (R \parr U_i) \triangleleft (S \parr V_i) : 1 \leq i \leq n \,\}}}{\mathcal{K}\{\, (R \triangleleft S) \parr (U_i \triangleleft V_i) : 1 \leq i \leq n \,\}}}{(R \triangleleft S) \parr \mathcal{K}\{\, U_i \triangleleft V_i : 1 \leq i \leq n \,\}}}{(R \triangleleft S) \parr W}$$

F Commutative cases induced by equivariance. There are certain commutative cases induced by the *equivariance* rule for nominal quantifiers. These are the cases that force the rules *all name*, *with name*, *left name* and *right name* to be included. Notice also that *equivariance* for *new* is required when handling the case induced by *equivariance* for *wen*; hence *equivariance* for both nominal quantifiers must be explicit structural rules rather than properties derived from each other.

F.1 Consider the commutative case for *wen* where the bottommost rule of a proof is an instance of the *close* rule of following form

$$\dfrac{\text{И}y.(\text{Э}x.P \parr Q) \parr R}{\text{Э}x.\text{Э}y.P \parr \text{И}y.Q \parr R} \text{ ,where} \vdash \text{И}y.(\text{Э}x.P \parr Q) \parr R,\ y \mathrel{\#} R \text{ and } x \mathrel{\#} R.$$

Notice that $\text{Э}x$ is the principal connective but the *close* rule is applied to $\text{Э}y$ behind the principal connective. Thus we desire some formula R' such that $\dfrac{R'}{\text{И}y.Q \parr R}$ and $x \mathrel{\#} R'$ and either $\vdash \text{Э}y.P \parr R'$ or there exists Q' such that $R' = \text{И}x.Q'$ and $\vdash \text{Э}y.P \parr Q'$, and the size of $\text{Э}y.P \parr R'$ is strictly smaller than $\text{Э}x.\text{Э}y.P \parr \text{И}y.Q \parr R$. By the induction hypothesis, there exist S and T such that $y \mathrel{\#} S$ and $\vdash \text{Э}x.P \parr Q \parr T$ and either $S = T$ or $S = \text{Э}y.T$

and the derivation $\dfrac{S}{R}$ holds. Furthermore the size of the proof of $\text{Э}x.P \parr Q \parr T$ is bounded above by the size of the proof of $\text{И}y.(\text{Э}x.P \parr Q) \parr R$; hence strictly bounded by the size of the proof of $\text{Э}x.\text{Э}y.P \parr \text{И}y.Q \parr R$. Hence, by induction, there exist U and V such that $\vdash P \parr V$ and $x \# U$ and either $U = V$ or $U = \text{И}x.V$ the derivation $\dfrac{U}{Q \parr T}$ holds. Observe that if $S = T$, then $\dfrac{\text{И}y.(Q \parr T)}{\text{И}y.Q \parr S}$, since $y \# S$. If $S = \text{Э}y.T$ then $\dfrac{\text{И}y.(Q \parr T)}{\text{И}y.Q \parr \text{Э}y.T}$. Thereby the following derivation can be constructed, where if $U = V$ then $W = \text{И}y.V$ and if $U = \text{И}x.V$ then $W = \text{И}x.\text{И}y.V$, and also the premise is equivalent to W by *equivariance* for *new*: $\cfrac{\cfrac{\cfrac{\text{И}y.U}{\text{И}y.(Q \parr T)}}{\text{И}y.Q \parr S}}{\text{И}y.Q \parr R}$. Furthermore, the following proof can be constructed $\cfrac{\cfrac{\cfrac{\cfrac{}{\circ}}{\text{И}y.\circ}}{\text{И}y.(P \parr V)}}{\text{Э}y.P \parr \text{И}y.V}$ and, by Lemma 4.18, $|\text{И}y.V| \leq |\text{И}y.Q \parr R|$ hence $|\text{Э}y.P \parr \text{И}y.V| \prec |\text{Э}x.\text{Э}y.P \parr \text{И}y.Q \parr R|$, as required.

F.2 Consider a commutative case for *new* induced by *equivariance* for *new*, where the bottommost rule is an instance of *extrude new* of the form

$$\frac{\text{И}y.(\text{И}x.P \parr Q) \parr R}{\text{И}x.\text{И}y.P \parr Q \parr R}\ \text{, where } y \# Q \text{ and } \vdash \text{И}y.(\text{И}x.P \parr Q) \parr R.$$

By the induction hypothesis, there exist S and T such that $y \# S$ and $\vdash \text{И}x.P \parr Q \parr T$ and either $S = T$ or $S = \text{Э}y.T$, where $\dfrac{S}{R}$. Furthermore, the size of the proof of $\text{И}x.P \parr Q \parr T$ is bound above by the size of the proof of $\text{И}y.(\text{И}x.P \parr Q) \parr R$, hence strictly bound above by the size of the proof of $\text{И}x.\text{И}y.P \parr Q \parr R$. Hence, by induction again, there exist U and V such that $x \# U$ and $\vdash P \parr V$ and either $U = V$ or $U = \text{Э}x.V$, and also $\dfrac{U}{Q \parr T}$. Now define $\hat{W}$ and W as follows. If $S = T$ then let $\hat{W} = V$. If $S = \text{Э}y.T$ then let $\hat{W} = \text{Э}y.V$. If $U = V$ then let $W = \hat{W}$. If $U = \text{Э}x.V$ then let $W = \text{Э}x.\hat{W}$. Now observe if $S = T$ then $\cfrac{\cfrac{U}{Q \parr T}}{Q \parr R}$ and $U = W$. For $S = \text{Э}y.T$ observe $\cfrac{\cfrac{\cfrac{\text{Э}y.U}{\text{Э}y.(Q \parr T)}}{Q \parr \text{Э}y.T}}{Q \parr R}$, since $y \# Q$, and if $U = V$ then $\text{Э}y.U = \hat{W}$, while if $U = \text{Э}x.V$ then $\text{Э}y.U \equiv \text{Э}x.\hat{W}$, by *equivariance* for *wen*. Hence in all cases $\dfrac{W}{Q \parr R}$ and, since $y \# Q$ and $y \# T$, we can arrange that $y \# W$. Now, for the cases where $\hat{W} = V$, we have $y \# V$, and hence $\dfrac{\text{И}y.(P \parr V)}{\text{И}y.P \parr V}$. Also if $\hat{W} = \text{Э}y.V$, then $\dfrac{\text{И}y.(P \parr V)}{\text{И}y.P \parr \text{Э}y.V}$. Hence in either case we can construct the proof $\cfrac{\cfrac{\cfrac{\cfrac{}{\circ}}{\text{И}y.\circ}}{\text{И}y.(P \parr V)}}{\text{И}y.P \parr \hat{W}}$. Furthermore, $\left|\text{И}y.P \parr \hat{W}\right| \prec |\text{И}x.\text{И}y.P \parr Q \parr R|$, since by Lemma 4.18 $\left|\hat{W}\right| \leq |Q \parr R|$.

F.3 Similar commutative cases for *wen* and *new* as principal formulae are induced by *equivariance* where the bottommost rule in a proof is an instance of the *close*, *right wen* or *suspend* rules. In each case, the quantifier involved in the bottommost rule appears behind the principal connective and is propagated in front of the principal connective using *equivariance.*

G Regular commutative cases. As in every splitting lemma, there are numerous *commutative* cases where the bottommost rule in a proof does not directly involve the principal connective. For each principal formula handled by this splitting lemma (*new*, *wen*, *with*, *seq* and *times*) there are commutative cases induced by *new*, *wen*, *all*, *with* and *times* and also two commutative cases induced by *seq*. Thus there are 35 similar commutative cases to check, that all follow a pattern, hence only a representative selection of four cases are presented that make special use of α-conversion and the rules *new wen*, *all name*, *with name*, *left name* and *right name*. Further, representative cases appear in the proof for existential quantifiers.

G.1 Consider the commutative case where the principal formula is $\text{И}x.P$ and the bottommost rule is an instance of *extrude new* but applied to a distinct *new* quantifier $\text{И}y.Q$, as in the following rule instance

$$\frac{\text{И}y.(\text{И}x.P \parr Q \parr R) \parr S}{\text{И}x.P \parr \text{И}y.Q \parr R \parr S}\ \text{, where } y \mathrel{\#} \text{И}x.P \parr R.$$

Also assume, by α-conversion, that $x \neq y$. By induction, there exist T and U such that $\vdash \text{И}x.P \parr Q \parr R \parr U$, $y \mathrel{\#} T$ and either $T = U$ or $T = \text{Э}y.U$, and also $\frac{T}{S}$. Furthermore, the size of the proof of $\text{И}x.P \parr Q \parr R \parr U$ is bounded above by the size of the proof of $\text{И}y.(\text{И}x.P \parr Q \parr R) \parr S$ and hence strictly bounded above by the size of the proof of $\text{И}x.P \parr \text{И}y.Q \parr R \parr S$, enabling the induction hypothesis. Hence, by the induction hypothesis, there exist formulae V and $\hat{V}$ such that $\vdash P \parr \hat{V}$ and $x \mathrel{\#} V$ and either $V = \hat{V}$ or $V = \text{Э}x.\hat{V}$, and also $\dfrac{V}{Q \parr R \parr U}$. Define W such that if $V = \hat{V}$ then $W = \text{И}y.\hat{V}$ and if $V = \text{Э}x.\hat{V}$ then $W = \text{Э}x.\text{И}y.\hat{V}$. Hence if $V = \text{Э}x.\hat{V}$ then $\dfrac{\text{Э}x.\text{И}y.\hat{V}}{\text{И}y.V}$ by applying the *new wen* rule, where the premise equals W. If $V = \hat{V}$ then $\text{И}y.V = W$. In both cases, $x \mathrel{\#} W$. Now observe that either $T = U$ and $y \mathrel{\#} U$, hence the derivation (a) below holds; or $T = \text{Э}y.U$, hence the derivation (b) below holds. Given these, the derivation (c) can be constructed:

$$\underset{(a)}{\dfrac{\text{И}y.(Q \parr R \parr U)}{\text{И}y.Q \parr R \parr T}} \qquad \underset{(b)}{\dfrac{\dfrac{\text{И}y.(Q \parr R \parr U)}{\text{И}y.(Q \parr R) \parr \text{Э}y.U}}{\text{И}y.Q \parr R \parr \text{Э}y.U}} \qquad \underset{(c)}{\dfrac{\dfrac{\dfrac{\dfrac{W}{\text{И}y.V}}{\text{И}y.(Q \parr R \parr U)}}{\text{И}y.Q \parr R \parr T}}{\text{И}y.Q \parr R \parr S}} \qquad \underset{(d)}{\dfrac{\dfrac{\dfrac{\circ}{\text{И}y.\circ}}{\text{И}y.\left(P \parr \hat{V}\right)}}{P \parr \text{И}y.\hat{V}}}$$

Since $y \mathrel{\#} \text{И}x.P \parr R$ and $x \neq y$, we have $y \mathrel{\#} P$; thereby the proof (d) above can be constructed. Furthermore, $\left|P \parr \text{И}y.\hat{V}\right| \prec |\text{Э}x.P \parr \text{И}y.Q \parr R \parr S|$ since by Lemma 4.18 $\left|\text{И}y.\hat{V}\right| \leq |\text{И}y.Q \parr R \parr S|$ and the *wen count* strictly decreases.

G.2 Consider the commutative case for principal formula $\text{Э}x.T$ where the bottommost rule is *external*:

$$\frac{((\text{Э}x.T \parr U \parr W) \mathbin{\&} (\text{Э}x.T \parr V \parr W)) \parr P}{\text{Э}x.T \parr (U \mathbin{\&} V) \parr W \parr P}$$

where $\vdash ((\text{Э}x.T \parr U \parr W) \mathbin{\&} (\text{Э}x.T \parr V \parr W)) \parr P$ holds. By the induction hypothesis, we have that both $\vdash \text{Э}x.T \parr U \parr W \parr P$ and $\vdash \text{Э}x.T \parr V \parr W \parr P$ hold; and furthermore the multiset inequalities

$$\begin{array}{lcl} |\text{Э}x.T \parr U \parr W \parr P|_{occ} & \sqsubset & |\text{Э}x.T \parr (U \mathbin{\&} V) \parr W \parr P|_{occ} \text{ and} \\ |\text{Э}x.T \parr V \parr W \parr P|_{occ} & \sqsubset & |\text{Э}x.T \parr (U \mathbin{\&} V) \parr W \parr P|_{occ} \end{array}$$

hold. Hence, by the induction hypothesis, there exist Q and $\hat{Q}$ such that $\vdash T \parr \hat{Q}$, $x \mathrel{\#} Q$ and either $Q = \hat{Q}$ or $Q = \text{И}x.\hat{Q}$. Also, by the induction hypothesis, there exist R and $\hat{R}$ such that $\vdash T \parr \hat{R}$, $x \mathrel{\#} R$ and either $R = \hat{R}$ or $R = \text{И}x.\hat{R}$. Furthermore the two derivations $\dfrac{Q}{U \parr W \parr P}$ and $\dfrac{R}{V \parr W \parr P}$ hold. Now define S such that if $Q = \hat{Q}$ and $R = \hat{R}$ then $S = \hat{Q} \mathbin{\&} \hat{R}$, and $S = \text{Э}x.\left(\hat{Q} \mathbin{\&} \hat{R}\right)$ otherwise, observing that in either case $x \mathrel{\#} S$. In the case $Q = \text{Э}x.\hat{Q}$ and $R = \text{Э}x.\hat{R}$, by the *with name* rule, $\dfrac{\text{Э}x.\left(\hat{Q} \mathbin{\&} \hat{R}\right)}{\text{Э}x.\hat{Q} \mathbin{\&} \text{Э}x.\hat{R}}$. In the case $Q = \text{Э}x.\hat{Q}$ and $R = \hat{R}$, by the *left name* rule, $\dfrac{\text{Э}x.\left(\hat{Q} \mathbin{\&} \hat{R}\right)}{\text{Э}x.\hat{Q} \mathbin{\&} \hat{R}}$. In the case that $Q = \hat{Q}$ and $R = \text{Э}x.\hat{R}$, by the *right name* rule, $\dfrac{\text{Э}x.\left(\hat{Q} \mathbin{\&} \hat{R}\right)}{\hat{Q} \mathbin{\&} \text{Э}x.\hat{R}}$. Thereby the following derivation and proof can be constructed:

$$\dfrac{\dfrac{\dfrac{S}{Q \mathbin{\&} R}}{(U \parr W \parr P) \mathbin{\&} (V \parr W \parr P)}}{(U \mathbin{\&} V) \parr W \parr P} \qquad \dfrac{\dfrac{\dfrac{\circ}{\circ \mathbin{\&} \circ}}{\left(T \parr \hat{Q}\right) \mathbin{\&} \left(T \parr \hat{R}\right)}}{T \parr \left(\hat{Q} \mathbin{\&} \hat{R}\right)} \ .$$

Furthermore, by Lemma 4.18, $|S| \leq |(U \mathbin{\&} V) \parr W \parr P|$; and, since the *wen* count strictly decreases, $\left|T \parr \hat{Q} \mathbin{\&} \hat{R}\right| \prec |\text{Э}x.T \parr (U \mathbin{\&} V) \parr W \parr P|$.

G.3 Consider the commutative case where the principal formula is $\text{Э}x.T$ and the bottommost rule is an instance of the *extrude1* rule of the form

$$\dfrac{\forall y.(\text{Э}x.T \parr U \parr V) \parr W}{\text{Э}x.T \parr \forall y.U \parr V \parr W}$$

assuming $y \mathrel{\#} (\text{Э}x.T \parr V)$ and $\vdash \forall y.(\text{Э}x.T \parr U \parr V) \parr W$ holds. By Lemma 4.2, for every variable z, $\vdash (\text{Э}x.T \parr U \parr V)\left\{{}^{z}\!/_{y}\right\} \parr W$ holds. Furthermore, since $y \mathrel{\#} (\text{Э}x.T \parr V)$, we have equivalence $(\text{Э}x.T \parr U \parr V)\left\{{}^{z}\!/_{y}\right\} \parr W \equiv \text{Э}x.T \parr U\left\{{}^{z}\!/_{y}\right\} \parr V \parr W$. The strict multiset inequality $\left|\text{Э}x.T \parr U\left\{{}^{z}\!/_{y}\right\} \parr V \parr W\right|_{occ} \sqsubset |\text{Э}x.T \parr \forall y.U \parr V \parr W|_{occ}$ holds. Hence, by the induction hypothesis, for every variable z, there exist formulae P^z and Q^z such that $\vdash T \parr Q^z$ and $x \mathrel{\#} P^z$ and either $P^z = Q^z$ or $P^z = \text{И}x.Q^z$, and also $\dfrac{P^z}{U\left\{{}^{z}\!/_{y}\right\} \parr V \parr W}$. Define W^z such that if $P^z = Q^z$ then $W^z = \forall z.Q^z$ and if $P^z = \text{И}x.Q^z$ then $W^z = \text{И}x.\forall z.Q^z$. Hence if $P^z = \text{И}x.Q^z$ then, since $\forall$ permutes with any quantifier using the *all name* rule, $\dfrac{\text{И}x.\forall z.Q^z}{\forall z.\text{И}x.Q^z}$. Hence, for a fresh z such that $z \mathrel{\#} (\forall y.U \parr V \parr W)$ and $z \mathrel{\#} T$, the following derivations can be constructed:

$$\dfrac{\dfrac{\dfrac{W^z}{\forall z.P^z}}{\forall z.\left(U\left\{{}^{z}\!/_{y}\right\} \parr V \parr W\right)}}{\forall y.U \parr V \parr W} \qquad \dfrac{\dfrac{\dfrac{\circ}{\forall z.\circ}}{\forall z.(T \parr Q^z)}}{T \parr \forall z.Q^z}$$

Furthermore, $|W^z| \leq |\forall y.U \parr V \parr W|$ by Lemma 4.18; hence

$$|T \parr \forall z.Q^z| \prec |\text{Э}x.T \parr \forall y.U \parr V \parr W|$$

since the wen count strictly decreases.

G.4 Consider the commutative case where the principal connective is *wen* and the bottommost rule is an instance of the extrude new rule of the form

$$\frac{\text{И}y.(\text{Э}x.P \parr Q \parr R) \parr S}{\text{Э}x.P \parr \text{И}y.Q \parr R \parr S} \; ,$$

where $y \# \text{Э}x.P \parr R$ and also $x \neq y$, where the second condition can be achieved by α-conversion. By the induction hypothesis, there exist T and U such that $\vdash \text{Э}x.P \parr Q \parr R \parr U$, $y \# T$ and either $T = U$ or $T = \text{Э}y.U$, and also $\frac{T}{S}$. Furthermore, the size of the proof of $\text{Э}x.P \parr Q \parr R \parr U$ is bounded above by the size of the proof of $\text{И}y.(\text{Э}x.P \parr Q \parr R) \parr S$ and hence strictly bounded above by the size of the proof of $\text{Э}x.P \parr \text{И}y.Q \parr R \parr S$, enabling the induction hypothesis. Hence, by the induction hypothesis, there exist formulae V and $\hat{V}$ such that $\vdash P \parr \hat{V}$ and $x \# V$ and either $V = \hat{V}$ or $V = \text{И}x.\hat{V}$, and also $\frac{V}{Q \parr R \parr U}$. Define W such that if $V = \hat{V}$ then $W = \text{И}y.\hat{V}$ and if $V = \text{И}x.\hat{V}$ then $W = \text{И}x.\text{И}y.\hat{V}$. Now observe that either we have that $T = U$ and $y \# U$ and hence the derivation (a) below left holds; or we have that $T = \text{Э}y.U$ and hence the derivation (b) belw holds. Hence, by applying one of these cases, we have the derivation (c) below, where the premise is equivalent to W.

$$\underset{(a)}{\frac{\text{И}y.(Q \parr R \parr U)}{\text{И}y.Q \parr R \parr T}} \qquad \underset{(b)}{\cfrac{\cfrac{\text{И}y.(Q \parr R \parr U)}{\text{И}y.(Q \parr R) \parr \text{Э}y.U}}{\text{И}y.Q \parr R \parr \text{Э}y.U}} \qquad \underset{(c)}{\cfrac{\cfrac{\cfrac{\text{И}y.V}{\text{И}y.(Q \parr R \parr U)}}{\text{И}y.Q \parr R \parr T}}{\text{И}y.Q \parr R \parr S}} \qquad \underset{(d)}{\cfrac{\cfrac{\cfrac{\circ}{\text{И}y.\circ}}{\text{И}y.\left(P \parr \hat{V}\right)}}{P \parr \text{И}y.\hat{V}}} \; .$$

Since $y \# \text{Э}x.P$ and $x \neq y$, we have $y \# P$; thereby the proof (d) above can be constructed. Furthermore, $\left|P \parr \text{И}y.\hat{V}\right| \prec |\text{Э}x.P \parr \text{И}y.Q \parr R \parr S|$ since by Lemma 4.18

$$\left|\text{И}y.\hat{V}\right| \leq |\text{И}y.Q \parr R \parr S|$$

and the *wen count* strictly decreases.

H Commutative cases deep in contexts. In many commutative cases, the bottommost rule does not interfere with the principal formula either directly or indirectly. Two such cases are presented for *wen* as the principal connective. Other such cases use almost identical reasoning.

H.1 Consider when a rule is applied outside the scope of the principal formula. In this case, the bottommost rule in a proof is of the form

$$\frac{\text{Э}x.U \parr C\{\, W \,\}}{\text{Э}x.U \parr C\{\, V \,\}} \; \text{, such that} \vdash \text{Э}x.U \parr C\{\, W \,\}.$$

By the induction hypothesis, there exist formulae P and Q such that $\vdash U \parr Q$ and $x \# P$ and either $P = Q$ or $P = \text{И}x.Q$, and also $\frac{P}{C\{\, W \,\}}$. Hence clearly derivation $\cfrac{\cfrac{P}{C\{\, W \,\}}}{C\{\, V \,\}}$ holds. Furthermore, by Lemma 4.18, $|\text{Э}x.U \parr C\{\, W \,\}| \prec |U \parr C\{\, W \,\}|$ and $|U \parr C\{\, W \,\}| \leq |\text{Э}x.U \parr C\{\, V \,\}|$.

H.2 Consider the case where the following application of any rule in a derivation of the form

$$\frac{\text{Ǝ}x.C\{\ U\ \} \parr W}{\text{Ǝ}x.C\{\ T\ \} \parr W}$$

is the bottommost rule is a proof of length $k + 1$, where $\vdash \text{Ǝ}x.C\{\ U\ \} \parr W$ has a proof of length k. Hence, by induction, there exist formulae P and Q such that $\vdash\ C\{\ U\ \} \parr Q$ and $x\ \#\ P$ and either $P = Q$ or $P = \text{И}x.Q$, and also $\frac{P}{W}$. Furthermore, the size of the proof of $C\{\ U\ \} \parr Q$ is bounded above by the size of the proof of $\text{Ǝ}x.C\{\ U\ \} \parr W$; hence either $|C\{\ U\ \} \parr Q| \prec |\text{Ǝ}x.C\{\ U\ \} \parr W|$ or $|C\{\ U\ \} \parr Q| = |\text{Ǝ}x.C\{\ U\ \} \parr W|$ and the length of the proof of $U \parr Q$ is bound by k. The proof $\dfrac{\dfrac{\circ}{C\{\ U\ \} \parr Q}}{C\{\ T\ \} \parr Q}$ can be constructed as required. Furthermore, if $|C\{\ U\ \} \parr Q| \prec \text{Ǝ}x.\ |C\{\ U\ \} \parr W|$ then $|C\{\ U\ \} \parr Q| \prec |\text{Ǝ}x.C\{\ U\ \} \parr C\{\ V\ \}|$, by Lemma 4.18. Otherwise, $|C\{\ U\ \} \parr Q| = |\text{Ǝ}x.C\{\ U\ \} \parr W|$ hence $|U \parr Q| \leq |\text{Ǝ}x.U \parr C\{\ V\ \}|$ by Lemma 4.18 and the length of the proof of $\vdash C\{\ T\ \} \parr Q$ is $k + 1$. Thereby in either case, the size of the proof of $C\{\ T\ \} \parr Q$ is bounded above by the size of the proof of $\text{Ǝ}x.C\{\ T\ \} \parr W$.

This covers all scenarios for the bottommost rule, hence splitting follows by induction over the size of the proof. □

The final three splitting lemmas mainly involve checking commutative cases. The commutative cases follow a similar pattern to the commutative cases in Lemma 4.19.

Lemma 4.20. *If $\vdash \exists x.P \parr Q$, then there exist formulae V_i and values v_i such that $\vdash P\{{}^{v_i}\!/_{x}\} \parr V_i$, where $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\ V_1, V_2, \ldots, V_n\ \}}{Q}$ and if $\mathcal{K}\{\ \}$ binds y then $y\ \#\ (\exists x.P)$.*

The proofs of the splitting lemmas for *plus* and atoms offer no new insight or difficulties compared to their treatment in MAV [23]. Similarly, to the above lemma for existential quantifiers, the proofs mainly involve commutative cases of a standard form.

Lemma 4.21. *If $\vdash (P \oplus Q) \parr R$, then there exist formulae W_i such that either $\vdash P \parr W_i$ or $\vdash Q \parr W_i$ where $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\ W_1, W_2, \ldots, W_n\ \}}{R}$ and if $\mathcal{K}\{\ \}$ binds x then $x\ \#\ (P \oplus Q)$.*

Lemma 4.22. *The following statements hold, for any atom α, where if $\mathcal{K}\{\ \}$ binds x then $x\ \#\ \alpha$.*

- *If $\vdash \overline{\alpha} \parr Q$, then there exist n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\ \alpha, \alpha, \ldots, \alpha\ \}}{Q}$.*
- *If $\vdash \alpha \parr Q$, then there exist n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\ \overline{\alpha}, \overline{\alpha}, \ldots, \overline{\alpha}\ \}}{Q}$.*

5 CONTEXT REDUCTION AND THE ADMISSIBILITY OF CO-RULES

The splitting lemmas in the previous section are formulated for sequent-like *shallow contexts*. By applying splitting repeatedly, *context reduction* (Lemma 5.2) is established, which can be used to extends normalisation properties to an arbitrary (deep) context. In particular, we extend a series of proof normalisation properties called *co-rule elimination* properties to any context, by first establishing the normalisation property in a shallow context, then applying context reduction to extend to any context. Together, these *co-rule elimination* properties establish cut elimination, by eliminating each connective directly involved in a cut one-by-one.

$$\frac{C\{\ \alpha \otimes \overline{\alpha}\ \}}{C\{\ \circ\ \}}\ \text{(atomic co-interaction)} \qquad \frac{C\{\ \forall x.P\ \}}{C\{\ P\{^{v}/_{x}\}\ \}}\ \text{(co-select1)}$$

$$\frac{C\{\ (P \lhd Q) \otimes (U \lhd V)\ \}}{C\{\ (P \otimes U) \lhd (Q \otimes V)\ \}}\ \text{(co-sequence)} \qquad \frac{C\{\ (P \oplus Q) \parr S\ \}}{C\{\ (P \parr R) \oplus (Q \parr S)\ \}}\ \text{(co-external)}$$

$$\frac{C\{\ \circ \oplus \circ\ \}}{C\{\ \circ\ \}}\ \text{(co-tidy)} \qquad \frac{C\{\ P \mathbin{\&} Q\ \}}{C\{\ P\ \}}\ \text{(co-left)} \qquad \frac{C\{\ P \mathbin{\&} Q\ \}}{C\{\ Q\ \}}\ \text{(co-right)}$$

$$\frac{C\{\ \exists x.P \otimes R\ \}}{C\{\ \exists x.(P \otimes R)\ \}}\ \text{(co-extrude1)} \qquad \frac{C\{\ \exists x.\circ\ \}}{C\{\ \circ\ \}}\ \text{(co-tidy1)}$$

$$\frac{C\{\ И x.P \otimes Э x.Q\ \}}{C\{\ Э x.(P \otimes Q)\ \}}\ \text{(co-close)} \qquad \frac{C\{\ Э x.\circ\ \}}{C\{\ \circ\ \}}\ \text{(co-tidy name)}$$

Fig. 8. Co-rules extending the system MAV1 to SMAV1, where $x \# R$.

5.1 Extending from a sequent-like context to a deep context

Context reduction extends rules simulated by splitting to any context. This appears to be the first context reduction lemma in the literature to handle first-order quantifiers. Of particular note is the use of substitutions to account for the effect of existential quantifiers in the context. The trick is to first establish the following stronger invariant.

Lemma 5.1. *If $\vdash C\{\ T\ \}$, then there exist formulae U_i and substitutions σ_i, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\vdash T\sigma_i \parr U_i$; and, for any formula V there exist W_i such that either $W_i = V\sigma_i \parr U_i$ or $W_i = \circ$ and the following holds:* $\dfrac{\mathcal{K}\{\ W_1, W_2, \ldots, W_n\ \}}{C\{\ V\ \}}$.

Having established the above stronger invariant, the context lemma follows directly.

Lemma 5.2 (Context reduction). *If $\vdash P\sigma \parr R$ yields that $\vdash Q\sigma \parr R$, for any formula R and substitution of terms for variables σ, then $\vdash C\{\ P\ \}$ yields $\vdash C\{\ Q\ \}$, for any context $C\{\ \}$.*

Proof. Assume that for any formula U, $\vdash S \parr U$ yields $\vdash T \parr U$, and fix any context $C\{\ \}$ such that $\vdash C\{\ S\ \}$ holds. By Lemma 5.1, there exist n-ary killing context $\mathcal{K}\{\ \}$ and, for $1 \leq i \leq n$, P_i such that either $P_i = \circ$ or there exists W_i where $P_i = T \parr W_i$ and $\vdash S \parr W_i$, and furthermore $\dfrac{\mathcal{K}\{\ P_1, \ldots, P_n\ \}}{C\{\ T\ \}}$.

Since, by our assumption, also $\vdash T \parr W_i$ holds for $1 \leq i \leq n$, the proof $\dfrac{\dfrac{\dfrac{\circ}{\mathcal{K}\{\ \circ, \ldots, \circ\ \}}}{\mathcal{K}\{\ P_1, \ldots, P_n\ \}}}{C\{\ T\ \}}$ can be constructed. Therefore $\vdash C\{\ T\ \}$ holds. □

Note that the case for existential quantifiers will not work for second-order quantifiers, since termination of the induction is reliant on the size of the term-free part of the formula being reduced. Thus the techniques in the above proof apply to first-order quantifiers only.

5.2 Cut elimination as co-rule elimination

For a rule of the form $\frac{Q}{P}$, there is a corresponding *co-rule* of the form $\frac{\overline{P}}{\overline{Q}}$, where premise and conclusion are interchanged and each formula is dualised using negation. The rules *switch*, *fresh* and *new wen* are their own co-rules. Also the co-rule of the *medial new* rule is an instance of the *suspend* rule. All other rules give rise to distinct co-rules, presented in Figure 8. Note co-rules with no role in cut elimination are ommitted from the figure.

The following nine lemmas each establish that a co-rule is admissible in MAV1. Only the following co-rules need be handled directly in order to establish cut elimination: *co-close*, *co-tidy name*, *co-extrude1*, *co-select1*, *co-tidy1*, *co-left*, *co-right*, *co-external*, *co-tidy*, *co-sequence* and *atomic co-interaction*. In each case, the proof proceeds by applying splitting in a shallow context, forming a new proof, and finally applying Lemma 5.2. Each co-rule can be treated independently, hence are established as separate lemmas.

Lemma 5.3 (co-close). *If* $\vdash C\{\ \text{Э}x.P \otimes \text{И}x.Q\ \}$ *holds then* $\vdash C\{\ \text{Э}x.(P \otimes Q)\ \}$ *holds.*

Proof. Assume that $\vdash (\text{Э}x.P \otimes \text{И}x.Q)\sigma \parr R$ for some substitution of terms for variables σ. By Lemma 4.19, there exist S_i and T_i such that $\vdash (\text{Э}x.P)\sigma \parr S_i$ and $\vdash (\text{И}x.Q)\sigma \parr T_i$, for $1 \leq i \leq n$, and n-ary killing context such that the derivation

$$\frac{\mathcal{K}\{\ S_i \parr T_i : 1 \leq i \leq n\ \}}{R}$$

holds. Also for some y such that $y \# \text{Э}x.P$, $y \# \text{И}x.Q$ and $y \# \sigma$, $(\text{Э}x.P)\sigma \equiv \text{Э}y.(P\{{}^{y}\!/_{x}\}\sigma)$ and $(\text{И}x.Q)\sigma \equiv \text{И}y.(Q\{{}^{y}\!/_{x}\}\sigma)$, where $y \# \sigma$ is defined such that y does not appear in the domain of σ nor free in any term in the range of σ. Hence both $\vdash \text{Э}y.(P\{{}^{y}\!/_{x}\}\sigma) \parr S_i$ and $\vdash \text{И}y.(Q\{{}^{y}\!/_{x}\}\sigma) \parr T_i$ hold.

Hence, by Lemma 4.19, there exist U_i and $\hat{U}_i$ such that $\vdash P\{{}^{y}\!/_{x}\}\sigma \parr \hat{U}_i$ and either $U_i = \hat{U}_i$ or $U_i = \text{И}y.\hat{U}_i$, and also the derivation $\frac{U_i}{S_i}$ holds.

Similarly, by Lemma 4.19, there exist W_i and $\hat{W}_i$ such that $\vdash Q\{{}^{y}\!/_{x}\}\sigma \parr \hat{W}_i$ and either $W_i = \hat{W}_i$ or $W_i = \text{Э}y.\hat{W}_i$, and also the derivation $\frac{W_i}{T_i}$ holds.

There are four cases to consider for each i. Three of the cases are as follows.

- If $U_i = \text{И}y.\hat{U}_i$ and $W_i = \text{Э}y.\hat{W}_i$ then

$$\frac{\text{И}y.\left(\hat{U}_i \parr \hat{W}_i\right)}{\text{И}y.\hat{U}_i \parr \text{Э}y.\hat{W}_i}\ .$$

- If $U_i = \hat{U}_i$, $y \# \hat{U}_i$, and $W_i = \text{Э}y.\hat{W}_i$, then

$$\cfrac{\cfrac{\text{И}y.\left(\hat{U}_i \parr \hat{W}_i\right)}{\text{Э}y.\left(\hat{U}_i \parr \hat{W}_i\right)}}{U_i \parr \text{Э}y.\hat{W}_i}\ .$$

- If $U_i = \text{И}y.\hat{U}_i$ and $W_i = \hat{W}_i$, such that $y \# \hat{W}_i$ then

$$\frac{\text{И}y.\left(\hat{U}_i \parr \hat{W}_i\right)}{\text{И}x.U_i \parr \hat{W}_i}\ .$$

Thereby in any of the above three cases the following derivation can be constructed.

$$\begin{array}{c} \text{И}y.\left((P \otimes Q)\{^{y}/_{x}\}\sigma \parr \hat{U}_i \parr \hat{W}_i\right) \\ \hline (\text{Э}x.(P \otimes Q))\sigma \parr \text{И}y.\left(\hat{U}_i \parr \hat{W}_i\right) \\ \hline (\text{Э}x.(P \otimes Q))\sigma \parr U_i \parr W_i \end{array}$$

In the fourth case $U_i = \hat{U}_i$ and $W_i = \hat{W}_i$, such that $y \# \hat{W}_i$ and $y \# \hat{U}_i$ yielding the following.

$$\begin{array}{c} \text{И}y.\left((P \otimes Q)\{^{y}/_{x}\}\sigma \parr \hat{U}_i \parr \hat{W}_i\right) \\ \hline \text{И}y.((P \otimes Q)\{^{y}/_{x}\}\sigma) \parr \hat{U}_i \parr \hat{W}_i \\ \hline (\text{Э}x.(P \otimes Q))\sigma \parr \hat{U}_i \parr \hat{W}_i \end{array}$$

By applying one of the above possible derivations for every i, the following proof can be constructed.

$$\begin{array}{c} \circ \\ \hline \mathcal{K}\{\ \text{И}y.\circ : 1 \leq i \leq n\ \} \\ \hline \mathcal{K}\left\{\ \text{И}y.\left(\left(P\{^{y}/_{x}\}\sigma \parr \hat{U}_i\right) \otimes \left(Q\{^{y}/_{x}\}\sigma \parr \hat{W}_i\right)\right) : 1 \leq i \leq n\ \right\} \\ \hline \mathcal{K}\left\{\ \text{И}y.\left((P \otimes Q)\{^{y}/_{x}\}\sigma \parr \hat{U}_i \parr \hat{W}_i\right) : 1 \leq i \leq n\ \right\} \\ \hline \mathcal{K}\{\ (\text{Э}x.(P \otimes Q))\sigma \parr U_i \parr W_i : 1 \leq i \leq n\ \} \\ \hline (\text{Э}x.(P \otimes Q))\sigma \parr \mathcal{K}\{\ U_i \parr W_i : 1 \leq i \leq n\ \} \\ \hline (\text{Э}x.(P \otimes Q))\sigma \parr \mathcal{K}\{\ S_i \parr T_i : 1 \leq i \leq n\ \} \\ \hline (\text{Э}x.(P \otimes Q))\sigma \parr R \end{array}$$

Therefore, by Lemma 5.2, for all contexts $C\{\ \}$, if $\vdash C\{\ \text{Э}x.P \otimes \text{И}x.Q\ \}$ then $\vdash C\{\ \text{И}x.(P \otimes Q)\ \}$. □

Lemma 5.4 (co-tidy name). *If* $\vdash C\{\ \text{Э}x.\circ\ \}$ *holds then* $\vdash C\{\ \circ\ \}$ *holds.*

Proof. Assume that $\vdash \text{Э}x.\circ \parr P$ holds. By Lemma 4.19, there exists Q such that $\vdash Q$ and $\dfrac{Q}{P}$. Hence the following proof of P can be constructed: $\begin{array}{c}\circ \\ \hline Q \\ \hline P\end{array}$. Therefore, by Lemma 5.2, for any context $C\{\ \}$, if $\vdash C\{\ \text{Э}x.\circ\ \}$ then $\vdash C\{\ \circ\ \}$, as required. □

Lemma 5.5 (co-extrude1). *If* $x \# Q$ *and* $\vdash C\{\ \exists x.P \otimes Q\ \}$ *holds then* $\vdash C\{\ \exists x.(P \otimes Q)\ \}$ *holds.*

Proof. Assume that $\vdash (\exists x.P \otimes Q)\sigma \parr V$ holds, where $x \# Q$. Now, since $y \# (\exists x.P \otimes Q)$ and $y \# \sigma$, we have $(\exists x.P \otimes Q)\sigma \parr V \equiv (\exists y.(P\{^{y}/_{x}\}\sigma) \otimes Q\sigma) \parr V$. So, by Lemma 4.19, there exist T_i and U_i such that $\vdash \exists y.(P\{^{y}/_{x}\}\sigma) \parr T_i$ and $\vdash Q\sigma \parr U_i$, for $1 \leq i \leq n$, and n-ary killing context such that the derivation

$$\begin{array}{c} \mathcal{K}\{\ T_1 \parr U_1, \ldots, T_n \parr U_n\ \} \\ \hline V \end{array}$$

holds. By Lemma 4.20, there exist R^i_j and v^i_j such that $\vdash P\{^{y}/_{x}\}\sigma\left\{^{v^i_j}/_{y}\right\} \parr R^i_j$, for $1 \leq j \leq m_i$, and m_i-ary killing context $\mathcal{K}^i\{\ \}$ such that the derivation

$$\begin{array}{c} \mathcal{K}^i\{\ R^i_1, R^i_2, \ldots, R^i_{m_i}\ \} \\ \hline T_i \end{array}$$

holds. Hence the following proof can be constructed, where we appeal to α-conversion in the conclusion.

$$\begin{array}{c}
\circ \\ \hline
\mathcal{K}\{\, \mathcal{K}^i\{\, \circ : 1 \leq j \leq m_i \,\} : 1 \leq i \leq n \,\} \\ \hline
\mathcal{K}\left\{\, \mathcal{K}^i\left\{\, \left(P\{^y/_x\}\sigma\left\{^{v^i_j}/_y\right\} \parr R^i_j\right) \otimes (Q\sigma \parr U_i) : 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline
\mathcal{K}\left\{\, \mathcal{K}^i\left\{\, \left(P\{^y/_x\}\sigma\left\{^{v^i_j}/_y\right\} \otimes Q\sigma\right) \parr R^i_j \parr U_i : 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline
\mathcal{K}\left\{\, \mathcal{K}^i\left\{\, \exists y.(P\{^y/_x\}\sigma \otimes Q\sigma) \parr R^i_j \parr U_i : 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline
\mathcal{K}\left\{\, \exists y.(P\{^y/_x\}\sigma \otimes Q\sigma) \parr \mathcal{K}^i\left\{\, R^i_j : 1 \leq j \leq m_i \,\right\} \parr U_i : 1 \leq i \leq n \,\right\} \\ \hline
\exists y.(P\{^y/_x\}\sigma \otimes Q\sigma) \parr \mathcal{K}\left\{\, \mathcal{K}^i\left\{\, R^i_j : 1 \leq j \leq m_i \,\right\} \parr U_i : 1 \leq i \leq n \,\right\} \\ \hline
\exists y.(P\{^y/_x\}\sigma \otimes Q\sigma) \parr \mathcal{K}\{\, T_i \parr U_i : 1 \leq i \leq n \,\} \\ \hline
\exists y.(P\{^y/_x\}\sigma \otimes Q\sigma) \parr V
\end{array}$$

Hence, by Lemma 5.2, if $\vdash C\{\, \exists x.P \otimes Q \,\}$, where $x \# Q$, then $\vdash C\{\, \exists x.(P \otimes Q) \,\}$. □

LEMMA 5.6 (CO-TIDY1). *If* $\vdash C\{\, \exists x.\circ \,\}$ *holds then* $\vdash C\{\, \circ \,\}$ *holds.*

Proof. Assume that $\vdash \exists x.\circ \parr T$ holds. By Lemma 4.20, there exists U_i such that $\vdash U_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that $\dfrac{\mathcal{K}\{\, U_1, \ldots, U_n \,\}}{T}$. Hence the following proof of T can be constructed:

$$\begin{array}{c}
\circ \\ \hline
\mathcal{K}\{\, \circ, \ldots, \circ \,\} \\ \hline
\mathcal{K}\{\, U_1, \ldots, U_n \,\} \\ \hline
\circ \parr T
\end{array} .$$

Therefore, by Lemma 5.2, if $\vdash C\{\, \exists x\circ \,\}$ then $\vdash C\{\, \circ \,\}$, as required. □

The above four lemmas are particular to MAV1. The following lemma is proven directly for MAV, similarly to Lemma 4.2; however, for MAV1 the proof is more indirect due to interdependencies between $\&$ and nominals.

LEMMA 5.7 (CO-LEFT AND CO-RIGHT). *If* $\vdash C\{\, P \& Q \,\}$ *holds then both* $\vdash C\{\, P \,\}$ *and* $\vdash C\{\, Q \,\}$ *hold.*

The proofs for the four co-rule elimination lemmas below are similar to the corresponding cases in MAV [23].

LEMMA 5.8 (CO-EXTERNAL). *If* $\vdash C\{\, P \otimes (Q \oplus R) \,\}$ *holds then* $\vdash C\{\, (P \otimes Q) \oplus (P \otimes R) \,\}$ *holds.*

LEMMA 5.9 (CO-SEQUENCE). *If* $\vdash C\{\, (P \lhd Q) \otimes (R \lhd S) \,\}$ *holds then* $\vdash C\{\, (P \otimes R) \lhd (Q \otimes S) \,\}$ *holds.*

LEMMA 5.10 (CO-TIDY). *If* $\vdash C\{\, \circ \oplus \circ \,\}$ *holds, then* $\vdash C\{\, \circ \,\}$ *holds.*

LEMMA 5.11 (ATOMIC CO-INTERACTION). *If* $\vdash C\{\, \alpha \otimes \overline{\alpha} \,\}$ *holds then* $\vdash C\{\, \circ \,\}$ *holds.*

5.3 The proof of cut elimination

The main result of this paper, Theorem 3.3, follows by induction on the structure of P in a formula of the form $\vdash C\left\{\, P \otimes \overline{P} \,\right\}$, by applying the above eight co-rule elimination lemmas and also Lemma 4.2 in the cases for *all* and *some*.

Proof. The base cases for any atom α follows since if $\vdash C\{\ \overline{\alpha} \otimes \alpha\ \}$ then $\vdash C\{\ \circ\ \}$ by Lemma 5.11. The base case for the unit is immediate. As the induction hypothesis in the following cases assume for any context $C\{\ \ \}$, $\vdash C\left\{\ P \otimes \overline{P}\ \right\}$ yields $C\{\ \circ\ \}$ and $\vdash \mathcal{D}\left\{\ Q \otimes \overline{Q}\ \right\}$ yields $\mathcal{D}\{\ \circ\ \}$.

Consider the case for *times*. Assume that $\vdash C\left\{\ P \otimes Q \otimes \left(\overline{P} \parr \overline{Q}\right)\ \right\}$ holds. By the *switch* rule, $\vdash C\left\{\ \left(P \otimes \overline{P}\right) \parr \left(Q \otimes \overline{Q}\right)\ \right\}$ holds. Hence, by the induction hypothesis twice, $\vdash C\{\ \circ\ \}$ holds. The case for *par* is symmetric to the case for *times*.

Consider the case for *seq*. Assuming that $\vdash C\left\{\ (P \triangleleft Q) \otimes \left(\overline{P} \triangleleft \overline{Q}\right)\ \right\}$ holds, by Lemma 5.9, it holds that $\vdash C\left\{\ \left(P \otimes \overline{P}\right) \triangleleft \left(Q \otimes \overline{Q}\right)\ \right\}$. Hence, by the induction hypothesis twice, $\vdash C\{\ \circ\ \}$ holds.

Consider the case for *with*. Assume that $\vdash C\left\{\ (P \mathbin{\&} Q) \otimes \left(\overline{P} \oplus \overline{Q}\right)\ \right\}$ holds. By Lemma 5.8, $\vdash C\left\{\ \left((P \mathbin{\&} Q) \otimes \overline{P}\right) \oplus \left((P \mathbin{\&} Q) \otimes \overline{Q}\right)\ \right\}$ holds. By Lemma 5.7 twice, $\vdash C\left\{\ \left(P \otimes \overline{P}\right) \oplus \left(Q \otimes \overline{Q}\right)\ \right\}$ holds. Hence by the induction hypothesis twice, $\vdash C\{\ \circ \oplus \circ\ \}$ holds. Hence by Lemma 5.10, $\vdash C\{\ \circ\ \}$ holds, as required. The case for *plus* is symmetric to the case for *with*.

Consider the case for universal quantification. Assume that $\vdash C\left\{\ \forall x.P \otimes \exists x.\overline{P}\ \right\}$ holds. By Lemma 5.5, it holds that $\vdash C\left\{\ \exists x.\left(\forall x.P \otimes \overline{P}\right)\ \right\}$, since $x \ \#\ \exists x.P$. By Lemma 4.2, $\vdash C\left\{\ \exists x.\left(P \otimes \overline{P}\right)\ \right\}$ holds. Hence by the induction hypothesis, $\vdash C\{\ \exists x.\circ\ \}$ holds. Hence by Lemma 5.6, $\vdash C\{\ \circ\ \}$ holds, as required. The case for existential quantification is symmetric to the case for universal quantification.

Consider the case for *new*. Assume that $\vdash C\left\{\ \text{И}x.P \otimes \text{Ǝ}x.\overline{P}\ \right\}$ holds. By Lemma 5.3, it holds that $\vdash C\left\{\ \text{Ǝ}x.\left(P \otimes \overline{P}\right)\ \right\}$. Hence by the induction hypothesis, $\vdash C\{\ \text{Ǝ}x.\circ\ \}$ holds. Hence by Lemma 5.4, $\vdash C\{\ \circ\ \}$ holds, as required. The case for *wen* is symmetric to the case for *new*.

Therefore, by induction on the structure of P, if $\vdash C\left\{\ P \otimes \overline{P}\ \right\}$ holds, then $\vdash C\{\ \circ\ \}$ holds. □

Notice that the structure of the above argument is similar to the structure of the argument for Proposition 3.2. The only difference is that the formulae are dualised and co-rule lemmas are applied instead of rules.

5.4 Discussion on alternative presentations of rules for MAV1

Having established cut elimination (Theorem 3.3), an immediate corollary is that all co-rules in Fig. 8 are admissible. This can be formulated by demonstrating that linear implication coincides with the inverse of a derivation in the symmetric system *SMAV1*.

Corollary 5.12. *$\vdash P \multimap Q$ in MAV1 if and only if $\dfrac{P}{Q}$ in SMAV1.*

Proof. Firstly, assume $\vdash P \multimap Q$ in MAV1, in which case the following can be constructed in SMAV1:

$$\dfrac{\dfrac{\dfrac{P}{P \otimes \left(\overline{P} \parr Q\right)}}{\left(P \otimes \overline{P}\right) \parr Q}}{Q}\ .$$

For the converse, assume $\frac{P}{Q}$ in SMAV1; hence

$$\dfrac{\dfrac{\circ}{\overline{P} \parr P}}{\overline{P} \parr Q}$$

can be constructed. Thereby by Lemma 4.2 and Lemmas 5.3 to 5.9, the above derivation in SMAV1 can be transformed into a proof in MAV1. □

The advantage of the definition of linear implication using provability in MAV rather than derivations in SMAV1, is that MAV1 is *analytic* [9]; hence, with some care taken for existential quantifiers [5, 34], each formula gives rise to finitely many derivations up-to congruence. In contrast, in SMAV1, many co-rules can be applied indefinitely. Notice co-rules including *atomic co-interaction*, *co-left* and *co-tidy* can infinitely increase the size of a formula during proof search.

A small rule set. Alternatively, we could extend the structural congruence with the following.

$$\text{Э}x.P \equiv P \text{ only if } x \mathrel{\#} P \qquad \text{И}x.P \equiv P \text{ only if } x \mathrel{\#} P \qquad \text{(vacuous)}$$

Vacuous allows nominals to be defined by the smaller set of rules *close*, *medial new*, *suspend*, *new wen*, *with name*, and *all wen*. Any formula provable in this smaller system is also provable in MAV1, since all rules of MAV1 can be simulated by the rules above. Perhaps the least obvious case is the *fresh* rule, where since $\frac{\text{Э}x.\text{И}x.P}{\text{И}x.\text{Э}x.P}$, by the *new wen* rule and both $\text{Э}x.\text{И}x.P \equiv \text{И}x.P$ and $\text{Э}x.P \equiv \text{И}x.\text{Э}x.P$ hold using the *vacuous* rule, we have $\frac{\text{И}x.P}{\text{Э}x.P}$.

Conversely, *vacuous* is a provable equivalence in MAV1; hence, by inductively applying cut elimination to eliminate each *vacuous* rule in a proof using the smaller set of rules, we can obtain a proof with the same conclusion in MAV1. The disadvantage of the above system is that the *vacuous* rules can introduce an arbitrary number of nominal quantifiers at any stage in the proof leading to infinite paths in proof search, i.e., the above system is not *analytic*. Indeed the multiset-based measure used to guide splitting would not be respected, hence our cut elimination strategy would fail. None the less, the smaller rule set above offers insight into design decisions.

Alternative approaches to cut elimination. Further styles of proof system are possible. For example, again as a consequence of cut elimination, we can show the equivalence of MAV1 and a system which reduces the implicit contraction in the *external* rule to an atomic form $\frac{\alpha \oplus \alpha}{\alpha}$, in which additional medial rules play a central role for propagating contraction [7, 10, 47]. Similarly, the implicit vacuous existential quantifier introduction can be given an explicit atomic treatment [50]. The point is that, although the cut elimination result in this work is sufficient to establish the equivalent expressive power of systems mentioned in this subsection, further proof theoretic insight may be gained by attempting direct proofs of cut elimination in such alternative systems. Indeed a different approach to cut elimination is required for tackling MAV2 with second-order quantifiers.

Note on probabilistic choice. Insight from investigating the proof theory of MAV1 led to the surprising observation that probabilistic choice has similar proof theoretic properties to *new*. A proof theory of MAV extended with *sub-additive* operators is explored in related work [24]. The sub-additives, similarly to nominal quantifiers which lie between universal and existential quantifiers, lie between the traditional additives *with* and *plus*. Sub-additives can either be self-dual, similarly to ∇, or de Morgan dual, similarly to И and Э — controlling distributivity properties which are undesirable when embedding probabilistic processes, much like the quantifiers in this work avoid undesirable distributivity properties when embedding processes with private names.

We remark that adapting recent work on splitting in *subatomic logic* [54] may help explain general patterns emerging, connecting the nominal quantifiers and sub-additives. Subatomic logic

Complexity class	Linear logic	Calculus of structures
NP-complete	MLL1 with functions [30]	BV1 with functions (Proposition 6.3)
PSPACE-complete	MALL1 without functions [33]	MAV1 without functions (Proposition 6.2)
NEXPTIME-complete	MALL1 with functions [34, 36]	MAV1 with functions (Proposition 6.1)
Undecidable	MAELL [33] and MLL2 [35]	NEL [49]

Fig. 9. Complexity results.

may also be used to provide a more concise proof of splitting by exploiting the evident general patterns in the case analysis. Beside abstractly explaining general patterns, the study of MAV1 in terms of subatomic logic would likely expose alternative formulations of the rules of MAV1.

6 DECIDABILITY OF PROOF SEARCH

Here we identify complexity classes for proof search in fragments of MAV1. The hardness results in this section are consequences of cut elimination (Theorem 3.3) and established complexity results for fragments of linear logic and extensions of BV.

NEXPTIME-hardness follows from the NEXPTIME-hardness of MALL1 [34]; while membership in NEXPTIME follows a similar argument as for MALL1 [36] (in a proof there are at most exponentially many *atomic interaction* rules, each involving quadratically bounded terms).

Proposition 6.1. *Deciding provability in MAV1 is NEXPTIME-complete.*

If we restrict terms to a nominal type, i.e. *some* can only be instantiated with variables and constants, we obtain a tighter complexity bound. PSPACE-hardness is a consequence of the PSPACE-hardness of MAV [23], which in turn follows from the PSPACE-hardness of MALL [33]. Membership in PSPACE follows a similar argument as for MALL1 without function symbols [34].

Proposition 6.2. *Deciding provability in MAV1 without function symbols is PSPACE-complete.*

If we consider the sub-system without *with* and *plus*, named BV1, we obtain a tighter complexity bound again, even with function symbols in terms. NP-hardness is a consequence of the NP-hardness of BV [28]; while membership in NP follows a similar argument as for MLL1 [36]

Proposition 6.3. *Deciding provability in BV1 is NP-complete.*

For problems in the complexity class NEXPTIME, we can always check a proof in exponential time. The high worst-case complexity means that proof search in general is considered to be infeasible. Implementations of NEXPTIME-complete problems that regularly work efficiently, include reasoning in description logic $\mathcal{ALCI}(\mathcal{D})$ [37].

Figure 9 summarises complexity results for related calculi. Notice the pattern that each fragment of linear logic has the same complexity as the calculus that is a conservative extension of that fragment of linear logic (with mix), where the extra operator is the self-dual non-commutative operator *seq*. The complexity classes match since the source of the NP-completeness in multiplicative-only linear logic (MLL) lies in the number of ways of partitioning resources (formulae), while the mix rule and sequence rule are also ways of partitioning the same resources.

An exceptional case is that BV extended with exponentials (NEL) is undecidable, whereas the decidability of multiplicative linear logic with exponentials (MELL) is unknown.[2] However, by

[2] MELL was claimed to be decidable in [3], but this was later refuted [51].

including additives to obtain full propositional linear logic (MAELL or simply LL) provability is known to be undecidable.

By the above observations, the complexity of deciding linear implication for embeddings of finite name passing processes, as in π-calculus, is in PSPACE. However, extending to finite value passing processes where terms constructed using function symbols can be communicated, e.g. capturing tuples in the polyadic π-calculus [40], the complexity class increases, but only for processes involving choice. Further extensions to MAV1 introducing second-order quantifiers, exponentials or fixed points would lead to undecidable proof search [32, 35, 49].

7 CONCLUSION

This paper makes two significant contributions to proof theory: the first cut elimination result for a novel de Morgan dual pair of nominal quantifiers; and the first direct cut elimination result for first-order quantifiers in the calculus of structures. As a consequence of cut-elimination (Theorem 3.3), we obtain the first proof system that features both non-commutative operator *seq* and first-order quantifiers $\forall$ and $\exists$. A novelty of the nominal quantifiers И and Э compared to established self-dual nominal quantifiers is in how they distribute over positive and negative operators. This greater control of bookkeeping of names enables private names to be modelled in direct embeddings of processes as formulae in MAV1. In Section 3, every rule in MAV1 is justified as necessary either: for soundly embedding processes; or for ensuring cut elimination holds. Of particular note, some rules were introduced for ensuring cut elimination holds in the presence of *equivariance*.

The cut elimination result is an essential prerequisite for recommending the system MAV1 as a logical system. This paper only hints about formal connections between MAV1 and models of processes, which receives separate attention in a companion paper [26]. In particular, we know that linear implication defines a precongruence over processes embedded as formulae, that is sound with respect to both weak simulation and pomset traces.

Further to connections with process calculi, there are several problems exposed as future work. Regarding the sequent calculus, in the setting of linear logic (i.e., without seq), it is an open problem to determine whether there is a sequent calculus presentation of *new* and *wen*. Regarding model theory, a model theory or game semantics may help to explain the nature of the de Morgan dual pair of nominal quantifiers, although note that it remains an open problem just to establish a sound and complete denotational model of BV. Another open question is whether quantifiers *new* and *wen* are relevant in a classical or intuitionistic setting, or whether these operators are uniquely interesting in a linear setting. Since *new* must distribute over classical disjunction (recall, in contrast, *new* does not distribute over multiplicative disjunction), nominal operators *new* and *wen* likely collapse to an established self-dual nominal operator in the classical setting; hence *wen* is probably unrelated to the 'generous' operator proposed in related work on stratifiable languages [15]. Regarding implementation, it is a challenge to reduce non-determinism in proof search [2, 12, 29]; a problem that can perhaps be tackled by restricting to well-behaved fragments of MAV1 or by exploiting complexity results to embed rules as constraints for a suitable solver. Regarding proof normalisation, systems including classical propositional logic [55], first-order logic [55], intuitionistic logic [20] and NEL (BV with exponentials) [52] satisfy a proof normalisation property called *decomposition* related to interpolation; leading to the question of whether there is an alternative presentation of the rules of MAV1, for which a decomposition result can be established. Finally, an expressivity problem, perhaps related to decomposition, is how to establish cut elimination for second-order extensions suitable for modelling infinite processes.

Acknowledgements. We thank the anonymous reviewers, whose thorough reading led to improvements in the presentation of MAV1.

REFERENCES

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

[2] Jean-Marc Andreoli. Logic programming with focusing proofs in linear logic. *Journal of Logic and Computation*, 2(3):297–347, 1992.

[3] Katalin Bimbó. The decidability of the intensional fragment of classical linear logic. *Theor. Comput. Sci.*, 597(C):1–17, 2015.

[4] Richard Blute, Prakash Panangaden, and Sergey Slavnov. Deep inference and probabilistic coherence spaces. *Applied Categorical Structures*, 20(3):209–228, 2012.

[5] Kai Brünnler. *Deep inference and symmetry in classical proofs*. PhD thesis, TU Dresden, 2003.

[6] Kai Brünnler. Locality for classical logic. *Notre Dame J. Form. Log.*, 47(4):557–580, 2006.

[7] Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In *Logic for Programming, Artificial Intelligence, and Reasoning, 8th International Conference, LPAR 2001, Havana, Cuba, December 3-7, 2001, Proceedings*, pages 347–361, 2001.

[8] Paola Bruscoli. A purely logical account of sequentiality in proof search. In *International Conference on Logic Programming*, volume 2401 of *LNCS*, pages 302–316. Springer, 2002.

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

[10] Paola Bruscoli, Alessio Guglielmi, Tom Gundersen, and Michel Parigot. Quasipolynomial normalisation in deep inference via atomic flows and threshold formulae. *Logical Methods in Computer Science*, 12(2:5), 2016.

[11] Luís Caires, Frank Pfenning, and Bernardo Toninho. Linear logic propositions as session types. *Mathematical Structures in Computer Science*, 26(3):367–423, 2016.

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

[13] Gabriel Ciobanu and Ross Horne. Behavioural analysis of sessions using the calculus of structures. In *International Andrei Ershov Memorial Conference (PSI'15)*, volume 9609 of *LNCS*, pages 91–106. Springer, 2015.

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

[15] Murdoch J. Gabbay. Consistency of quine's new foundations using nominal techniques. arXiv:1406.4060v4, 2016.

[16] Murdoch J Gabbay and Andrew M Pitts. A new approach to abstract syntax with variable binding. *Formal Aspects of Computing*, 13(3):341–363, 2002.

[17] Andrew Gacek, Dale Miller, and Gopalan Nadathur. Nominal abstraction. *Information and Computation*, 209(1):48–73, 2011.

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

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

[20] Nicolas Guenot and Lutz Straßburger. Symmetric normalisation for intuitionistic logic. In *Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 45:1–45:10. ACM, 2014.

[21] Alessio Guglielmi. A system of interaction and structure. *ACM Transactions on Computational Logic*, 8(1), 2007.

[22] Alessio Guglielmi and Lutz Straßburger. A system of interaction and structure V: The exponentials and splitting. *Math. Struct. Comp. Sci.*, 21(03):563–584, 2011.

[23] Ross Horne. The consistency and complexity of multiplicative additive system virtual. *Sci. Ann. Comp. Sci.*, 25(2):245–316, 2015.

[24] Ross Horne. The sub-additives: A proof theory for probabilistic choice extending linear logic. In Herman Geuvers, editor, *In 4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019)*, volume 131, pages 23:1–23:16. Leibniz International Proceedings in Informatics, 2019.

[25] Ross Horne, Sjouke Mauw, and Alwen Tiu. Semantics for specialising attack trees based on linear logic. *Fundamenta Informaticae*, 153(1-2):57–86, 2017.

[26] Ross Horne and Alwen Tiu. Constructing weak simulations from linear implications for processes with private names. *Mathematical Structures in Computer Science*, n.d.:1–34, 2019.

[27] Ross Horne, Alwen Tiu, Bogdan Aman, and Gabriel Ciobanu. Private Names in Non-Commutative Logic. In Josée Desharnais and Radha Jagadeesan, editors, *27th International Conference on Concurrency Theory (CONCUR 2016)*, volume 59 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:16, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

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

[29] Ozan Kahramanoğulları. Interaction and depth against nondeterminism in proof search. *Logical Methods in Computer Science*, 10(2):5:1–5:49, 2014.

[30] Max I Kanovich. The complexity of Horn fragments of linear logic. *Annals of Pure and Applied Logic*, 69(2):195–241, 1994.

[31] Naoki Kobayashi and Akinori Yonezawa. ACL — a concurrent linear logic programming paradigm. In *ILPS'93*, pages 279–294. MIT Press, 1993.

[32] Yves Lafont. The undecidability of second order linear logic without exponentials. *The Journal of Symbolic Logic*, 61(02):541–548, 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 Lincoln and Andre Scedrov. First-order linear logic without modalities is NEXPTIME-hard. *Theoretical Computer Science*, 135(1):139–153, 1994.

[35] Patrick Lincoln, Andre Scedrov, and Natarajan Shankar. Decision problems for second-order linear logic. In *LICS 1995*, pages 476–485. IEEE Computer Society, 1995.

[36] Patrick Lincoln and Natarajan Shankar. Proof search in first-order linear logic and other cut-free sequent calculi. In *LICS'94*, pages 282–291. IEEE, 1994.

[37] Carsten Lutz. NEXPTIME-complete description logics with concrete domains. *ACM Transactions on Computational Logic (TOCL)*, 5(4):669–705, 2004.

[38] Dale Miller and Alwen Tiu. A proof theory for generic judgements. *ACM Transactions on Computational Logic (TOCL)*, 6(4):749–783, 2005.

[39] Robin Milner. *A calculus of communicating systems.* Springer-Verlag New York, Inc., 1982.

[40] Robin Milner. The polyadic π-calculus: a tutorial. In Friedrich Bauer, Wilfried Brauer, and Helmut Schwichtenberg, editors, *Logic and Algebra of Specification*, pages 203–246, 1993.

[41] Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, parts I and II. *Information and computation*, 100(1):1–77, 1992.

[42] Peter O'Hearn and David Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

[43] Andrew Pitts. Nominal logic, a first order theory of names and binding. *Information and Computation*, 186(2):165–193, 2003.

[44] Vaughan Pratt. Modelling concurrency with partial orders. *International Journal of Parallel Programming*, 15(1):33–71, 1986.

[45] Christian Retoré. Pomset logic: A non-commutative extension of classical linear logic. In Philippe de Groote, editor, *TLCA'97*, volume 1210 of *LNCS*, pages 300–318. Springer, 1997.

[46] Luca Roversi. A deep inference system with a self-dual binder which is complete for linear lambda calculus. *J. Log. Comput.*, 26(2):677–698, 2016.

[47] Lutz Straßburger. A local system for linear logic. In Matthias Baaz and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning, 9th International Conference, LPAR 2002, Tbilisi, Georgia, October 14-18, 2002, Proceedings*, volume 2514 of *LNCS*, pages 388–402. Springer, 2002.

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

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

[50] Lutz Straßburger. Some observations on the proof theory of second order propositional multiplicative linear logic. In *TLCA 2009*, volume 5608 of *LNCS*, pages 309–324. Springer, 2009.

[51] Lutz Straßburger. On the decision problem for MELL. *Theor. Comput. Sci.*, 768:91–98, 2019.

[52] Lutz Straßburger and Alessio Guglielmi. A system of interaction and structure IV: the exponentials and decomposition. *ACM Transactions on Computational Logic (TOCL)*, 12(4):23, 2011.

[53] Alwen Tiu. A system of interaction and structure II: The need for deep inference. *Logical Methods in Computer Science*, 2(2:4):1–24, 2006.

[54] Andrea Aler Tubella and Alessio Guglielmi. Subatomic proof systems: Splittable systems. *ACM Trans. Comput. Logic*, 19(1):5:1–5:33, January 2018.

[55] Andrea Aler Tubella, Alessio Guglielmi, and Benjamin Ralph. Removing cycles from proofs. In *CSL 2017*, volume 82 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:17, 2017.

[56] Philip Wadler. Propositions as sessions. *J. of Fun. Prog.*, 24(2-3):384–418, 2014.

A ELECTRONIC APPENDIX

Proposition A.1 (Reflexivity: Proposition 3.2). *For any formula P, $\vdash \overline{P} \parr P$ holds, i.e., $\vdash P \multimap P$.*

Proof. The proof proceeds by induction on the structure of a formula P. The base cases for any atom α follows immediately from the *atomic interaction* rule.The base case for the unit is immediate by definition of a proof. For the following inductive cases assume that $\vdash \overline{P} \parr P$ and $\vdash \overline{Q} \parr Q$ hold.

Consider when the root connective in the formula is the $\otimes$ operator. Observe, by definition, $\overline{(P \otimes Q)} \parr (P \otimes Q) = \overline{P} \parr \overline{Q} \parr (P \otimes Q)$ and by applying the *switch* rule and then the *induction hypothesis* we have the following proof:

$$\dfrac{\dfrac{\circ}{\left(\overline{P} \parr P\right) \otimes \left(\overline{Q} \parr Q\right)}}{\overline{P} \parr \overline{Q} \parr (P \otimes Q)}\ .$$

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

Consider when the root connective in the formula is the *seq* operator. We have, by definition, $\overline{(P \triangleleft Q)} \parr (P \triangleleft Q) = \left(\overline{P} \triangleleft \overline{Q}\right) \parr (P \triangleleft Q)$ and, by applying the *sequence* rule and then the *induction hypothesis*, the following proof holds:

$$\dfrac{\dfrac{\circ}{\left(\overline{P} \parr P\right) \triangleleft \left(\overline{Q} \parr Q\right)}}{\left(\overline{P} \triangleleft \overline{Q}\right) \parr (P \triangleleft Q)}\ .$$

Consider when the root connective in the formula is the *with* operator. By definition we have $\overline{(P \mathbin{\&} Q)} \parr (P \mathbin{\&} Q) = \left(\overline{P} \oplus \overline{Q}\right) \parr (P \mathbin{\&} Q)$ and the following proof holds.

$$\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\circ \mathbin{\&} \circ}\ \text{by } \textit{tidy}}{\left(\overline{P} \parr P\right) \mathbin{\&} \left(\overline{Q} \parr Q\right)}\ \text{by the } \textit{induction hypothesis}}{\left(\left(\overline{P} \oplus \overline{Q}\right) \parr P\right) \mathbin{\&} \left(\left(\overline{P} \oplus \overline{Q}\right) \parr Q\right)}\ \text{by the } \textit{left} \text{ and } \textit{right} \text{ rules}}{\left(\overline{P} \oplus \overline{Q}\right) \parr (P \mathbin{\&} Q)}\ \text{by the } \textit{external} \text{ rule}$$

The case for when *plus*, $\oplus$, is the root connective is symmetric to the case for *with*.

Consider when the root connective in the formula is $\forall$. By definition, $\overline{\forall x.P} \parr \forall x.P = \exists x.\overline{P} \parr \forall x.P$ and the following proof holds:

$$\dfrac{\dfrac{\dfrac{\dfrac{\circ}{\forall x.\circ}\ \text{by the } \textit{tidy1} \text{ rule}}{\forall x.\left(\overline{P} \parr P\right)}\ \text{by the } \textit{induction hypothesis}}{\forall x.\left(\exists x.\overline{P} \parr P\right)}\ \text{by the } \textit{select1} \text{ rule}}{\exists x.\overline{P} \parr \forall x.P}\ \text{by the } \textit{extrude1} \text{ rule}$$

The case for when $\exists$ is the root connective is symmetric to the case for $\forall$.

Consider when the root connective in the formula is И. By definition $\overline{\text{И}x.P} \parr \text{И}x.P = \text{Э}x.\overline{P} \parr \text{И}x.P$ and the following proof holds:

$$\dfrac{\dfrac{\dfrac{\circ}{\text{И}x.\circ}\ \text{by the \textit{tidy name} rule}}{\text{И}x.\left(\overline{P} \parr P\right)}\ \text{by the \textit{induction hypothesis}}}{\text{Э}x.\overline{P} \parr \text{И}x.P}\ \text{by the \textit{close} rule}$$

The case for when the root connective is Э is symmetric to the case for И.

Hence, by induction on the number of connectives in the formula, reflexivity holds. □

Lemma A.2 (Universal: Lemma 4.2). *If* $\vdash C\{\ \forall x.P\ \}$ *holds then, for all terms* v, $\vdash C\{\ P\{^{v}\!/_{x}\}\ \}$ *holds.*

Proof. We require a function over formulae $s_v(T)$ that replaces a certain universal quantifier in T with a substitution for a value v. The universal quantifiers to be replaced are highlighted in bold $\boldsymbol{\forall}$. Note that during a proof the bold operator may be duplicated by the *external* rule and *medial1* rule, hence there may be multiple bold occurrences in a formula. The function is defined as follows, where $\odot \in \{\lhd, \parr, \otimes, \oplus, \&\}$ is any binary connective, $\text{Ծ} \in \{\forall, \exists, \text{И}, \text{Э}\}$ is any quantifier except bold universal quantification and $\kappa \in \{\alpha, \overline{\alpha}, \circ\}$ is any constant or atom.

$$s_v(\boldsymbol{\forall}x.T) = s_v(T\{^{v}\!/_{x}\}) \qquad s_v\left(\text{Ծ}x.T\right) = \text{Ծ}x.s_v(T) \qquad s_v(T \odot U) = s_v(T) \odot s_v(U) \qquad s_v(\kappa) = \kappa$$

In what follows we use that $s_v(C\{\ U\ \}) = C'\{\ s_v(U')\ \}$, for some context $C\{\ \}$ and U' such that $C'\{\ \}$ is obtained from $C\{\ \}$ by applying the s_v function and U' is obtained by substituting free variables in U, that are bound by $\boldsymbol{\forall}$ quantifiers in the context $C\{\ \}$, with v.

We shall prove a stronger statement in the following: for every R, if $\vdash R$ holds then for all terms v, $\vdash s_v(R)$ holds.

Without loss of generality, we can assume that the bound and the free variables in R are pairwise distinct and that the bound variables in R are also distinct from the variables in v. This simplifies the proof below since substitutions of $\boldsymbol{\forall}$-quantified variables commute with other connectives and quantifiers in R.

For the base case, $s_v(R) = R$, in which case trivially if $\vdash R$ then $\vdash s_v(R)$, for example where $R \equiv \circ$.

Consider the case when the bottommost rule in a proof is an instance of the *extrude1* rule involving a bold universal quantifier, as follows, $\dfrac{C\{\ \boldsymbol{\forall}x.(T \parr U)\ \}}{C\{\ \boldsymbol{\forall}x.T \parr U\ \}}$, where $x \# U$ and $\vdash C\{\ \boldsymbol{\forall}x.(T \parr U)\ \}$.

By the induction hypothesis, $\vdash s_v(C\{\ \boldsymbol{\forall}x.(T \parr U)\ \})$ holds. Now the following equalities hold.

$$\begin{aligned} s_v(C\{\ \boldsymbol{\forall}x.(T \parr U)\ \}) &= C'\{\ s_v((T' \parr U')\{^{v}\!/_{x}\})\ \} \\ &= C'\{\ s_v(T'\{^{v}\!/_{x}\}) \parr s_v(U')\ \} \\ &= s_v(C\{\ \boldsymbol{\forall}x.T \parr U\ \}) \end{aligned}$$

Hence $\vdash s_v(C\{\ \boldsymbol{\forall}x.T \parr U\ \})$ holds as required.

Consider the case where the bottommost rule of a proof is an instance of the *tidy1* rule of the form $\dfrac{C\{\ \circ\ \}}{C\{\ \boldsymbol{\forall}x.\circ\ \}}$, where $\vdash C\{\ \circ\ \}$ holds. By the induction hypothesis, $\vdash s_v(C\{\ \circ\ \})$ holds. Since $s_v(C\{\ \boldsymbol{\forall}x.\circ\ \}) = s_v(C\{\ \circ\ \})$, we have $\vdash s_v(C\{\ \boldsymbol{\forall}x.\circ\ \})$ holds, as required.

Consider the case where the bottommost rule of a proof is an instance of the *all name* rule of the form $\dfrac{C\{\ \text{Э}y.\boldsymbol{\forall}x.P\ \}}{C\{\ \boldsymbol{\forall}x.\text{Э}y.P\ \}}$, where $\vdash C\{\ \text{Э}y.\boldsymbol{\forall}x.P\ \}$ holds. By the induction hypothesis, $\vdash s_v\ (C\{\ \text{Э}y.\boldsymbol{\forall}x.P\ \})$ holds. Observe that the following equalities hold, by definition of function s_v.

$$s_v(C\{\ \boldsymbol{\forall}x.\text{Э}y.P\ \}) = C'\{\ s_v((\text{Э}y.P')\{^{v}\!/_{x}\})\ \} = C'\{\ \text{Э}y.s_v(P'\{^{v}\!/_{x}\})\ \} = s_v(C\{\ \text{Э}y.\boldsymbol{\forall}x.P\ \})$$

Hence $\vdash s_v(C\{\ \exists y.\boldsymbol{\forall} x.P\ \})$ holds, as required. The case where *all name* involves *new* is similar.

Consider the case when the bottommost rule does not involve a bold universal quantifier. We show here one instance where the rule involved is *extrude1*; the other cases are similar. So suppose the bottommost rule instance is

$$\frac{C\{\ \forall x.(T \parr U)\ \}}{C\{\ \forall x.T \parr U\ \}}\ .$$

By the induction hypothesis, $\vdash s_v(C\{\ \forall x.(T \parr U)\ \})$. So, since

$$s_v(C\{\ \forall x.(T \parr U)\ \}) = C'\{\ \forall x.(s_v(T') \parr s_v(U'))\ \}$$

we have $\vdash C'\{\ \forall x.(s_v(T') \parr s_v(U'))\ \}$ also holds. Hence, since

$$s_v(C\{\ \forall x.T \parr U\ \}) = C'\{\ \forall x.s_v(T') \parr s_v(U')\ \}$$

and

$$\frac{C'\{\ \forall x.(s_v(T') \parr s_v(U'))\ \}}{C'\{\ \forall x.s_v(T') \parr s_v(U')\ \}}$$

we have $\vdash s_v(C\{\ \forall x.T \parr U\ \})$ holds, as required.

The statement of the lemma is then a special case of the stronger statement established by induction. If $\vdash C\{\ \boldsymbol{\forall} x.T\ \}$, where no further bold universal quantifiers occur in the context, then $\vdash C\{\ T\{^{v}\!/_{x}\}\ \}$ holds, since in such a scenario $s_v(C\{\ \boldsymbol{\forall} x.T\ \}) = C\{\ T\{^{v}\!/_{x}\}\ \}$. □

Lemma A.3 (Lemma 4.5). *Assume that I is a finite subset of natural numbers, P_i and Q_i are formulae, for $i \in I$, and $\mathcal{K}\{\ \}$ is a killing context. There exist killing contexts $\mathcal{K}^0\{\ \}$ and $\mathcal{K}^1\{\ \}$ and sets of natural numbers $J \subseteq I$ and $K \subseteq I$ such that the following derivation holds:* $\dfrac{\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \lhd \mathcal{K}^1\{\ Q_k : k \in K\ \}}{\mathcal{K}\{\ P_i \lhd Q_i : i \in I\ \}}$.

Proof. Proceed by induction on the structure of the killing context. The base case is immediate.

Consider a predicate of the form $Иx.\mathcal{K}\{\ P_i \lhd Q_i : i \in I\ \}$. By the induction hypothesis, assume there exists $\mathcal{K}^0\{\ \}$ and $\mathcal{K}^1\{\ \}$ such that

$$\frac{\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \lhd \mathcal{K}^1\{\ Q_k : k \in K\ \}}{\mathcal{K}\{\ P_i \lhd Q_i : i \in I\ \}}$$

where $J \subseteq I$ and $K \subseteq I$. There are three cases to consider.

If $\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \equiv \circ$, then we have derivation

$$\cfrac{\cfrac{Иx.(\circ \lhd \mathcal{K}^1\{\ Q_k : k \in K\ \})}{\circ \lhd Иx.\mathcal{K}^1\{\ Q_k : k \in K\ \}}\ \text{by using} \equiv}{Иx.\mathcal{K}\{\ P_i \lhd Q_i : i \in I\ \}}\ .$$

If $\mathcal{K}^1\{\ Q_k : k \in K\ \} \equiv \circ$, then we have derivation

$$\cfrac{\cfrac{Иx.(\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \lhd \circ)}{Иx.\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \lhd \circ}\ \text{using} \equiv}{Иx.\mathcal{K}\{\ P_i \lhd Q_i : i \in I\ \}}\ .$$

Otherwise, $\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \not\equiv \circ$ and $\mathcal{K}^1\{\ Q_k : k \in K\ \} \not\equiv \circ$ in which case the *medial new* rule can be applied as follows:

$$\cfrac{\cfrac{Иx.\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \lhd Иx.\mathcal{K}^1\{\ Q_k : k \in K\ \}}{Иx.(\mathcal{K}^0\left\{\ P_j : j \in J\ \right\} \lhd \mathcal{K}^1\{\ Q_k : k \in K\ \})}\ \text{by the } \textit{medial new} \text{ rule}}{Иx.\mathcal{K}\{\ P_i \lhd Q_i : i \in I\ \}}\ .$$

In each of the three cases above, killing contexts of the correct form are obtained. The arguments in the cases of universal quantifiers and with follow a similar pattern. □

Lemma A.4 (Affine: Lemma 4.18). *Any derivation* $\frac{P}{Q}$, *is bound such that* $|P| \leq |Q|$.

Proof. The proof proceeds by checking that each rule preserves the bound on the size of the formula, from which the result follows by induction on the length of a derivation.

Consider the case of the *close* rule. $|\text{И}x.P \parr \text{Э}x.Q|_{occ} = |P|_{occ} \boxplus |Q|_{occ} = |\text{И}x.(P \parr Q)|_{occ}$, since $P \not\equiv \circ$ and $Q \not\equiv \circ$, and $|\text{И}x.P \parr \text{Э}x.Q|_{\text{Э}} = |P|_{\text{Э}} + \left(1 + |Q|_{\text{Э}}\right) > |P|_{\text{Э}} + |Q|_{\text{Э}} = |\text{И}x.(P \parr Q)|_{\text{Э}}$.

Consider the case of the *fresh* rule. For the occurrence count, $|\text{Э}x.P|_{occ} = |\text{И}x.P|_{occ}$ and the wen count strictly decreases as follows: $|\text{Э}x.P|_{\text{Э}} = 1 + |P|_{\text{Э}} > |P|_{\text{Э}} = |\text{И}x.P|_{\text{Э}}$.

Consider the case of the *extrude new* rule, where $Q \not\equiv \circ$. If $P \equiv \circ$, then the occurence count is such that $|\text{И}x.P \parr Q|_{occ} = \{\{0, 0\}\} \boxplus |Q|_{occ} > |Q|_{occ} = |\text{И}x.(P \parr Q)|_{occ}$. If however $P \not\equiv \circ$, then $|\text{И}x.P \parr Q|_{occ} = |P|_{occ} \boxplus |Q|_{occ} = |\text{И}x.(P \parr Q)|_{occ}$. Furthermore, for the new count, the following inequality holds: $|\text{И}x.P \parr Q|_{\text{И}} = (1 + |P|_{\text{И}})\, |Q|_{\text{И}} \geq 1 + |P|_{\text{И}}|Q|_{\text{И}} = |\text{И}x.(P \parr Q)|_{\text{И}}$.

Consider the case of the *external* rule, where $R \not\equiv \circ$. For the occurrence count, by distributivity of $\sqcup$ over $\boxplus$, the following multiset equality holds:

$$\begin{aligned} |(P \mathbin{\&} Q) \parr R|_{occ} &= \left(|P|_{occ} \sqcup |Q|_{occ}\right) \boxplus |R|_{occ} \\ &= (|P|_{occ} \boxplus |R|_{occ}) \sqcup \left(|Q|_{occ} \boxplus |R|_{occ}\right) \\ &= |(P \parr R) \mathbin{\&} (Q \parr R)|_{occ} \end{aligned}$$

For the wen count

$$|(P \mathbin{\&} Q) \parr R|_{\text{Э}} = \left(|P|_{\text{Э}} + |Q|_{\text{Э}}\right) |R|_{\text{Э}} = |P|_{\text{Э}}|R|_{\text{Э}} + |Q|_{\text{Э}}|R|_{\text{Э}} = |(P \parr R) \mathbin{\&} (Q \parr R)|_{\text{Э}}$$

and similarly for the new count.

Consider the case of the *suspend* rule, where $P \not\equiv \circ$ and $Q \not\equiv \circ$. For the occurrence count, $|\text{Э}x.P \triangleleft \text{Э}x.Q|_{occ} = |P|_{occ} \uplus |Q|_{occ} = |\text{Э}x.(P \triangleleft Q)|_{occ}$ and $|\text{Э}x.P \parr \text{Э}x.Q|_{occ} = |P|_{occ} \boxplus |Q|_{occ} = |\text{Э}x.(P \parr Q)|_{occ}$ for *par* and *seq* respectively. For the wen count for either operator, $\odot \in \{\parr, \triangleleft\}$, the following strict inequality holds, noting $|P|_{\text{Э}} \geq 1$ for any formula:

$$|\text{Э}x.P \odot \text{Э}x.Q|_{\text{Э}} = (1 + |P|_{\text{Э}}) \left(1 + |Q|_{\text{Э}}\right) = |P|_{\text{Э}} + |P|_{\text{Э}}|Q|_{\text{Э}} + |Q|_{\text{Э}} > 1 + |P|_{\text{Э}}|Q|_{\text{Э}} = |\text{Э}x.(P \triangleleft Q)|_{\text{Э}}$$

Consider the case of the *left wen* rules, where $x \# Q$ and $Q \not\equiv \circ$. For the occurrence count, there are four cases covering the operators *seq* and *par*.

- If $P \equiv \circ$ then, for *seq*: $|\text{Э}x.(P \triangleleft Q)|_{occ} = |Q|_{occ} \sqsubset \{\{0, 0\}\} \uplus |Q|_{occ} = |\text{Э}x.P \triangleleft Q|_{occ}$.
- If $P \not\equiv \circ$ then, for *seq*: $|\text{Э}x.P \triangleleft Q|_{occ} = |P|_{occ} \uplus |Q|_{occ} = |\text{Э}x.(P \triangleleft Q)|_{occ}$.
- If $P \equiv \circ$ then for *par*: $|\text{Э}x.(P \parr Q)|_{occ} = |Q|_{occ} \sqsubset \{\{0, 0\}\} \boxplus |Q|_{occ} = |\text{Э}x.P \parr Q|_{occ}$.
- If $P \not\equiv \circ$ then for *par*: $|\text{Э}x.P \parr Q|_{occ} = |P|_{occ} \boxplus |Q|_{occ} = |\text{Э}x.(P \parr Q)|_{occ}$.

For the wen count $|\text{Э}x.P \odot Q|_{\text{Э}} = (1 + |P|_{\text{Э}})\, |Q|_{\text{Э}} = |Q|_{\text{Э}} + |P|_{\text{Э}}|Q|_{\text{Э}} \geq 1 + |P|_{\text{Э}}|Q|_{\text{Э}} = |\text{Э}x.(P \odot Q)|_{\text{Э}}$ holds, for $\odot \in \{\parr, \triangleleft\}$. Also, for the new count $|\text{Э}x.P \triangleleft Q|_{\text{И}} = \max\left(|P|_{\text{И}}, |Q|_{\text{И}}\right) = |\text{Э}x.(P \triangleleft Q)|_{\text{И}}$ and $|\text{Э}x.P \parr Q|_{\text{И}} = |P|_{\text{И}}|Q|_{\text{И}} = |\text{Э}x.(P \parr Q)|_{\text{И}}$. The case *right wen* follows a symmetric argument.

Consider the case for the *extrude* rule, where $Q \not\equiv \circ$. $|\forall x.(P \parr Q)|_{occ} \sqsubset |\forall x.P \parr Q|_{occ}$ by the following: $\{\{0\}\} \sqcup \left(|P|_{occ} \boxplus |Q|_{occ}\right) \sqsubset \left(\{\{0\}\} \boxplus |Q|_{occ}\right) \sqcup \left(|P|_{occ} \boxplus |Q|_{occ}\right) = (\{\{0\}\} \sqcup |P|_{occ}) \boxplus |Q|_{occ}$.

Consider the case for the *medial1* rule, where $P \not\equiv \circ$ and $Q \not\equiv \circ$. By distributivity of $\uplus$ over $\sqcup$, $|\forall x.(P \triangleleft Q)|_{occ} = \{\{0\}\} \sqcup \left(|P|_{occ} \uplus |Q|_{occ}\right) = (\{\{0\}\} \sqcup |P|_{occ}) \uplus \left(\{\{0\}\} \sqcup |Q|_{occ}\right) = |\forall x.P \triangleleft \forall x.Q|_{occ}$. Also $|\forall x.(P \triangleleft Q)|_{\text{Э}} = |\forall x.P \triangleleft \forall x.Q|_{\text{Э}}$ and $|\forall x.(P \triangleleft Q)|_{\text{И}} = |\forall x.P \triangleleft \forall x.Q|_{\text{И}}$.

For the *select* rule, $|\exists x.P|_{occ} = \{\{0\}\} \sqcup |P|_{occ} \sqsubset |P|_{occ} = \left|P\{{}^{t}\!/_{x}\}\right|_{occ}$, by Lemma 4.16.

Consider the case for the *switch* rule, where $P \not\equiv \circ$ and $R \not\equiv \circ$. If $Q \not\equiv \circ$, then, since $R \not\equiv \circ$ we have $\{\{0\}\} \sqsubset |R|_{occ}$ and hence $|P|_{occ} = |P|_{occ} \boxplus \{\{0\}\} \sqsubset |P|_{occ} \boxplus |R|_{occ}$; and therefore the following holds since $\uplus$ distributes over $\boxplus$.

$$\begin{aligned} |P \otimes (Q \parr R)|_{occ} &= |P|_{occ} \uplus \left(|Q|_{occ} \boxplus |R|_{occ}\right) \\ &\sqsubset (|P|_{occ} \boxplus |R|_{occ}) \uplus \left(|Q|_{occ} \boxplus |R|_{occ}\right) \\ &= \left(|P|_{occ} \uplus |Q|_{occ}\right) \boxplus |R|_{occ} = |(P \otimes Q) \parr R|_{occ} \end{aligned}$$

If $Q \equiv \circ$ then, since $\{\{0\}\} \sqsubset |P|_{occ}$ and $\{\{0\}\} \sqsubset |R|_{occ}$, the following hold.

$$|P \otimes (\circ \parr R)|_{occ} = |P|_{occ} \uplus |R|_{occ} \sqsubset |P|_{occ} \boxplus |R|_{occ} = |(P \otimes \circ) \parr R|_{occ}$$

Consider the case of the *sequence* rule, where $P \not\equiv \circ$ and $S \not\equiv \circ$. If $Q \not\equiv \circ$ and $R \not\equiv \circ$, then the following holds since $\uplus$ distributes over $\boxplus$.

$$\begin{aligned} |(P \parr R) \triangleleft (Q \parr S)|_{occ} &= (|P|_{occ} \boxplus |R|_{occ}) \uplus \left(|Q|_{occ} \boxplus |S|_{occ}\right) \\ &\sqsubset (|P|_{occ} \boxplus |R|_{occ}) \uplus \left(|Q|_{occ} \boxplus |S|_{occ}\right) \uplus (|P|_{occ} \boxplus |S|_{occ}) \uplus \left(|Q|_{occ} \boxplus |R|_{occ}\right) \\ &= \left(|P|_{occ} \uplus |Q|_{occ}\right) \boxplus (|R|_{occ} \uplus |S|_{occ}) = |(P \triangleleft Q) \parr (R \parr S)|_{occ} \end{aligned}$$

If $Q \equiv \circ$ and $R \not\equiv \circ$, then, since $\{\{0\}\} \sqsubset |R|_{occ}$, and hence $|S|_{occ} = |S|_{occ} \boxplus \{\{0\}\} \sqsubset |S|_{occ} \boxplus |R|_{occ}$, therefore since $\uplus$ distributes over $\boxplus$.

$$\begin{aligned} |(P \parr R) \triangleleft (\circ \parr S)|_{occ} = (|P|_{occ} \boxplus |R|_{occ}) \uplus |S|_{occ} &\sqsubset (|P|_{occ} \boxplus |R|_{occ}) \uplus (|P|_{occ} \boxplus |S|_{occ}) \\ &= |P|_{occ} \boxplus (|R|_{occ} \uplus |S|_{occ}) = |(P \triangleleft \circ) \parr (R \parr S)|_{occ} \end{aligned}$$

A symmetric argument holds when $Q \not\equiv \circ$ and $R \equiv \circ$.

If $Q \equiv \circ$ and $R \equiv \circ$, then $\{\{0\}\} \sqsubset |P|_{occ}$ and $\{\{0\}\} \sqsubset |S|_{occ}$; hence the following strict inequality holds: $|(P \parr \circ) \triangleleft (\circ \parr S)|_{occ} = |P|_{occ} \uplus |S|_{occ} \sqsubset |P|_{occ} \boxplus |S|_{occ} = |(P \triangleleft \circ) \parr (\circ \triangleleft S)|_{occ}$.

Consider the case of the *medial new* rule where $P \not\equiv \circ$ and $Q \not\equiv \circ$. For the occurrence count the equality $|\text{И}x.(P \triangleleft Q)|_{occ} = |P|_{occ} \boxplus |Q|_{occ} = |\text{И}x.P \triangleleft \text{И}x.Q|_{occ}$ holds. For the wen count, $|\text{И}x.(P \triangleleft Q)|_{\text{Э}} = |P|_{\text{Э}}|Q|_{\text{Э}} = |\text{И}x.P \triangleleft \text{И}x.Q|_{\text{Э}}$. For the new count the following equality holds: $|\text{И}x.(P \triangleleft Q)|_{\text{И}} = 1 + \max\left(|P|_{\text{И}}, |Q|_{\text{И}}\right) = \max\left(1 + |P|_{\text{И}}, 1 + |Q|_{\text{И}}\right) = |\text{И}x.P \triangleleft \text{И}x.Q|_{\text{И}}$.

Consider the case for the *medial* rule, where either $P \not\equiv \circ$ or $R \not\equiv \circ$ and also either $Q \not\equiv \circ$ or $S \not\equiv \circ$. When all of P, Q, R and S are not equivalent to the unit, we have the following.

$$\begin{aligned} |(P \mathbin{\&} R) \triangleleft (Q \mathbin{\&} S)|_{occ} &= (|P|_{occ} \sqcup |R|_{occ}) \uplus \left(|Q|_{occ} \sqcup |S|_{occ}\right) \\ &\sqsubset (|P|_{occ} \sqcup |R|_{occ}) \uplus \left(|Q|_{occ} \sqcup |S|_{occ}\right) \uplus (|P|_{occ} \sqcup |S|_{occ}) \uplus \left(|Q|_{occ} \sqcup |R|_{occ}\right) \\ &= \left(|P|_{occ} \uplus |Q|_{occ}\right) \sqcup (|R|_{occ} \uplus |S|_{occ}) = |(P \triangleleft Q) \mathbin{\&} (R \triangleleft S)|_{occ} \end{aligned}$$

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 $S \equiv \circ$ (and possibly also $Q \equiv \circ$, but $R \not\equiv \circ$). By distributivity of $\uplus$ over $\sqcup$ the following holds.

$$\begin{aligned} |(P \mathbin{\&} R) \triangleleft (Q \mathbin{\&} \circ)|_{occ} &= (|P|_{occ} \sqcup |R|_{occ}) \uplus \left(|Q|_{occ} \sqcup \{\{0\}\}\right) \\ &\sqsubset (|P|_{occ} \sqcup |R|_{occ}) \uplus \left(|Q|_{occ} \sqcup |R|_{occ}\right) \\ &= \left(|P|_{occ} \uplus |Q|_{occ}\right) \sqcup |R|_{occ} = |(P \triangleleft Q) \mathbin{\&} (R \triangleleft \circ)|_{occ} \end{aligned}$$

There is one more form of case to consider for the medial: either $P \not\equiv \circ$, $Q \equiv \circ$, $R \equiv \circ$ and $S \not\equiv \circ$; or $P \equiv \circ$, $Q \not\equiv \circ$, $R \not\equiv \circ$ and $S \equiv \circ$. We consider only the former case. The later case, can be treated symmetrically. Since $P \not\equiv \circ$ and $S \not\equiv \circ$, $\{\{0\}\} \sqsubset |P|_{occ}$ and $\{\{0\}\} \sqsubset |S|_{occ}$. Therefore, $|P|_{occ} \sqcup \{\{0\}\} \sqsubset |P|_{occ} \sqcup |S|_{occ}$ and $|Q|_{occ} \sqcup \{\{0\}\} \sqsubset |P|_{occ} \sqcup |S|_{occ}$. Hence, we have established that $(|P|_{occ} \sqcup \{\{0\}\}) \uplus \left(|Q|_{occ} \sqcup \{\{0\}\}\right) \sqsubset |P|_{occ} \sqcup |S|_{occ}$. Note that the restriction on the *medial* rule, either $P \not\equiv \circ$ or $R \not\equiv \circ$ and also either $Q \not\equiv \circ$ or $S \not\equiv \circ$, excludes any further cases. Hence we have established that $|(P \mathbin{\&} R) \triangleleft (Q \mathbin{\&} S)|_{occ} \sqsubset |(P \triangleleft Q) \mathbin{\&} (R \triangleleft S)|_{occ}$.

For the *with name* rule $\left|\mho x.P \mathbin{\&} \mho x.Q\right|_{occ} = |P|_{occ} \sqcup |Q|_{occ} = \left|\mho x.(P \mathbin{\&} Q)\right|_{occ}$, where $\mho \in \{\text{И}, \text{Э}\}$. For the new count $|\text{И}x.P \mathbin{\&} \text{И}x.Q|_{\text{И}} = 2 + |P|_{\text{И}} + |Q|_{\text{И}} > 1 + |P|_{\text{И}} + |Q|_{\text{И}} = |\text{И}x.(P \mathbin{\&} Q)|_{\text{И}}$ and

$|\text{Ǝ}x.P \mathbin{\&} \text{Ǝ}x.Q|_{\text{И}} = |\text{Ǝ}x.(P \mathbin{\&} Q)|_{\text{И}}$. Similarly, $|\text{Ǝ}x.P \mathbin{\&} \text{Ǝ}x.Q|_{\text{Э}} > |\text{Ǝ}x.(P \mathbin{\&} Q)|_{\text{Э}}$. For *left name*, *right name* and *all name*, the size of formulae are invariant.

The cases for the rules *tidy*, *tidy name*, *left*, *right*, *atomic interact* are established by the following inequalities: $|\circ|_{occ} \sqsubset |\circ \mathbin{\&} \circ|_{occ}$, $|\circ|_{occ} \sqsubset |\text{И}x.\circ|_{occ}$, $|\circ|_{occ} \sqsubset |\overline{a} \parr a|_{occ}$, $|P|_{occ} \sqsubset |P \oplus Q|_{occ}$ and $|Q|_{occ} \sqsubset |P \oplus Q|_{occ}$.

Hence the lemma holds by induction on the length of the derivation. □

Lemma A.5 (Lemma 4.20). *If* $\vdash \exists x.P \parr Q$, *then there exist formulae* V_i *and values* v_i *such that* $\vdash P\{^{v_i}\!/_{x}\} \parr V_i$, *where* $1 \leq i \leq n$, *and* n*-ary killing context* $\mathcal{K}\{\ \}$ *such that* $\dfrac{\mathcal{K}\{\, V_1, V_2, \ldots, V_n \,\}}{Q}$ *and if* $\mathcal{K}\{\ \}$ *binds* y *then* $y \mathrel{\#} (\exists x.P)$.

Proof. The proof proceeds by induction on the size of the proof in Definition 4.15, until the principal *exists* operator is removed from the proof, according to the base case. In the base case, the bottommost rule in a proof is an instance of the *select* rule of the form $\dfrac{T\{^{v}\!/_{x}\} \parr U}{\exists x.T \parr U}$, where $\vdash T\{^{v}\!/_{x}\} \parr V$ holds; hence splitting is immediately satisfied. As in every splitting lemma, there are commutative cases for *new*, *wen*, *all*, *with*, *times* and two for *seq*.

Consider the commutative case induced by the *external* rule. The bottommost rule is the form

$$\frac{(\exists x.T \parr U \parr W \mathbin{\&} \exists x.T \parr V \parr W) \parr P}{\exists x.T \parr (U \mathbin{\&} V) \parr W \parr P}$$

where it holds that $\vdash ((\exists x.T \parr U \parr W) \mathbin{\&} (\exists x.T \parr V \parr W)) \parr P$. By Lemma 4.19, $\vdash \exists x.T \parr U \parr W \parr P$ and $\vdash \exists x.T \parr V \parr W \parr P$; and furthermore $|\exists x.T \parr U \parr W \parr P| \sqsubset |\exists x.T \parr (U \mathbin{\&} V) \parr W \parr P|$ and $|\exists x.T \parr V \parr W \parr P| \sqsubset |\exists x.T \parr (U \mathbin{\&} V) \parr W \parr P|$ hold. Hence, by the induction hypothesis, there exist Q_i and u_i such that $\vdash T\{^{u_i}\!/_{x}\} \parr Q_i$, for $1 \leq i \leq m$, and R_j and v_j such that $\vdash T\{^{v_j}\!/_{x}\} \parr R_j$, for $1 \leq j \leq n$; and m-ary and n-ary killing contexts $\mathcal{K}^0\{\ \}$ and $\mathcal{K}^1\{\ \}$ such that the derivations (1) and (2) below hold.

$$\underset{(1)}{\frac{\mathcal{K}^0\{\, Q_1, \ldots, Q_m \,\}}{U \parr W \parr P}} \qquad \underset{(2)}{\frac{\mathcal{K}^1\{\, R_1, \ldots, R_n \,\}}{V \parr W \parr P}} \qquad \underset{(3)}{\frac{\dfrac{\mathcal{K}^0\{\, Q_1, \ldots, Q_m \,\} \mathbin{\&} \mathcal{K}^1\{\, R_1, \ldots, R_n \,\}}{(U \parr W \parr P) \mathbin{\&} (V \parr W \parr P)}}{(U \mathbin{\&} V) \parr W \parr P}}$$

Thus the derivation (3) above can be constructed. Notice that $\mathcal{K}^0\{\ \} \mathbin{\&} \mathcal{K}^1\{\ \}$ is an $m+n$-ary killing context, as required.

Consider the commutative case induced by the *extrude1* rule. In this case, the bottommost rule is

$$\frac{\forall y.(\exists x.T \parr U \parr V) \parr W}{\exists x.T \parr \forall y.U \parr V \parr W}$$

assuming $y \mathrel{\#} (\exists x.T \parr V)$ where $\vdash \forall y.(\exists x.T \parr U \parr V) \parr W$ holds. By Lemma 4.2, for every variable z, $\vdash (\exists x.T \parr U \parr V)\left\{^{z}\!/_{y}\right\} \parr W$ holds. Furthermore, by definition of substitution $(\exists x.T \parr U \parr V)\left\{^{z}\!/_{y}\right\} \parr W \equiv \exists x.T \parr U\left\{^{z}\!/_{y}\right\} \parr V \parr W$, since $y \mathrel{\#} (\exists x.T \parr V)$. Now observe the strict multiset inequality $\left|\exists x.T \parr U\left\{^{z}\!/_{y}\right\} \parr V \parr W\right| \sqsubset |\exists x.T \parr \forall y.U \parr V \parr W|$ holds; hence, by the induction hypothesis, for every variable z, there exist formulae P_i^z and values v_i^z such that $\vdash T\left\{^{v_i^z}\!/_{x}\right\} \parr P_i^z$ holds, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that derivation (4) below can be constructed. Hence, for

$z \mathrel{\#} (\forall y.U \parr V \parr W)$, the derivation (5) below can be constructed:

$$\underset{(4)}{\dfrac{\mathcal{K}\{\, P^z_1, \ldots, P^z_n \,\}}{U\{^z\!/_y\} \parr V \parr W}} \qquad \underset{(5)}{\dfrac{\dfrac{\forall z.\mathcal{K}\{\, P^z_1, \ldots, P^z_n \,\}}{\forall z.\left(U\{^z\!/_y\} \parr V \parr W\right)}}{\forall y.U \parr V \parr W}}$$

Notice that $\forall z.\mathcal{K}\{\ \}$ is a n-ary killing context as required.

Consider the commutative cases involving the *sequence* rule. We present the scenario where the principal formula $\exists x.U$ moves entirely to the left hand side of *seq* operator. The cases where the principal formula moves entirely to the right hand side of the *seq* operator and the commutative case for *times*, are similar to the cases presented below. In the scenario we consider, the bottommost rule in a proof is of the following form:

$$\frac{((\exists x.U \parr V \parr W) \triangleleft P) \parr Q}{\exists x.U \parr (V \triangleleft P) \parr W \parr Q}$$

such that $\vdash ((\exists x.U \parr V \parr W) \triangleleft P) \parr Q$ holds. By Lemma 4.19, there exist R_i and S_i such that $\vdash \exists x.U \parr V \parr W \parr R_i$ and $\vdash P \parr S_i$ hold, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that the derivation $\dfrac{\mathcal{K}\{\, R_1 \triangleleft S_1, \ldots, R_n \triangleleft S_n \,\}}{Q}$ holds, and furthermore the size of the proof of $\exists x.U \parr V \parr W \parr R_i$ is bounded above by the size of the proof of $((\exists x.U \parr V \parr W) \triangleleft P) \parr Q$ hence strictly bounded above by the size of the proof of $\exists x.U \parr (V \triangleleft P) \parr W \parr Q$. By the induction hypothesis, for $1 \leq i \leq n$, there exist formulae P^i_j and terms t^i_j such that $\vdash U\left\{^{t^i_j}\!/_x\right\} \parr P^i_j$, for $1 \leq j \leq m_i$, and killing contexts $\mathcal{K}^i\{\ \}$ such that the derivation $\dfrac{\mathcal{K}^i\{\, P^i_1, \ldots, P^i_{m_i} \,\}}{V \parr W \parr R_i}$ holds. Hence the following derivation can be constructed, as required.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathcal{K}\{\, \mathcal{K}^1\{\, P^1_1, \ldots, P^1_{m_1} \,\}, \ldots, \mathcal{K}^n\{\, P^n_1, \ldots, P^n_{m_n} \,\} \,\}}{\mathcal{K}\{\, V \parr W \parr R_i : 1 \leq i \leq n \,\}}}{\mathcal{K}\{\, (V \parr W \parr R_i) \triangleleft (P \parr S_i) : 1 \leq i \leq n \,\}}}{\mathcal{K}\{\, (V \triangleleft P) \parr W \parr R_i \triangleleft S_i : 1 \leq i \leq n \,\}}}{(V \triangleleft P) \parr W \parr \mathcal{K}\{\, R_1 \triangleleft S_1, \ldots, R_n \triangleleft S_n \,\}}}{(V \triangleleft P) \parr W \parr Q}$$

Notice that $\mathcal{K}\left\{\, \mathcal{K}^1\{\ \}, \ldots, \mathcal{K}^n\{\ \} \,\right\}$ is a $\sum_{i=1}^{n} m_i$-ary killing context as required.

Consider the commutative case induced by the *extrude new* rule. In this case, the bottommost rule of a proof is of the form

$$\frac{\text{И}y.(\exists x.P \parr Q \parr R) \parr S}{\exists x.P \parr \text{И}y.Q \parr R \parr S}\text{, where } y \mathrel{\#} \exists x.P \parr R \text{ and } \vdash \text{И}y.(\exists x.P \parr Q \parr R) \parr S \text{ holds.}$$

By Lemma 4.19, there exist T and U such that $\vdash \exists x.P \parr Q \parr R \parr U$, $y \mathrel{\#} T$ holds and either $T = U$ or $T = \reflectbox{$\exists$}y.U$, and also $\frac{T}{S}$. Furthermore, the size of the proof of $\exists x.P \parr Q \parr R \parr U$ is bounded above by the size of the proof of $\text{И}y.(\exists x.P \parr Q \parr R) \parr S$ and hence strictly bounded above by the size of the proof of $\exists x.P \parr \text{И}y.Q \parr R \parr S$, enabling the induction hypothesis. Hence, by the induction hypothesis, there exist formulae V_i and terms t_i such that $\vdash P\{^{t_i}\!/_x\} \parr V_i$ holds, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \}$ such that the derivation $\dfrac{\mathcal{K}\{\, V_1, \ldots, V_n \,\}}{Q \parr R \parr U}$ holds. Observe that, either $T = U$ and $y \mathrel{\#} U$, and hence we have derivation (6) below; or $T = \text{Э}y.U$ and hence we have derivation (7) below. Thereby we can construct the derivation (8) below.

$$\underset{(6)}{\cfrac{\text{И}y.(Q \parr R \parr U)}{\text{И}y.Q \parr R \parr T}} \qquad \underset{(7)}{\cfrac{\cfrac{\text{И}y.(Q \parr R \parr U)}{\text{И}y.(Q \parr R) \parr \text{Э}y.U}}{\text{И}y.Q \parr R \parr \text{Э}y.U}} \qquad \underset{(8)}{\cfrac{\cfrac{\cfrac{\text{И}y.\mathcal{K}\{\ V_1, \dots, V_n\ \}}{\text{И}y.(Q \parr R \parr U)}}{\text{И}y.Q \parr R \parr T}}{\text{И}y.Q \parr R \parr S}}$$

Observe that $\text{И}y.\mathcal{K}\{\ \ \}$ is a n-ary killing context as required.

Consider the commutative case induced by the *right wen* rule. In this case, the bottommost rule of a proof is of the form

$$\frac{\text{Э}y\,(\exists x.P \parr Q \parr R) \parr S}{\exists x.P \parr \text{Э}y.Q \parr R \parr S}\text{ , where } y \mathrel{\#} \exists x.P \parr R.$$

By Lemma 4.19, there exist T and U such that $\vdash \exists x.P \parr Q \parr R \parr U$, $y \mathrel{\#} T$ and either $T = U$ or $T = \text{И}y.U$, and also $\frac{T}{S}$. Furthermore, the size of the proof of $\exists x.P \parr Q \parr R \parr U$ is bounded above by the size of the proof of $\text{Э}y.(\exists x.P \parr Q \parr R) \parr S$ and hence strictly bounded above by the size of the proof of $\exists x.P \parr \text{Э}y.Q \parr R \parr S$, enabling the induction hyothesis. Hence, by the induction hypothesis, there exist formulae V_i and terms t_i such that $\vdash P\left\{{}^{t_i}\!/_x\right\} \parr V_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \ \}$ such that $\dfrac{\mathcal{K}\{\ V_1, \dots, V_n\ \}}{Q \parr R \parr U}$. Observe that either $T = U$ and $y \mathrel{\#} U$ hence the derivation (9) below holds; or $T = \text{И}y.U$ hence the derivation (10) below holds. Hence the derivation (11) below can be constructed:

$$\underset{(9)}{\cfrac{\cfrac{\text{И}y.(Q \parr R \parr U)}{\text{Э}y.(Q \parr R \parr U)}}{\text{Э}y.Q \parr R \parr T}} \qquad \underset{(10)}{\cfrac{\cfrac{\text{И}y.(Q \parr R \parr U)}{\text{Э}y.(Q \parr R) \parr \text{И}y.U}}{\text{Э}y.Q \parr R \parr \text{И}y.U}} \qquad \underset{(11)}{\cfrac{\cfrac{\cfrac{\text{И}y.\mathcal{K}\{\ V_1, \dots, V_n\ \}}{\text{И}y.(Q \parr R \parr U)}}{\text{Э}y.Q \parr R \parr T}}{\text{Э}y.Q \parr R \parr S}}$$

Observe that $\text{И}y.\mathcal{K}\{\ \ \}$ is a n-ary killing context as required.

In many commutative cases, the bottommost rule does not interfere with the principal formula. Consider when a rule is applied outside the scope of the principal formula. In this case, the bottommost rule in a proof is of the form $\dfrac{\exists x.U \parr C\{\ W\ \}}{\exists x.U \parr C\{\ V\ \}}$ such that $\vdash \exists x.U \parr C\{\ W\ \}$. By the induction hypothesis, there exist formulae P_i and terms t_i, for $1 \leq i \leq n$ such that $\vdash U\left\{{}^{t_i}\!/_x\right\} \parr P_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \ \}$ such that $\dfrac{\mathcal{K}\{\ P_1, \dots, P_n\ \}}{C\{\ W\ \}}$. Hence $\cfrac{\cfrac{\mathcal{K}\{\ P_1, \dots, P_n\ \}}{C\{\ W\ \}}}{C\{\ V\ \}}$ as required.

Consider the following application of any rule $\dfrac{\exists x.C\{\ U\ \} \parr W}{\exists x.C\{\ T\ \} \parr W}$ such that $\vdash \exists x.C\{\ U\ \} \parr W$. By the induction hypothesis, there exist formulae P_i and terms t_i where $\vdash C\{\ U\ \}\left\{{}^{t_i}\!/_x\right\} \parr P_i$, for $1 \leq i \leq n$, and n-ary killing context $\mathcal{K}\{\ \ \}$ such that $\dfrac{\mathcal{K}\{\ P_1, \dots, P_n\ \}}{W}$. Hence, by Lemma 4.1, the proof $\cfrac{\cfrac{\circ}{C\{\ U\ \}\{{}^{v_i}\!/_x\} \parr P_i}}{C\{\ T\ \}\{{}^{v_i}\!/_x\} \parr P_i}$ holds.

All cases have been considered hence the lemma holds by induction on the size of a proof. □

Lemma A.6 (Lemma 5.1). *If* $\vdash C\{\ T\ \}$*, then there exist formulae* U_i *and substitutions* σ_i*, for* $1 \leq i \leq n$*, and* n*-ary killing context* $\mathcal{K}\{\ \}$ *such that* $\vdash T\sigma_i \parr U_i$*; and, for any formula* V *there exist* W_i *such that either* $W_i = V\sigma_i \parr U_i$ *or* $W_i = \circ$ *and the following holds:* $\dfrac{\mathcal{K}\{\ W_1, W_2, \ldots, W_n\ \}}{C\{\ V\ \}}$.

Proof. The proof proceeds by induction on the size of the formula part of the context (n.b. not counting the size of atoms). The base case concerning one hole is immediate.

Consider the case for a context of the form $\exists x.C\{\ \} \parr P$, where $\vdash \exists x.C\{\ T\ \} \parr P$. By Lemma 4.20, there exist formulae Q_i and values v_i such that $\vdash C\{\ T\ \}\{^{v_i}/_x\} \parr Q_i$, for $1 \leq i \leq n$; and n-ary killing context $\mathcal{K}\{\ \}$ such that the following derivation holds.

$$\frac{\mathcal{K}\{\ Q_1, Q_2, \ldots, Q_n\ \}}{P}$$

For context $C\{\ \}$ and any formula U, let $C^i\{\ \}$ and σ_i be such that $C\{\ U\ \}\{^{v_i}/_x\} \equiv C^i\{\ U\sigma_i\ \}$. Notice that for first-order quantifiers, the substitutions does not increase the size of the formula part of the context. It can only increases the size of terms in atoms, which are not counted in this induction. Since $\vdash C\{\ T\ \}\{^{v_i}/_x\} \parr Q_i$ holds, then $\vdash C^i\{\ T\sigma_i\ \} \parr Q_i$ holds. Therefore, by the induction hypothesis, there exists formula V^i_j such that either $V^i_j = \circ$ or $V^i_j = (U\sigma_i)\,\sigma^i_j \parr W^i_j$, where $\vdash (T\sigma_i)\,\sigma^i_j \parr W^i_j$, for $1 \leq j \leq m_i$; and m_i-ary killing context $\mathcal{K}^i\{\ \}$ such that $C\{\ U\ \}\{^{v_i}/_x\} \parr Q_i \equiv C^i\{\ U\sigma_i\ \} \parr Q_i$ and the following derivation holds:

$$\frac{\mathcal{K}^i\{\ V^i_1, V^i_2, \ldots, V^i_{m_i}\ \}}{C^i\{\ U\sigma_i\ \} \parr Q_i}\ .$$

Hence the following derivation can be constructed for all formulae U.

$$\begin{array}{c}
\mathcal{K}\left\{\ \mathcal{K}^i\left\{\ V^i_j : 1 \leq j \leq m_i\ \right\} : 1 \leq i \leq n\ \right\} \\ \hline
\mathcal{K}\{\ C\{\ U\ \}\{^{v_i}/_x\} \parr Q_i : 1 \leq i \leq n\ \} \\ \hline
\mathcal{K}\{\ \exists x.C\{\ U\ \} \parr Q_i : 1 \leq i \leq n\ \} \\ \hline
\exists x.C\{\ U\ \} \parr \mathcal{K}\{\ Q_i : 1 \leq i \leq n\ \} \\ \hline
\exists x.C\{\ U\ \} \parr \mathcal{K}\{\ Q_1, \ldots, Q_n\ \} \\ \hline
\exists x.C\{\ U\ \} \parr P
\end{array}$$

Observe $V^i_j = \circ$ or $V^i_j = U\left(\sigma_i \cdot \sigma^i_j\right) \parr W^i_j$, such that $\vdash T\left(\sigma_i \cdot \sigma^i_j\right) \parr W^i_j$, for all i and j, as required.

Consider the case for a context of the form $\text{И}x.C\{\ \} \parr P$, where $\vdash \text{И}x.C\{\ T\ \} \parr P$. By Lemma 4.19, there exist formulae Q and $\hat{Q}$ such that $\vdash C\{\ T\ \} \parr \hat{Q}$ and either $Q = \hat{Q}$ or Q and $\text{Э}x.\hat{Q}$, and also $\dfrac{Q}{P}$. Therefore, by the induction hypothesis, there exist formulae V_i and W_i and substitutions σ_i such that either $V_i = \circ$ or $V_i = U\sigma_i \parr W_i$, where $\vdash T\sigma_i \parr W_i$, for $1 \leq i \leq n$; and n-ary killing context $\mathcal{K}\{\ \}$ such that

$$\frac{\mathcal{K}\{\ V_1, V_2, \ldots, V_n\ \}}{C\{\ U\ \} \parr \hat{Q}}\ .$$

Hence the following derivation

$$\begin{array}{c}
\text{И}x.\mathcal{K}^i\{\ V_i : 1 \leq i \leq n\ \} \\ \hline
\text{И}x.\left(C\{\ U\ \} \parr \hat{Q}\right) \\ \hline
\text{И}x.C\{\ U\ \} \parr Q \\ \hline
\text{И}x.C\{\ U\ \} \parr P
\end{array}$$

can be constructed for all formulae U, as required.

Consider the case for a context of the form $\text{Э}x.C\{\ \} \parr P$, where $\vdash \text{Э}x.C\{\ T\ \} \parr P$. By Lemma 4.19, there exist formulae Q and R such that $x \# Q$ and $\vdash C\{\ T\ \} \parr R$ and either $Q = R$ or $Q = \text{И}x.R$, and also $\frac{Q}{P}$. Therefore, by the induction hypothesis, there exist formulae V_i and W_i and substitutions σ_i such that either $V_i = \circ$ or $V_i = U\sigma_i \parr W_i$, where $\vdash T\sigma_i \parr W_i$, for $1 \leq i \leq n$; and n-ary killing context $\mathcal{K}\{\ \}$ such that

$$\frac{\mathcal{K}\{\ V_1, V_2, \ldots, V_n\ \}}{C\{\ U\ \} \parr R}\ .$$

In the former case that $Q = R$, since $x \# Q$, the derivation

$$\begin{array}{c} \text{И}x.\,(C\{\ U\ \} \parr R) \\ \hline \text{И}x.C\{\ U\ \} \parr R \\ \hline \text{Э}x.C\{\ U\ \} \parr R \end{array}$$

holds. In the case, $Q = \text{И}x.R$ the derivation

$$\begin{array}{c} \text{И}x.(C\{\ U\ \} \parr R) \\ \hline \text{Э}x.C\{\ U\ \} \parr \text{И}x.R \end{array}$$

holds. Hence, for all formulae U,

$$\begin{array}{c} \text{И}x.\mathcal{K}\{\ V_1, V_2, \ldots, V_n\ \} \\ \hline \text{И}x.(C\{\ U\ \} \parr R) \\ \hline \text{Э}x.C\{\ U\ \} \parr Q \\ \hline \text{Э}x.C\{\ U\ \} \parr P \end{array}\ .$$

Consider the case of a context of the form $\forall x.C\{\ \} \parr P$, where $\vdash \forall x.C\{\ T\ \} \parr$ holds. By Lemma 4.2, for any variable y, $\vdash C\{\ T\ \}\{^{y}\!/\!_{x}\} \parr P$ holds. For name y, let $C^{y}\{\ \}$ be such that for any formula U, $C\{\ U\ \}\{^{y}\!/\!_{x}\} \equiv C^{y}\{\ U\{^{y}\!/\!_{x}\}\ \}$. For any y, by the induction hypothesis, for any formula U, there exist formulae V_i^{y} such that either $V_i^{y} = \circ$ or $V_i^{y} = U\{^{y}\!/\!_{x}\}\sigma_i^{y} \parr W_i^{y}$, where $\vdash T\{^{y}\!/\!_{x}\}\sigma_i^{y} \parr W_i^{y}$ holds, for $1 \leq i \leq n$; and n-ary killing context $\mathcal{K}^{y}\{\ \}$ such that $C\{\ U\ \}\{^{y}\!/\!_{x}\} \parr P \equiv C^{y}\{\ U\{^{y}\!/\!_{x}\}\ \} \parr P$ and the following derivation can be constructed:

$$\frac{\mathcal{K}^{y}\left\{\ V_i^{y} : 1 \leq i \leq n\ \right\}}{C^{y}\{\ U\{^{y}\!/\!_{x}\}\ \} \parr P}\ .$$

Therefore, for $y \# (\forall x.C\{\ U\ \} \parr P)$ and any U, derivation

$$\begin{array}{c} \forall y.\mathcal{K}^{y}\left\{\ V_i^{y} : 1 \leq i \leq n\ \right\} \\ \hline \forall y.(C\{\ U\ \}\{^{y}\!/\!_{x}\} \parr P) \\ \hline \forall x.C\{\ U\ \} \parr P \end{array}$$

holds. In the above $V_i^{y} = \circ$ or $V_i^{y} = U\{^{y}\!/\!_{x}\}\sigma_i^{y} \parr W_i^{y}$, where $\vdash T\{^{y}\!/\!_{x}\}\sigma_i^{y} \parr W_i^{y}$ holds, for all i, as required.

The cases for *plus*, *with*, *tensor* and *seq* do not differ significantly from MAV [23]. □

Lemma A.7 (co-left and co-right: Lemma 5.7). *If* $\vdash C\{\ P \mathbin{\&} Q\ \}$ *holds then both* $\vdash C\{\ P\ \}$ *and* $\vdash C\{\ Q\ \}$ *hold.*

Proof. Assume that $\vdash (P \mathbin{\&} Q)\sigma \parr R$ holds. By Lemma 4.19, $\vdash P\sigma \parr R$ and $\vdash Q\sigma \parr R$ hold. Hence by Lemma 5.2, for any context $C\{\ \}$, if $\vdash C\{\ P \mathbin{\&} Q\ \}$ then $\vdash C\{\ P\ \}$ and $\vdash C\{\ Q\ \}$. □

Lemma A.8 (co-external: Lemma 5.8). *If* $\vdash C\{\ P \otimes (Q \oplus R)\ \}$ *holds then* $\vdash C\{\ (P \otimes Q) \oplus (P \otimes R)\ \}$ *holds.*

Proof. Assume that $\vdash ((P \oplus Q) \otimes R)\sigma \parr W$ holds, for some substitution σ. By Lemma 4.19, there exist formulae T_i and U_i such that $\vdash (P \oplus Q)\sigma \parr T_i$ and $\vdash R\sigma \parr U_i$, for $1 \leq i \leq n$, and killing context $\mathcal{K}\{\ \}$ such that

$$\begin{array}{c} \mathcal{K}\{\, T_1 \parr U_1, \ldots, T_n \parr U_n \,\} \\ \hline W \end{array} \; .$$

Now, by Lemma 4.21, for every i, there exists killing context $\mathcal{K}^i\{\ \}$ and types V^i_j such that either $\vdash P\sigma \parr V^i_j$ or $\vdash Q\sigma \parr V^i_j$ holds, for $1 \leq j \leq m_i$, and the derivation

$$\begin{array}{c} \mathcal{K}^i\{\, V^i_1, V^i_2, \ldots, V^i_{m_i} \,\} \\ \hline T_i \end{array}$$

holds.

Notice that if $\vdash P\sigma \parr V^i_j$ holds then the following derivation can be constructed.

$$\begin{array}{c} \circ \\ \hline \left(P\sigma \parr V^i_j\right) \otimes (R\sigma \parr U_i) \\ \hline (P \otimes R)\sigma \parr V^i_j \parr U_i \\ \hline ((P \otimes R) \oplus (Q \otimes R))\sigma \parr V^i_j \parr U_i \end{array}$$

Otherwise $\vdash Q \parr V^i_j$ holds, hence the following derivation can be constructed.

$$\begin{array}{c} \circ \\ \hline \left(Q\sigma \parr V^i_j\right) \otimes (R\sigma \parr U_i) \\ \hline (Q \otimes R)\sigma \parr V^i_j \parr U_i \\ \hline ((P \otimes R) \oplus (Q \otimes R))\sigma \parr V^i_j \parr U_i \end{array}$$

Hence by applying one of the above proofs for each i and j we can construct the following proof.

$$\begin{array}{c} \circ \\ \hline \mathcal{K}\left\{\, \mathcal{K}^i\{\, \circ \colon 1 \leq j \leq m_i \,\} : 1 \leq i \leq n \,\right\} \\ \hline \mathcal{K}\left\{\, \mathcal{K}^i\left\{\, ((P \otimes R) \oplus (Q \otimes R))\sigma \parr V^i_j \parr U_i \colon 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline \mathcal{K}\left\{\, ((P \otimes R) \oplus (Q \otimes R))\sigma \parr \mathcal{K}^i\left\{\, V^i_j \parr U_i \colon 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline ((P \otimes R) \oplus (Q \otimes R))\sigma \parr \mathcal{K}\left\{\, \mathcal{K}^i\left\{\, V^i_j \parr U_i \colon 1 \leq j \leq m_i \,\right\} : 1 \leq i \leq n \,\right\} \\ \hline ((P \otimes R) \oplus (Q \otimes R))\sigma \parr \mathcal{K}\{\, \mathcal{K}^i\{\, V^i_1, V^i_2, \ldots, V^i_{m_i} \,\} \parr U_i \colon 1 \leq i \leq n \,\} \\ \hline ((P \otimes R) \oplus (Q \otimes R))\sigma \parr \mathcal{K}\{\, T_1 \parr U_1, \ldots, T_n \parr U_n \,\} \\ \hline ((P \otimes R) \oplus (Q \otimes R))\sigma \parr W \end{array}$$

Hence $\vdash ((P \otimes R) \oplus (Q \otimes R)) \parr W$. Therefore, by Lemma 5.2, for any context $\vdash C\{\, (P \oplus Q) \otimes R \,\}$ yields $\vdash C\{\, (P \otimes R) \oplus (Q \otimes R) \,\}$, as required. □

Lemma A.9 (co-sequence: Lemma 5.9). *If* $\vdash C\{\, (P \triangleleft Q) \otimes (R \triangleleft S) \,\}$ *holds then* $\vdash C\{\, (P \otimes R) \triangleleft (Q \otimes S) \,\}$ *holds.*

Proof. Assume that $\vdash ((P \triangleleft Q) \otimes (R \triangleleft S))\sigma \parr U$ holds, for some substitution σ. By Lemma 4.19, there exist n-ary killing context $\mathcal{K}\{\ \}$ and U^0_i and U^1_i, for $1 \leq i \leq n$, such that $\vdash (P \triangleleft Q)\sigma \parr U^0_i$ and

$\vdash (R \triangleleft S)\,\sigma \parr U^1_i$ and the derivation

$$\frac{\mathcal{K}\{\ U^0_1 \parr U^1_1, U^0_2 \parr U^1_2, \ldots\ \}}{U}$$

holds.

Hence by Lemma 4.19, for $k \in \{0,1\}$ there exists m^k_i-ary killing context $\mathcal{K}^k_i\{\ \}$ and types $V^k_{i,j}$, $W^k_{i,j}$ for $1 \leq j \leq m^k_i$, such that $\vdash P\sigma \parr V^0_{i,j}$ and $\vdash Q\sigma \parr W^0_{i,j}$ and $\vdash R\sigma \parr V^1_{i,j}$ and $\vdash S\sigma \parr W^1_{i,j}$ and the following derivation

$$\frac{\mathcal{K}^k_i\left\{\ V^k_{i,1} \triangleleft W^k_{i,1}, V^k_{i,2} \triangleleft W^k_{i,2} \ldots \right\}}{U^k_i}$$

holds.

Hence we can construct the following proof.

$$
\begin{array}{c}
\circ \\ \hline
\mathcal{K}\{\ \ \mathcal{K}^1_i\{\ \ \mathcal{K}^0_i\{\ \ \circ : 1 \leq j \leq m^0_i\ \ \} : 1 \leq k \leq m^1_i\ \ \} : 1 \leq i \leq n\ \ \} \\ \hline
\mathcal{K}\left\{ \mathcal{K}^1_i\left\{ \mathcal{K}^0_i\left\{ \begin{array}{l} \left(\left(P\sigma \parr V^0_{i,j}\right) \otimes \left(R\sigma \parr V^1_{i,k}\right)\right) \triangleleft \\ \left(\left(Q\sigma \parr W^0_{i,j}\right) \otimes \left(S\sigma \parr W^1_{i,k}\right)\right) \end{array} : 1 \leq j \leq m^0_i \right\} : 1 \leq k \leq m^1_i \right\} : 1 \leq i \leq n \right\} \\ \hline
\mathcal{K}\left\{ \mathcal{K}^1_i\left\{ \mathcal{K}^0_i\left\{ \begin{array}{l} \left((P \otimes R)\,\sigma \parr V^0_{i,j} \parr V^1_{i,k}\right) \triangleleft \\ \left((Q \otimes S)\,\sigma \parr W^0_{i,j} \parr W^1_{i,k}\right) \end{array} : 1 \leq j \leq m^0_i \right\} : 1 \leq k \leq m^1_i \right\} : 1 \leq i \leq n \right\} \\ \hline
\mathcal{K}\left\{ \mathcal{K}^1_i\left\{ \mathcal{K}^0_i\left\{ \begin{array}{l} ((P \otimes R) \triangleleft (Q \otimes S))\sigma \parr \\ \left(\left(V^0_{i,j} \parr V^1_{i,k}\right) \triangleleft \left(W^0_{i,j} \parr W^1_{i,k}\right)\right) \end{array} : 1 \leq j \leq m^0_i \right\} : 1 \leq k \leq m^1_i \right\} : 1 \leq i \leq n \right\} \\ \hline
((P \otimes R) \triangleleft (Q \otimes S))\,\sigma \parr \mathcal{K}\left\{ \begin{array}{r} \mathcal{K}^1_i\left\{ \begin{array}{r} \mathcal{K}^0_i\left\{ \left(V^0_{i,j} \parr V^1_{i,k}\right) \triangleleft \left(W^0_{i,j} \parr W^1_{i,k}\right) : 1 \leq j \leq m^0_i \right\} \\ : 1 \leq k \leq m^1_i \end{array} \right\} \\ : 1 \leq i \leq n \end{array} \right\} \\ \hline
((P \otimes R) \triangleleft (Q \otimes S))\sigma \parr \mathcal{K}\left\{ \begin{array}{r} \mathcal{K}^1_i\left\{ \begin{array}{r} \mathcal{K}^0_i\left\{ \left(V^0_{i,j} \triangleleft W^0_{i,j}\right) \parr \left(V^1_{i,k} \triangleleft W^1_{i,k}\right) : 1 \leq j \leq m^0_i \right\} \\ : 1 \leq k \leq m^1_i \end{array} \right\} \\ : 1 \leq i \leq n \end{array} \right\} \\ \hline
((P \otimes R) \triangleleft (Q \otimes S))\sigma \parr \mathcal{K}\left\{ \begin{array}{r} \mathcal{K}^1_i\left\{ \begin{array}{r} \mathcal{K}^0_i\left\{ V^0_{i,j} \triangleleft W^0_{i,j} : 1 \leq j \leq m^0_i \right\} \parr \left(V^1_{i,k} \triangleleft W^1_{i,k}\right) \\ : 1 \leq k \leq m^1_i \end{array} \right\} \\ : 1 \leq i \leq n \end{array} \right\} \\ \hline
((P \otimes R) \triangleleft (Q \otimes S))\sigma \parr \mathcal{K}\left\{ \begin{array}{l} \quad\ \ \mathcal{K}^0_i\left\{ V^0_{i,j} \triangleleft W^0_{i,j} : 1 \leq j \leq m^0_i \right\} \\ \parr \ \ \mathcal{K}^1_i\left\{ V^1_{i,k} \triangleleft W^1_{i,k} : 1 \leq k \leq m^1_i \right\} \end{array} : 1 \leq i \leq n \right\} \\ \hline
((P \otimes R) \triangleleft (Q \otimes S))\sigma \parr \mathcal{K}\{\ U^0_1 \parr U^1_1, U^0_2 \parr U^1_2, \ldots\ \} \\ \hline
((P \otimes R) \triangleleft (Q \otimes S))\sigma \parr U
\end{array}
$$

Therefore, by Lemma 5.2, for any context $\vdash C\{\ (P \triangleleft Q) \otimes (R \triangleleft S)\ \}$ yields $\vdash C\{\ (P \otimes R) \triangleleft (Q \otimes S)\ \}$. □

Lemma A.10 (co-tidy: Lemma 5.10). *If* $\vdash C\{\ \circ \oplus \circ\ \}$ *holds, then* $\vdash C\{\ \circ\ \}$ *holds.*

Proof. Assume that $\vdash (\circ \oplus \circ) \parr P$ holds. By Lemma 4.21, there exist killing context $\mathcal{K}\{\ \}$ and formulae U_i for $1 \leq i \leq n$ such that $\vdash \circ \parr U_i$ or $\vdash \circ \parr U_i$ hold, hence $\vdash U_i$ holds, and the following derivation can be constructed.

$$\frac{\mathcal{K}\{\, U_1, \ldots, U_n \,\}}{P} \;.$$

Thereby the following proof can be constructed:

$$\begin{array}{c} \circ \\ \hline \mathcal{K}\{\, \circ, \circ, \ldots \,\} \\ \hline \mathcal{K}\{\, U_1, \ldots, U_n \,\} \\ \hline P \end{array} \;.$$

Therefore, by Lemma 5.2, for any context $\vdash C\{\, \circ \oplus \circ \,\}$ yields $\vdash C\{\, \circ \,\}$, as required. □

Lemma A.11 (Atomic co-interaction: Lemma 5.11). *If* $\vdash C\{\, \alpha \otimes \overline{\alpha} \,\}$ *holds then* $\vdash C\{\, \circ \,\}$ *holds.*

Proof. Assume for atom α that $\vdash (\alpha \otimes \overline{\alpha})\, \sigma \parr P$, for some formula P and some substitution σ. By Lemma 4.19, there exist n-ary killing context $\mathcal{K}\{\ \}$ and formulae U_i and V_i such that $\vdash \alpha\sigma \parr U_i$ and $\vdash \overline{\alpha\sigma} \parr V_i$, for $1 \leq i \leq n$, such that

$$\frac{\mathcal{K}\{\, U_1 \parr V_1, U_2 \parr V_2, \ldots \,\}}{P} \;.$$

By Lemma 4.22, for every i, there exist m_i^0-ary killing contexts $\mathcal{K}_i^0\{\ \}$ such that

$$\frac{\mathcal{K}_i^0\{\, \overline{\alpha\sigma}, \ldots, \overline{\alpha\sigma} \,\}}{U_i} \;.$$

By Lemma 4.22, for every i, there exist m_i^1-ary killing contexts $\mathcal{K}_i^1\{\ \}$ such that

$$\frac{\mathcal{K}_i^1\{\, \alpha\sigma, \ldots, \alpha\sigma \,\}}{V_i} \;.$$

Thereby the following proof can be constructed.

$$\begin{array}{c} \circ \\ \hline \mathcal{K}\{\, \mathcal{K}_i^1\{\, \mathcal{K}_i^0\{\, \circ \colon 1 \leq j \leq m_i^0 \,\} : 1 \leq k \leq m_i^1 \,\} : 1 \leq i \leq n \,\} \\ \hline \mathcal{K}\{\, \mathcal{K}_i^1\{\, \mathcal{K}_i^0\{\, \overline{\alpha\sigma} \parr \alpha\sigma \colon 1 \leq j \leq m_i^0 \,\} : 1 \leq k \leq m_i^1 \,\} : 1 \leq i \leq n \,\} \\ \hline \mathcal{K}\{\, \mathcal{K}_i^1\{\, \mathcal{K}_i^0\{\, \overline{\alpha\sigma} \colon 1 \leq j \leq m_i^0 \,\} \parr \alpha\sigma \colon 1 \leq k \leq m_i^1 \,\} : 1 \leq i \leq n \,\} \\ \hline \mathcal{K}\{\, \mathcal{K}_i^0\{\, \overline{\alpha\sigma} \colon 1 \leq j \leq m_i^0 \,\} \parr \mathcal{K}_i^1\{\, \alpha\sigma \colon 1 \leq k \leq m_i^1 \,\} : 1 \leq i \leq n \,\} \\ \hline \mathcal{K}\{\, U_1 \parr V_1, U_2 \parr V_2, \ldots \,\} \\ \hline P \end{array}$$

Therefore, by Lemma 5.2, for any context $C\{\ \}$, $\vdash C\{\, \alpha \otimes \overline{\alpha} \,\}$ yields that $\vdash C\{\, \circ \,\}$, as required. □

Received November 2017; revised September 2018; accepted April 2019