On the Power of Substitution in the Calculus of Structures

Novak Novaković, Inria
Lutz Straßburger, Inria

There are two contributions in this paper. First, we give a direct proof of the known fact that Frege systems with substitution can be p-simulated by the calculus of structures extended with the substitution rule. This is done without referring to the p-equivalence of extended Frege systems and Frege systems with substitution. Second, we then show that the cut-free calculus of structures with substitution is p-equivalent to the cut-free calculus of structures with extension.

Categories and Subject Descriptors: F.4.1 [**Mathematical Logic**]: Proof Theory

General Terms: Theory

Additional Key Words and Phrases: Calculus of structures, classical logic, deep inference, extension, Frege systems, proof complexity, substitution

ACM Reference Format:
Novak Novaković and Lutz Straßburger, 2014. On the Power of Substitution in the Calculus of Structures. ACM Trans. Comput. Logic V, N, Article A (January YYYY), 21 pages.
DOI:http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

Extension and substitution are concepts studied in proof complexity of propositional classical logic. The basic idea behind both concepts is that complex formulas can be abbreviated by propositional variables in order to shorten a proof. So far, extension and substitution have mostly been investigated together with Frege systems, which, for a long time, have been the main tool for studying proof complexity. In [Cook and Reckhow 1979], Cook and Reckhow have shown that Frege systems with substitution can p-simulate Frege systems with extension. Several years later, Dowd in [Dowd 1985] and Krajíček and Pudlák in [Krajíček and Pudlák 1989] have shown that Frege systems with extension can also p-simulate Frege systems with substitution. It is still an open problem whether Frege systems without extension/substitution can p-simulate Frege systems with extension/substitution.

Only recently, Bruscoli and Guglielmi [Bruscoli and Guglielmi 2009] have shown that also deep inference proof systems, like the calculus of structures (CoS) [Guglielmi 2007; Brünnler and Tiu 2001; Guglielmi and Straßburger 2001], can provide a nat-

This work has been supported by the French National Research Agency (ANR), project “STRUCTURAL”, and by the Ministry of Education and Science of Serbia, project ON 174026.

DOI:http://dx.doi.org/10.1145/0000000.0000000

ural framework for studying extension and substitution. As shown in [Bruscoli and Guglielmi 2009], Frege systems and calculus of structures (with cut) p-simulate each other and are therefore equally powerful with respect to proof complexity. However, unlike Frege systems, the calculus of structures is a proof formalism that comes with methods for proof search [Kahramanoğulları 2006; Chaudhuri et al. 2011; Chaudhuri 2013b] and proof normalization [Brünnler 2003a; Brünnler 2006; Straßburger and Guglielmi 2011; Guglielmi and Straßburger 2011]. This means that we can now study *cut-free* proof systems with extension and substitution [Straßburger 2012]. Some research in that direction has already been done by Arai in [Arai 1996].

The purpose of this paper is to fill two gaps that have been left open in the previous work [Bruscoli and Guglielmi 2009; Straßburger 2012] investigating the concepts of extension and substitution within the calculus of structures.

(1) There is a straightforward translation between proofs in Frege systems and proofs in the calculus of structures [Bruscoli and Guglielmi 2009], leading only to a polynomial increase in the size of proofs in both directions, and thus establishing the p-equivalence of Frege systems and CoS. This translation carries over to the case where extension is present. But when substitution is present, the naive translation of Frege proofs into calculus of structures proofs breaks down. This might cause the belief that substitution in the calculus of structures is *a priori* a weaker concept than substitution in Frege systems [Guglielmi 2010]. However, in this paper we show that this is not justified. We show that, with a subtle modification, the naive translation carries over to the case with substitution. This properly establishes the correspondence between Frege systems with substitution and CoS with substitution. As a consequence, the construction used in [Straßburger 2012] for showing that CoS with extension p-simulates CoS with substitution can now be seen as alternative proof of the result by Krajíček and Pudlák [Krajíček and Pudlák 1989].
(2) In [Straßburger 2012], it has been shown that also in the cut-free case CoS with extension p-simulates CoS with substitution, but it was left open whether the converse also holds. In this paper we show that cut-free CoS with substitution p-simulates cut-free CoS with extension. This establishes the p-equivalence of extension and substitution also in the cut-free case.

The whole picture is summarized in Figure 1, where an arrow from one system to the other means that the first system p-simulates the second. The label indicates the place where this has been proven first. The dotted arrows refer to open problems and the double arrows to the results of this paper, which is organized as follows: Sections 2 and 3 present preliminaries on Frege systems and calculus of structures, Section 4 corresponds to the first point above, and Section 5 to the second point above.

2. PRELIMINARIES ON FREGE SYSTEMS

Formulas. Let $\mathcal{A}t = \{a, b, c, \dots\}$ be a countable set of *propositional variables*, also called *atoms*, and let $\overline{\mathcal{A}t} = \{\bar{a}, \bar{b}, \bar{c}, \dots\}$ be the assigned set of *negated atoms*. We refer to elements of $\mathcal{A}t$ and $\overline{\mathcal{A}t}$ as *literals*. The set of Boolean propositional formulas $\mathcal{F}orm$ whose elements are denoted by capital Latin letters $(A, B, C, \dots)$ is the smallest language over the alphabet $\mathcal{A}t \cup \overline{\mathcal{A}t} \cup \{\wedge, \vee, (,), [,]\}$, such that $\mathcal{A}t, \overline{\mathcal{A}t} \subset \mathcal{F}orm$, and if $A, B \in \mathcal{F}orm$, then $(A \wedge B) \in \mathcal{F}orm$ and $[A \vee B] \in \mathcal{F}orm$. Notice the use of $(-)$ and $[-]$ brackets for conjunction and disjunction formulas, respectively. Technically speaking, this is redundant, but we think it improves readability for larger formulas. Furthermore, outermost brackets are always omitted. For reasons of convenience, we think of

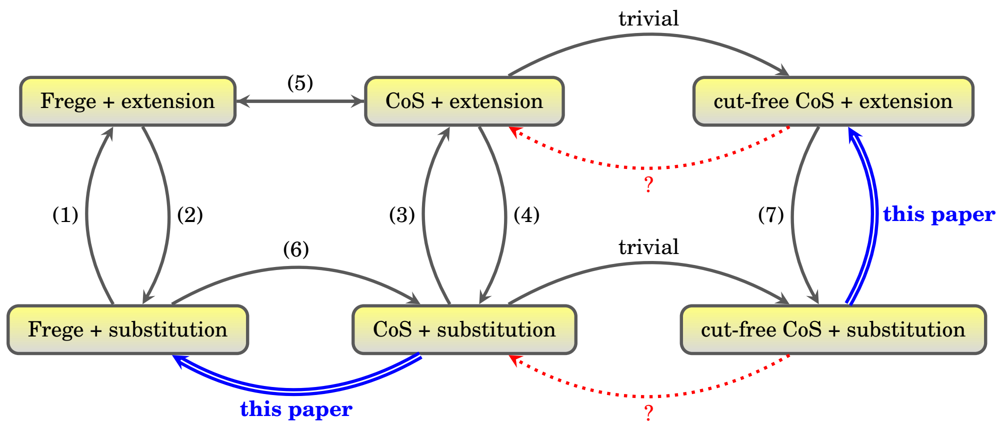

Fig. 1. Relation between Frege systems and calculus of structures. An arrow denotes that the source system p-simulates the target system. Dotted arrows denote open problems, while double arrows stand for results of this paper. (1) has been shown in [Cook and Reckhow 1979], (2) in [Krajíček and Pudlák 1989] and [Dowd 1985], (3) and (6) in [Bruscoli and Guglielmi 2009], (4) and (7) in [Straßburger 2012], and (5) in [Bruscoli and Guglielmi 2009] and [Straßburger 2012].

the Boolean negation as non-primitive. For an atom a, its negation is defined as its assigned negated atom $\bar{a}$. Then the definition is extended to arbitrary formulas by de Morgan laws: $\bar{\bar{a}} = a$ and $\overline{A \wedge B} = \bar{A} \vee \bar{B}$ and $\overline{A \vee B} = \bar{A} \wedge \bar{B}$. This entails $\bar{\bar{A}} = A$ for all A. Implication $A \Rightarrow B$ is defined as $\bar{A} \vee B$ and equivalence $A \Leftrightarrow B$ as $[\bar{A} \vee B] \wedge [\bar{B} \vee A]$.

Proof systems. We adopt a general view of proof systems as presented in [Cook and Reckhow 1979]. A proof system is defined as a surjective **PTIME** function $S\colon \Sigma^* \to \mathcal{T}$, from a set of finite words Σ^* over a signature Σ to the set $\mathcal{T}$ of all propositional tautologies. The assignment $S\colon \Pi \mapsto S(\Pi)$ assigns to an element of Σ^*, called a *proof*, its *conclusion*. A size of a proof is a function $|{-}|\colon \Sigma^* \to \mathbb{N}$, assigning to a proof Π the number $|\Pi|$ of symbols in Π. For proof systems $S_1\colon \Sigma_1^* \to \mathcal{T}$ and $S_2\colon \Sigma_2^* \to \mathcal{T}$ we say that S_2 *p-simulates* S_1 if there is a polynomial p such that for every proof $\Pi_1 \in \Sigma_1^*$ there is a proof $\Pi_2 \in \Sigma_2^*$ such that $S_1(\Pi_1) = S_2(\Pi_2)$ and $|\Pi_2| \leq p(|\Pi_1|)$, i.e. proofs of Σ_1^* can be assigned proofs Σ_2^* of same conclusions whose size is dominated by a fixed polynomial in the size of Σ_1^* proofs. Systems which p-simulate each other are said to be *p-equivalent*.

Frege systems. A (general) *Frege system* is defined by a set *Ax* of formulas called *axioms* and a set R of (general) inference rule schemata, where a schema $r \in R$ is of the form

$$r\,\frac{B_1, \ldots, B_n}{B} \quad ,$$

where $B_1, \ldots, B_n, B$ are formula variables, i.e., meta variables, denotations of arbitrary formulas. A derivation of a formula A in a Frege system from a given set of axioms and a collection of inference rules is a sequence of formulas $A_1, \ldots, A_m$ such that $A_m = A$, and every A_k is either an axiom, or it is derived from some of the formulas A_i, $i < k$, as an instance of a rule from R.

These systems are named after Gottlob Frege in [Cook and Reckhow 1979], but they also appear in literature as Hilbert-Frege, Hilbert or Hilbert-Ackermann systems. For the case of classical propositional logic, there are numerous possible axiomatizations of Frege systems, and an example system consists of the following axioms (usually expressed in the implication/negation language):

$$\begin{array}{ll} \text{AX-1:} & \bar{A} \vee [\bar{B} \vee A] \\ \text{AX-2:} & (A \wedge (B \wedge \bar{C})) \vee [(A \wedge \bar{B}) \vee [\bar{A} \vee C]] \\ \text{AX-3:} & (\bar{B} \wedge A) \vee [(\bar{B} \wedge \bar{A}) \vee B] \end{array} \tag{2.1}$$

where A, B, and C are formula variables, and a single inference rule *modus ponens*, MP:

$$\mathsf{MP}\,\frac{A \qquad \bar{A} \vee B}{B} \quad .$$

Besides the essential properties of soundness and completeness of the Frege system for classical propositional logic, it has been shown in [Cook and Reckhow 1979] that all Frege systems for this logic p-simulate each other. That allows us to think of the system F defined by the set of axioms (2.1) as 'the' Frege system, since all of the proof complexity results we may have on a specific system translate to the entire formalism. Also,

THEOREM 2.1. [Cook and Reckhow 1979] *Every Frege system is p-equivalent to sequent calculus for classical propositional logic with cut.*

Extension. The notion of *extension* in Frege systems, due to Tseitin [Tseitin 1968], comes from the idea of using abbreviations in a proof. The concept can be formalized in as follows. An *extended Frege system* is a Frege system whose set of axioms *Ax* is augmented by the *extension axioms* of the form

$$a_i \Leftrightarrow A_i, \qquad\qquad 1 \leq i \leq k; \tag{2.2}$$

where a_i are fresh propositional variables which abbreviate formulas A_i, subject to the condition that a variable a_i does neither occur in the conclusion of the proof nor in any of the $A_1, \ldots, A_j$, for $j \leq i$. We call the a_i *extension variables* and the A_i *extension formulas*. We write eF for an extended Frege system.

Substitution. The notion of *substitution* comes from a slightly different principle than extension, a widely used technique of replacing propositional variables by formulas. Formally, a *substitution* is a map $\sigma : \mathcal{A}t \to \mathcal{F}orm$ from the set of atoms to the set of formulas, such that $\sigma(a) = a$ holds on all but finitely many atoms in $\mathcal{A}t$. The reader should notice that there is no constraint put on the nature of the map σ, as it is the case with extension. To have substitution in a Frege system amounts to adding an inference rule, called the *substitution rule*

$$\mathsf{sub}{\downarrow}\,\frac{A}{\sigma A} \tag{2.3}$$

to the system, where σA denotes the result of applying the substitution σ to the formula A, i.e., replacing every atom a by $\sigma(a)$ and every negated atom $\bar{a}$ by $\overline{\sigma(a)}$. We refer to F augmented by the substitution rule as sF.

THEOREM 2.2. [Cook and Reckhow 1979] sF *p-simulates* eF.

THEOREM 2.3. [Krajíček and Pudlák 1989; Dowd 1985] eF *p-simulates* sF.

3. PRELIMINARIES ON CALCULUS OF STRUCTURES

Inference rules. The principle of deep inference, as used in the *calculus of structures* [Brünnler and Tiu 2001; Guglielmi 2007; Guglielmi and Straßburger 2001], means that one is allowed to apply inference rules arbitrarily deep inside a formula, to the contrast with sequent calculus or natural deduction [Gentzen 1934] where rules are always applied on the outermost connectives. In this paper we follow the formulations as given in [Straßburger 2012]. We use the following rule schemata:

$$\begin{array}{lll} \mathsf{ai}{\downarrow}\,\dfrac{F\{B\}}{F\{B \wedge [\bar{a} \vee a]\}}\ ,\ {\scriptstyle F\{B\}\text{ is allowed to be empty}} & & \mathsf{s}\,\dfrac{F\{[A \vee B] \wedge C\}}{F\{(A \wedge C) \vee B\}} \\ \mathsf{m}\,\dfrac{F\{(A \wedge B) \vee (C \wedge D)\}}{F\{[A \vee C] \wedge [B \vee D]\}} & \mathsf{w}{\downarrow}\,\dfrac{F\{B\}}{F\{B \vee A\}} & \mathsf{ac}{\downarrow}\,\dfrac{F\{a \vee a\}}{F\{a\}}\ . \end{array} \tag{3.1}$$

where A, B, C, D are meta variables denoting formulas, while a is a meta variable for a literal (i.e., an atom or a negated atom). The notation $F\{\ \}$ is used for a formula context. We write $F\{B\}$ for the formula that is obtained from filling the hole of $F\{\ \}$ with B.

The rules in 3.1 are called *(atomic) identity, switch, medial, weakening* and *(atomic) contraction*, respectively. Rule ai↓ is the only rule that need not have a premise, i.e. allowing $F\{B\}$ to be the empty word over the formula alphabet in the definition of ai↓ means that $\bar{a} \vee a$ can be derived without premise, as an instance of the rule. Notice that in every rules the context is monotone with respect to the subformula that is manipulated.

On the set $\mathcal{F}orm$ of formulas we define the relation $=$ to be the smallest congruence generated by

$$\begin{array}{ll} A \wedge (B \wedge C) = (A \wedge B) \wedge C & \qquad A \wedge B = B \wedge A \\ A \vee [B \vee C] = [A \vee B] \vee C & \qquad A \vee B = B \vee A \end{array} \tag{3.2}$$

Then, we add another inference rule

$$= \frac{F\{A\}}{F\{B\}} \tag{3.3}$$

with the side condition that $A = B$.

Derivations. A *derivation* in the calculus of structures is a rewriting sequence using the inference rules of a given system. There can be at most one instance of an inference rule with empty premise in a derivation. If there is no such instance then we use the notation

$$\begin{array}{c} A \\ \mathcal{S}\big\Vert\,\Pi \\ B \end{array}$$

for saying that the derivation Π has premise A, conclusion B, and uses only inference rules in the system $\mathcal{S}$. If a derivation contains a rule with an empty formula in its premise then this must be the topmost rule, and we use the notation

$$\begin{array}{c} \mathcal{S}\overline{\big\Vert}\,\Pi \\ B \end{array}$$

for a derivation in the system $\mathcal{S}$ with no premise and with conclusion B. In this case we also say that Π is a *proof* of B. The *length* of a derivation (or proof) Π is the number of lines in Π. The *width* of Π is the largest number of literals in a formula occurring in Π.

System KS. The deep inference proof system defined as above by the set of rules (3.1) and (3.3) is called KS. Strictly speaking, the original presentation of the system with the same name in [Brünnler and Tiu 2001] differs from ours; it relies on the presence of units for disjunction and conjunction in syntax, **f** and **t**, respectively. It is argued in [Straßburger 2012] how our presentation is only a mild variation to the presentation of KS in [Brünnler and Tiu 2001], and that the two versions of KS p-simulate each other. Later, we will make use of the following properties of KS.

PROPOSITION 3.1. [Brünnler and Tiu 2001] *The system* KS *is sound and complete for classical logic, i.e., a propositional formula is a tautology iff there is a* KS *proof of it.*

PROPOSITION 3.2. [Brünnler and Tiu 2001] *The inference rules*

$$\mathsf{i}{\downarrow}\,\frac{F\{B\}}{F\{B \wedge [\bar{A} \vee A]\}} \qquad \textit{and} \qquad \mathsf{c}{\downarrow}\,\frac{F\{A \vee A\}}{F\{A\}}$$

are derivable in KS*, where in* $\mathsf{i}{\downarrow}$ *the premise* $F\{B\}$ *is allowed to be empty. Moreover,* KS *p-simulates* $\mathsf{KS} \cup \{\mathsf{i}{\downarrow}, \mathsf{c}{\downarrow}\}$.

The rules $\mathsf{i}{\downarrow}$ and $\mathsf{c}{\downarrow}$ are the non-atomic versions of identity and contraction rules, respectively.

PROPOSITION 3.3. [Brünnler and Tiu 2001; Bruscoli and Guglielmi 2009] *The system* KS *p-simulates cut-free sequent calculus. But the opposite does not hold.*

Cut and system SKS. The (atomic) cut rule in deep inference systems is dual to the (atomic) identity

$$\mathsf{ai}{\uparrow}\,\frac{F\{B \vee (\bar{a} \wedge a)\}}{F\{B\}}\ . \tag{3.4}$$

We refer to the system $\mathsf{KS} \cup \{\mathsf{ai}{\uparrow}\}$ as SKS.

Again, this definition of the system SKS is a mild modification of the original definition of SKS found in [Brünnler and Tiu 2001]. The same paper shows that adding atomic cut yields the non-atomic version of cut, co-contraction, and co-weakening, rules dual to the contraction and weakening, respectively:

PROPOSITION 3.4. [Brünnler and Tiu 2001] *The following rules are derivable in* SKS

$$\mathsf{i}{\uparrow}\,\frac{F\{B \wedge (\bar{A} \wedge A)\}}{F\{B\}} \qquad \mathsf{c}{\uparrow}\,\frac{F\{A\}}{F\{A \wedge A\}} \qquad \mathsf{w}{\uparrow}\,\frac{F\{A \wedge B\}}{F\{B\}}$$

Moreover, SKS *p-simulates* $\mathsf{SKS} \cup \{\mathsf{i}{\uparrow}, \mathsf{c}{\uparrow}, \mathsf{w}{\uparrow}\}$.

PROPOSITION 3.5. [Brünnler and Tiu 2001] *There is an* SKS *derivation from* A *to* B *if and only if* $A \Rightarrow B$ *is a tautology.*

THEOREM 3.6. [Bruscoli and Guglielmi 2009] SKS *and* F *are p-equivalent.*

Note that this follows from Theorem 2.1 and the p-equivalence of SKS and sequent calculus. But Bruscoli and Guglielmi give in [Bruscoli and Guglielmi 2009] a direct construction. To show how SKS can be p-simulated in F, it suffices to first exhibit an F proof of $A \Rightarrow B$ for every SKS rule $\mathsf{r}\,\dfrac{F\{A\}}{F\{B\}}$. Then, it can be shown by induction on the size of the context $F\{\}$ that there is an F derivation of $(A \Rightarrow B) \Rightarrow (F\{A\} \Rightarrow F\{B\})$ whose size is polynomial in $|F\{A\} \Rightarrow F\{B\}|$. so an entire SKS proof can be simulated by consecutive applications of MP, whose number is linear in the size of the SKS proof. The other direction, i.e., the p-simulation of F in SKS will be discussed in detail in Section 4.

Extension. There are two ways of adding extension to the calculus of structures. First, on can do the same as in Frege systems and simply add additional axioms. This has been done in [Bruscoli and Guglielmi 2009] in the following way: A proof in xSKS of conclusion B is an SKS derivation whose conclusion is B and whose premise is the conjunction of the extension axioms (2.2). Then, the proof of Theorem 3.6 can be used to prove the following:

THEOREM 3.7. [Bruscoli and Guglielmi 2009] xSKS *and* eF *are p-equivalent.*

The second way of adding extension to SKS, proposed in [Straßburger 2012], is to add for every extension axiom $a_i \Leftrightarrow A_i$ the two rules

$$\mathsf{ext}\!\downarrow \frac{F\{a_i\}}{F\{A_i\}} \qquad \text{and} \qquad \mathsf{ext}\!\downarrow \frac{F\{\bar{a}_i\}}{F\{\bar{A}_i\}} \tag{3.5}$$

This allows us to use extension in the absence of cut (or modus ponens). We write eKS for KS $\cup$ {ext↓}, and eSKS for SKS $\cup$ {ext↓}.

THEOREM 3.8. [Straßburger 2012] xSKS *and* eSKS *are p-equivalent.*

Substitution. Substitution is added to the calculus of structures in exactly the same way as it is added to Frege systems: by adding the inference rule

$$\mathsf{sub}\!\downarrow \frac{A}{\sigma A} \tag{3.6}$$

for a given a substitution $\sigma : \mathcal{A}t \rightarrow \mathcal{F}orm$. However, note that this rule cannot be applied deeply, even if it is added to a deep inference system. The rule in 3.6 is only sound when applied to the whole formula, and not just to a selected subformula. We define sKS to be KS $\cup$ {sub↓}, and sSKS to be SKS $\cup$ {sub↓}. The following have been shown previously via simple direct constructions:

THEOREM 3.9. [Bruscoli and Guglielmi 2009] sSKS *p-simulates* xSKS.

THEOREM 3.10. [Straßburger 2012] eSKS *p-simulates* sSKS.

Together with Theorem 3.8 (which is also shown via rather simple direct translations) these two results show that in the calculus of structures extension and substitution are p-equivalent, and their proofs show that this fact is almost a triviality. Furthermore, we have the following (again, with a rather simple proof):

THEOREM 3.11. [Bruscoli and Guglielmi 2009] sF *p-simulates* sSKS.

On the one hand, this shows (together with Theorems 2.2, 2.3, and 3.7) that extension and substitution are p-equivalent in Frege systems and in the calculus of structures:

COROLLARY 3.12. sF*,* eF*,* sSKS*,* xSKS*, and* eSKS *are all p-equivalent.*

On the other hand, this fact relies (so far), on Theorem 2.3 whose proof is much more involved than the others. The reason is that (so far) there is no simple simulation of sF in any of sSKS, xSKS, or eSKS. In the following section we show that sSKS p-simulates sF by giving a direct construction which follows the scheme of the p-simulation of F in SKS (Theorem 3.6).

4. SUBSTITUTION IN FREGE AND COS

In this section we show that CoS with substitution p-simulates Frege systems with substitution. Let us start by recalling the simple construction by Bruscoli and Guglielmi [Bruscoli and Guglielmi 2009] for translating a (substitution-free) F-proof into an SKS-proof, with a polynomial blow-up. This is a rather standard construction (see e.g. [Krajíček 1996]), and it is done in three steps. First, we observe that every axiom A in the Frege system has an SKS-proof Π_A of size $O(|A|^2)$. Second, from a given F-proof $A_1, A_2, \ldots, A_n$, we proceed by induction on n to produce an SKS-proof Π of the conjunction $A_1 \wedge A_2 \wedge \cdots \wedge A_n$. This is done as follows. Assume by induction hypothesis an SKS-proof Π' of the conjunction $A_1 \wedge A_2 \wedge \cdots \wedge A_{n-1}$. If A_n is an axiom, we immediately obtain Π by combining Π' and the proof Π_{A_n} of A_n. If A_n is obtained by applying modus ponens to some A_i and A_j, where A_j is $A_i \Rightarrow A_n$ and $0 < i, j < n$, then we obtain Π from Π' as follows:

$$
\begin{array}{r c}
 & \Vert\,\Pi' \\
 & A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge [\bar{A}_i \vee A_n] \wedge \cdots \wedge A_{n-1} \\
{}_{2*}\mathsf{c}\!\uparrow & \overline{A_1 \wedge \cdots \wedge A_i \wedge A_i \wedge \cdots \wedge [\bar{A}_i \vee A_n] \wedge [\bar{A}_i \vee A_n] \wedge \cdots \wedge A_{n-1}} \\
= & \overline{A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge [\bar{A}_i \vee A_n] \wedge \cdots \wedge A_{n-1} \wedge A_i \wedge [\bar{A}_i \vee A_n]} \\
\mathsf{s} & \overline{A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge [\bar{A}_i \vee A_n] \wedge \cdots \wedge A_{n-1} \wedge [(A_i \wedge \bar{A}_i) \vee A_n]} \\
\mathsf{i}\!\uparrow & \overline{A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge [\bar{A}_i \vee A_n] \wedge \cdots \wedge A_{n-1} \wedge A_n}
\end{array}
\qquad (4.1)
$$

In the third step, the proof of $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ is transformed into a proof of A_n by an application of the rule w↑.

It has been shown in [Bruscoli and Guglielmi 2009] (for xSKS) and [Straßburger 2012] (for eSKS), how this argument easily carries over when extension is present. However, as observed by Bruscoli [Guglielmi 2010], the same cannot be used when substitution is present: If in the argument above the formula A_n is obtained by applying the substitution rule to some A_i with $0 < i < n$, i.e., $A_n = \sigma A_i$ for some substitution σ, then in the sF-proof, the formula A_i is still available for later use. However, in sSKS, the substitution rule cannot be applied deeply. So, the whole conjunction $A_1 \wedge \cdots \wedge A_i \wedge A_i \wedge \cdots \wedge A_{n-1}$ is subject to the substitution, and a simple use of the c↑-rule is not enough to keep A_i for later reuse. Furthermore, all formulas in the chain are destroyed.

In order to make the argument work again, we have to find a way to apply the substitution such that both, A_i and σA_i, are subformulas of the resulting formula. To see how this can be achieved, consider first the substitution σ', that is obtained from σ

as follows:

$$\sigma' \;=\; \{\, a \mapsto a \wedge B \;\mid\; a \mapsto B \;\in\; \sigma \,\}$$

When we apply σ' to A_i we get a "merge" of A_i and $A_n = \sigma A_i$, and we would like to get two derivations

$$\begin{array}{c} \sigma' A_i \\ \| \\ A_i \end{array} \qquad \text{and} \qquad \begin{array}{c} \sigma' A_i \\ \| \\ \sigma A_i \end{array} \tag{4.2}$$

by using a series of $\mathsf{w}\!\uparrow$-applications. Depending on whether we chose to delete the new B-occurrences, or the superfluous a-occurrences, we can get

$$\mathsf{w}\!\uparrow \frac{F\{a \wedge B\}}{F\{a\}} \qquad \text{or} \qquad \mathsf{w}\!\uparrow \frac{F\{a \wedge B\}}{F\{B\}} \quad .$$

Of course this does not work because σ' sends $\bar{a}$ to $\bar{a} \vee \bar{B}$, and there is no way of getting back $\bar{a}$ nor $\bar{B}$ by a $\mathsf{w}\!\uparrow$ or any other sound inference rule. To overcome this problem, we construct now a slightly more complicated substitution σ^*, for which we can obtain something similar to (4.2). For every substitution σ used in the sF-proof we pick a fresh propositional variable x_σ, and we assign to σ the substitution σ^* as follows:

$$\sigma^* \;=\; \{\, a \mapsto [\bar{x}_\sigma \vee a] \wedge [x_\sigma \vee B] \;\mid\; a \mapsto B \;\in\; \sigma \,\} \tag{4.3}$$

This has the following crucial property:

LEMMA 4.1. *Let A be a formula and σ be a substitution and let x_σ be a fresh propositional variable. Then there are two* SKS*-derivations*

$$\begin{array}{c} \sigma^* A \wedge x_\sigma \\ \| \\ A \wedge x_\sigma \end{array} \qquad \textit{and} \qquad \begin{array}{c} \sigma^* A \wedge \bar{x}_\sigma \\ \| \\ \sigma A \wedge \bar{x}_\sigma \end{array} \tag{4.4}$$

of length $O(|A|^2)$ and width $O(|\sigma^* A|)$.

PROOF. First note that σ^* sends a to $[\bar{x}_\sigma \vee a] \wedge [x_\sigma \vee B]$ and $\bar{a}$ to $(x_\sigma \wedge \bar{a}) \vee (\bar{x}_\sigma \wedge \bar{B})$ if $a \mapsto B$ is in σ. The heart of our proof consists of the following four derivations:

$$\mathsf{w}\!\uparrow \dfrac{[\bar{x}_\sigma \vee a] \wedge [x_\sigma \vee B] \wedge x_\sigma}{\mathsf{s}\dfrac{[\bar{x}_\sigma \vee a] \wedge x_\sigma}{\mathsf{ai}\!\uparrow \dfrac{(\bar{x}_\sigma \wedge x_\sigma) \vee a}{a}}} \qquad \text{and} \qquad \mathsf{w}\!\uparrow \dfrac{[\bar{x}_\sigma \vee a] \wedge [x_\sigma \vee B] \wedge \bar{x}_\sigma}{\mathsf{s}\dfrac{[x_\sigma \vee B] \wedge \bar{x}_\sigma}{\mathsf{ai}\!\uparrow \dfrac{(x_\sigma \wedge \bar{x}_\sigma) \vee B}{B}}} \tag{4.5}$$

and

$$\mathsf{w}\!\uparrow \dfrac{[(x_\sigma \wedge \bar{a}) \vee (\bar{x}_\sigma \wedge \bar{B})] \wedge x_\sigma}{\mathsf{w}\!\uparrow \dfrac{[\bar{a} \vee (\bar{B} \wedge \bar{x}_\sigma)] \wedge x_\sigma}{\mathsf{s}\dfrac{[\bar{a} \vee \bar{x}_\sigma] \wedge x_\sigma}{\mathsf{ai}\!\uparrow \dfrac{\bar{a} \vee (\bar{x}_\sigma \wedge x_\sigma)}{\bar{a}}}}} \qquad \text{and} \qquad \mathsf{w}\!\uparrow \dfrac{[(x_\sigma \wedge \bar{a}) \vee (\bar{x}_\sigma \wedge \bar{B})] \wedge \bar{x}_\sigma}{\mathsf{w}\!\uparrow \dfrac{[(x_\sigma \wedge \bar{a}) \vee \bar{B}] \wedge \bar{x}_\sigma}{\mathsf{s}\dfrac{[x_\sigma \vee \bar{B}] \wedge \bar{x}_\sigma}{\mathsf{ai}\!\uparrow \dfrac{(x_\sigma \wedge \bar{x}_\sigma) \vee \bar{B}}{\bar{B}}}}} \tag{4.6}$$

Note how the structure of the formula after substitution allows us in (4.6) to overcome the problem of the naive approach using σ' mentioned above. The derivations in (4.4) are now obtained by plugging the derivations in (4.5) and (4.6) into each place in A

where a variable is affected by σ. The additional occurrence of x_σ (resp. $\bar{x}_\sigma$) is provided by the following derivation, which exists for every formula D and context $C\{\ \}$:

$$\mathsf{c}\!\uparrow \frac{C\{D\} \wedge x}{C\{D\} \wedge x \wedge x} \qquad \{\mathsf{s}\}\Big\Vert \Pi_s \qquad C\{D \wedge x\} \wedge x \tag{4.7}$$

where x is either x_σ or $\bar{x}_\sigma$, and where Π_s consists only of instances of s, and its length is linear in the depth of D in $C\{\ \}$. In our case, this is $O(|A|)$. The existence of Π_s can be shown by a straightforward induction on the structure of $C\{\ \}$ (see, e.g., [Straßburger 2003; Brünnler 2003b]). Furthermore, since the number of variables affected by σ in A is smaller than $|A|$, we have that the length of the overall derivations is $O(|A|^2)$. Finally, the width of the overall derivation is smaller than or equal to $|\sigma^* A| + 2$. □

We can now use this lemma to perform the inductive step that has been done for the rule of modus ponens in (4.1) above, also for the substitution rule. We obtain Π from Π' as follows (where A_n is obtained from A_i by applying σ):

$$\begin{array}{rc}
 & \Big\Vert \Pi' \\
\mathsf{c}\!\uparrow & A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1} \\ \hline
= & A_1 \wedge \cdots \wedge A_i \wedge A_i \wedge \cdots \wedge A_{n-1} \\ \hline
\mathsf{sub}\!\downarrow & A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1} \wedge A_i \\ \hline
\mathsf{ai}\!\downarrow & \sigma^*(A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1}) \wedge \sigma^* A_i \\ \hline
2{*}\mathsf{s} & \sigma^*(A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1}) \wedge \sigma^* A_i \wedge [x_\sigma \vee \bar{x}_\sigma] \\ \hline
 & (\sigma^*(A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1}) \wedge x_\sigma) \vee (\sigma^* A_i \wedge \bar{x}_\sigma) \\
 & \mathsf{SKS}\Big\Vert \text{Lemma 4.1} \\
\mathsf{sub}\!\downarrow & (A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1} \wedge x_\sigma) \vee (\sigma A_i \wedge \bar{x}_\sigma) \\ \hline
\mathsf{i}\!\uparrow & (A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1} \wedge \sigma A_i) \vee (\sigma A_i \wedge \overline{\sigma A_i}) \\ \hline
= & A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1} \wedge \sigma A_i \\ \hline
 & A_1 \wedge \cdots \wedge A_i \wedge \cdots \wedge A_{n-1} \wedge A_n
\end{array} \tag{4.8}$$

where in the first instance of $\mathsf{sub}\!\downarrow$ we use σ^* as substitution, as defined in (4.3), and in the second instance of $\mathsf{sub}\!\downarrow$, we use $\{x_\sigma \mapsto \sigma A_i\}$ as substitution, observing that x_σ occurs nowhere else.

We now have a direct proof of the following:

THEOREM 4.2. sSKS *p-simulates* sF.

PROOF. Given an sF-proof $A_1, A_2, \ldots, A_n$, where each A_k is either an axiom, or obtained via the substitution rule from some A_i with $1 \leqslant i < k$, or obtained via modus ponens from some A_i and A_j, where A_j is $A_i \Rightarrow A_k$ with $1 \leqslant i, j < k$. We construct an sSKS-proof Π of A_n of the following shape:

$$\begin{array}{c} \Big\Vert \Pi \\ \mathsf{w}\!\uparrow \dfrac{A_1 \wedge A_2 \wedge \cdots \wedge A_n}{A_n} \end{array}$$

where Π is obtained by induction on n, following the construction above. The overall size of the constructed sSKS derivation can be assessed as follows. Let m be the size of the sF-proof. The total length of the sSKS-derivation (using general rules) is bounded by a quadratic function in m, while width is $O(m^2)$, due to the substitution. This gives the combined estimate of size of $O(m^4)$. Abandoning general rules, i.e., replacing i↑, i↓, c↑, and c↓ by their atomic versions ai↑, ai↓, ac↑, and ac↓, respectively, increases the estimate for the size to $O(m^8)$. Removing all instances of ac↑ (i.e., replacing them by derivations consisting of ai↓, ai↑, ac↓, s) does not increase that estimate. □

In Lemma 4.1 and its corollary Theorem 4.2 the goal is to derive $B = \sigma A$ by a substitution from A, while keeping A. The main idea there is the essential use of substitution

$$\{x_\sigma \mapsto \sigma A\} \circ \sigma^* \;=\; \{\, a \mapsto (B \Rightarrow a) \wedge (\bar{B} \Rightarrow \sigma a) \mid a \text{ positive}\}$$

that encompasses the following reasoning: if B is true, map a to a, i.e. do nothing, keep A. If B is false, map a to whatever it is turned to by σ, to get B. The rest of the trick is suitable use of co-weakenings, as in (4.5) and (4.6), which is something we have tried to do with σ', but which fails for negative polarities. This time, the substitution works for negative polarities, since it maps

$$\bar{a} \mapsto (B \wedge \bar{a}) \vee (\bar{B} \wedge \overline{\sigma a}), \quad \text{for } a \text{ positive},$$

and the result entails $(B \Rightarrow \bar{a}) \wedge (\bar{B} \Rightarrow \overline{\sigma a})$, as can be seen by a single instance of the medial rule:

$$\mathsf{m}\,\frac{(\bar{a} \wedge B) \vee (\bar{B} \wedge \overline{\sigma a})}{[\bar{a} \vee \bar{B}] \wedge [B \vee \overline{\sigma a}]}$$

This gives an alternative way of obtaining the the two derivations in (4.6) by using an instance of medial (and commutativity of $\wedge$ and $\vee$):

$$\mathsf{m}\,\frac{[(x_\sigma \wedge \bar{a}) \vee (\bar{x}_\sigma \wedge \bar{B})] \wedge x_\sigma}{[\bar{x}_\sigma \vee \bar{a}] \wedge [x_\sigma \vee \bar{B}] \wedge x_\sigma}$$

followed by derivations of the same shape as the ones in (4.5).

Note how the described construction can be carried out in one substitution step instead of two, by using $\{\, a \mapsto [\bar{\sigma} A \vee a] \wedge [\sigma A \vee B] \;\mid\; a \mapsto B \;\in\; \sigma \,\}$. We present it in two separate steps for the sake of simpler exposition.

5. EXTENSION AND SUBSTITUTION IN CUT-FREE SYSTEMS

The work in [Straßburger 2012] has shown how extension and substitution can be used in cut-free systems. Furthermore, Theorem 3.10 immediately lifts to the cut-free case:

THEOREM 5.1. [Straßburger 2012] eKS *p-simulates* sKS.

However, the other direction remained open in [Straßburger 2012]. The reason is that xSKS was used to show that sSKS p-simulates eSKS, and thus, the cut played a crucial role.

In this section we give a direct proof showing that sKS also p-simulates eKS. The actual difficulty is that if we naively replace an instance of ext↓ by an instance of sub↓:

$$\mathsf{ext}{\downarrow}\,\frac{F\{a\}}{F\{A\}} \quad \rightsquigarrow \quad \mathsf{sub}{\downarrow}\,\frac{F\{a\}}{\sigma F\{a\}} \tag{5.1}$$

with $\sigma = \{a \mapsto A\}$, *all* occurrences of a in $F\{\ \}$ are replaced by A. This can lead to an exponential blow-up, due to the presence of contraction, as shown in the following example.

$a_1 \Leftrightarrow a_2 \vee a_2, \ \ a_2 \Leftrightarrow a_3 \vee a_3, \ \ldots, \ a_n \Leftrightarrow A$

$$
\begin{array}{rc}
 & S\{a_1 \vee a_1\} \\ \hline
\mathsf{ext}{\downarrow} & S\{a_1 \vee a_2 \vee a_2\} \\ \hline
\mathsf{c}{\downarrow} & S\{a_1 \vee a_2\} \\ \hline
\mathsf{ext}{\downarrow} & S\{a_1 \vee a_3 \vee a_3\} \\ \hline
\mathsf{c}{\downarrow} & S\{a_1 \vee a_3\} \\
 & \Vert \\
 & S\{a_1 \vee a_n \vee a_n\} \\ \hline
\mathsf{c}{\downarrow} & S\{a_1 \vee a_n\} \\ \hline
\mathsf{ext}{\downarrow} & S\{a_1 \vee A\} \\
 & \Vert \\
 & S\{A \vee A\} \\ \hline
\mathsf{c}{\downarrow} & S\{A\}
\end{array}
$$

$$\rightsquigarrow$$

$$
\begin{array}{rc}
 & S\{a_1 \vee a_1\} \\ \hline
\mathsf{sub}{\downarrow} & S\{a_2 \vee a_2 \vee a_2 \vee a_2\} \\ \hline
\mathsf{c}{\downarrow} & S\{a_2 \vee a_2 \vee a_2\} \\ \hline
\mathsf{sub}{\downarrow} & S\{a_3 \vee a_3 \vee a_3 \vee a_3 \vee a_3 \vee a_3\} \\ \hline
\mathsf{c}{\downarrow} & S\{a_3 \vee a_3 \vee a_3 \vee a_3 \vee a_3\} \\
 & \Vert \\
 & S\{a_n \vee a_n \vee \ldots \vee a_n \vee a_n \vee a_n\} \\ \hline
\mathsf{c}{\downarrow} & S\{a_n \vee a_n \vee \ldots \vee a_n \vee a_n\} \\ \hline
\mathsf{sub}{\downarrow} & S\{A \vee A \vee \cdots \vee A \vee A\} \\
 & \Vert \\
 & S\{A \vee A\} \\ \hline
\mathsf{c}{\downarrow} & S\{A\}
\end{array}
$$

Fig. 2. An example of an eKS derivation and a naive translation to sKS resulting in an exponential blow-up in size.

Example 5.2. Let $a_1 \Leftrightarrow a_2 \vee a_2$, $a_2 \Leftrightarrow a_3 \vee a_3$, ..., $a_n \Leftrightarrow A$ be the extension axioms in the eKS derivation depicted in the left part of Figure 2, whose size is is linear in n. The naive attempt to simply replace all the instances of extension by substitutions results in an exponential increase in size, as depicted on the right of that figure.

To overcome the problem of the exponential blow-up exhibited in Figure 2, we transform the whole derivation in a first step into a derivation with the property that whenever we encounter an instance of extension (3.5) with extension variable a, there is at most one other occurrence of a in the formula (namely as $\bar{a}$), so that the replacement (5.1) — done in the second step — causes only a limited increase of the size of the proof.

The first transformation is achieved by a rather aggressive renaming of extension variable occurrences in the derivation. Informally, this can be described using the notion of *atomic flows* [Guglielmi and Gundersen 2008; Guglielmi et al. 2010], which are similar to *logical flow-graphs* [Buss 1991], but which only trace occurrences of literals in the derivation: The vertices of the graph are the instances of the inference rules — except s and m, which are ignored by atomic flows. Then, the first transformation of our p-simulation consists of two sub-steps: first, we integrate all contraction nodes on extension variables into the corresponding extension rule node (done in Lemma 5.3 below). This does not change the size of the atomic flow (when size is counted as number of paths), but can cause a quadratic increase in the size of the derivation. Then we do the actual renaming that does not change the structure of the atomic flow. But after this renaming, every extension variable labels exactly two edges in the graph, one positively and one in negated form. This is done in Lemma 5.6.

We do not go into further details on atomic flows here, because first, they are not needed for the formal construction, second, they are only developed for the extension-free case and developing the theory of atomic flows for systems with extension would go beyond the scope of this paper, and third, atomic flows do not help at all in understanding the second transformation of our simulation (done in Lemma 5.8) which essentially performs steps of the form (5.1) and reintroduces contractions that have been deleted before. This has to be done in the right order to avoid the exponential blow-up shown in Figure 2 above.

For making the first transformation mentioned above formally correct, we need to generalize the extension rule. In particular, we need to allow extension variables to abbreviate more than one extension formula. We clearly have to take some precautions to avoid inconsistency.

Let $\mathcal{E}$ be a set of propositional variables. A *variable preorder* $\precsim$ is a a transitive and reflexive relation on $\mathcal{E}$. We write $a \sim b$ iff $a \precsim b$ and $b \precsim a$. We call a substitution σ *banal* if for all variables $a \notin \mathcal{E}$ we have $\sigma a = a$, and for all $a \in \mathcal{E}$ we have $\sigma a = b$ for some $b \sim a$. Note that $\sim$ is an equivalence relation that we can extend to all formulas as follows: We say $B \sim C$ iff there is a banal σ such that $\sigma B = \sigma C$.

Now, we define a set of *generalized extension axioms* to be a finite set of statements

$$a_i \stackrel{\sim}{\Leftrightarrow} A_i, \qquad 1 \leq i \leq k; \tag{5.2}$$

where the set $\{a_1, \ldots, a_k\}$ is equipped with a variable preorder, such that the following conditions are fulfilled:

(1) For all $i \in \{1, \ldots, k\}$, the variable a_i must not occur in the conclusion of a proof nor in any A_j with $a_j \precsim a_i$, and
(2) for all $i, j \in \{1, \ldots, k\}$, if $a_i \sim a_j$ then $A_i \sim A_j$.

As before, we call the a_i *extension variables* and the A_i *extension formulas*.

Notice how the standard definition of the set of extension axioms, which we now call *strict*, is a special case where every equivalence class in $\sim$ is singleton. Also, notice how the generalized definition allows simultaneous presence of $a \stackrel{\sim}{\Leftrightarrow} B$ and $a \stackrel{\sim}{\Leftrightarrow} C$, as long as B and C are in a same equivalence class under $\sim$.

We can now define a generalization of the extension rule given in (3.5):

$$\widetilde{\mathsf{ext}}{\downarrow}\,\frac{F\{b_1 \vee b_2 \vee \cdots \vee b_k \vee B_1 \vee B_2 \vee \cdots \vee B_m\}}{F\{A\}} \tag{5.3}$$

where $m, k \geqslant 0$ and

— for all $i \in \{1, \ldots, k\}$ we have either $b_i \stackrel{\sim}{\Leftrightarrow} A$ or $\bar{b}_i \stackrel{\sim}{\Leftrightarrow} \bar{A}$ is among the (generalized) extension axioms,
— either all $b_1, \ldots, b_k$ are positive atoms or all $b_1, \ldots, b_k$ are negated atoms,
— for all $i, j \in \{1, \ldots, k\}$, we have $b_i \sim b_j$,
— for all $i, j \in \{1, \ldots, m\}$ we have $B_i \sim B_j$,
— there is a banal substitution σ such that for all $j \in \{1, \ldots, m\}$ we have $\sigma B_j = A$.

An instance of $\widetilde{\mathsf{ext}}{\downarrow}$ is said to be *naive* if $m = 0$ and all b_i in (5.3) are equal to each other. We call an instance of $\widetilde{\mathsf{ext}}{\downarrow}$ *clever* if $m = 0$, all b_i in (5.3) are pairwise distinct, no extension variable in A occurs above the $\widetilde{\mathsf{ext}}{\downarrow}$-instance in the proof, and A does not contain two different occurrences of a same extension variable.

We define $\tilde{\mathsf{e}}\mathsf{sKS}$ to be the system obtained from sKS by adding the $\widetilde{\mathsf{ext}}{\downarrow}$-rule and allowing a set of generalized extension axioms. We call a derivation Π in $\tilde{\mathsf{e}}\mathsf{sKS}$

— *naive* if all instances of $\widetilde{\mathsf{ext}}{\downarrow}$ in Π are naive, the set of extension axioms is strict, and there is no instance of $\mathsf{sub}{\downarrow}$ in Π, and

— *clever* if
(1) every instance of $\widetilde{\mathsf{ext}}\downarrow$ in Π is clever,
(2) there is no instance of $\mathsf{sub}\downarrow$ in Π, and
(3) every extension variable occurs at most twice in each line of Π, once in positive form, and at most once in negated form, and if this is the case, the positive/negative pair can be traced up in Π to an instance of $\mathsf{ai}\downarrow$.

Clearly, every eKS-proof is at the same time also a naive $\tilde{\mathsf{e}}\mathsf{sKS}$-proof, because $\mathsf{ext}\downarrow$ is just a special case of naive $\widetilde{\mathsf{ext}}\downarrow$. Furthermore, every naive $\tilde{\mathsf{e}}\mathsf{sKS}$-proof can trivially be transformed into an eKS-proof by replacing all $\widetilde{\mathsf{ext}}\downarrow$-instances by a derivation of $\mathsf{ac}\downarrow$ and $\mathsf{ext}\downarrow$.

LEMMA 5.3. *Let Π be a naive $\tilde{\mathsf{e}}\mathsf{sKS}$ proof with conclusion B. Then there is a naive $\tilde{\mathsf{e}}\mathsf{sKS}$ proof Π' with conclusion B such that the rule $\mathsf{ac}\downarrow$ is never applied to an extension variable, and such that the size of Π' is $O(|\Pi|^2)$. Furthermore, Π' has the same extension axioms as Π.*

PROOF. To obtain Π', we iteratively permute the lowest $\mathsf{ac}\downarrow$ on an extension variable (or a negated extension variable) down in the derivation until it vanishes. This is done as follows (see also [Brünnler 2003b]): Consider the rule instance r immediately below such a contraction, where r is some rule in $\tilde{\mathsf{e}}\mathsf{sKS}$. There are two cases. If r is $\widetilde{\mathsf{ext}}\downarrow$ applied on the freshly obtained literal in the conclusion of the contraction then our instance of $\mathsf{ac}\downarrow$ can be removed as follows:

$$\widetilde{\mathsf{ext}}\downarrow \dfrac{\mathsf{ac}\downarrow \dfrac{F\{a \vee \cdots \vee a \vee a \vee \cdots \vee a\}}{F\{a \vee \cdots \vee a \vee \cdots \vee a\}}}{F\{A\}} \quad \rightsquigarrow \quad \widetilde{\mathsf{ext}}\downarrow \dfrac{F\{a \vee \cdots \vee a \vee a \vee \cdots \vee a\}}{F\{A\}}$$

In all other cases we can trivially permute r and $\mathsf{ac}\downarrow$:

$$\mathsf{r} \dfrac{\mathsf{ac}\downarrow \dfrac{F\{a \vee a\}}{F\{a\}}}{F'\{a\}} \quad \rightsquigarrow \quad \mathsf{ac}\downarrow \dfrac{\mathsf{r} \dfrac{F\{a \vee a\}}{F'\{a \vee a\}}}{F'\{a\}}$$

Since the conclusion of the proof does not contain any extension variables, all $\mathsf{ac}\downarrow$ on extension variables must eventually disappear. Now notice that the size increasing step is permuting the contraction with non-$\widetilde{\mathsf{ext}}\downarrow$ rules. One contraction on its way down can increase the size of the proof by at most the height h of the derivation. Thus, if c is the number of contractions in Π, then we have $h, c \leq |\Pi|$, and the size of Π' is dominated by $|\Pi| + c \cdot h$, which is $O(|\Pi|^2)$. $\square$

Example 5.4. Figure 3 shows an example of our construction. The first derivation in that figure is a proof in eKS and the second one is the result of applying Lemma 5.3 to it.

Remark 5.5. Note that the proof of Lemma 5.3 relies on the fact that we are cut-free. It would not work for $\tilde{\mathsf{e}}\mathsf{sSKS}$ (which is sSKS extended with $\widetilde{\mathsf{ext}}\downarrow$) because in the presence of cocontraction

$$\mathsf{c}\uparrow \dfrac{F\{A\}}{F\{A \wedge A\}} \qquad \text{or} \qquad \mathsf{ac}\uparrow \dfrac{F\{a\}}{F\{a \wedge a\}}$$

permuting down $\mathsf{ac}\downarrow$ leads to an exponential blow-up of the size of the proof.

$a \overset{\approx}{\Leftrightarrow} b, \quad b \overset{\approx}{\Leftrightarrow} C$	$a \overset{\approx}{\Leftrightarrow} b, \quad b \overset{\approx}{\Leftrightarrow} C$	$\begin{array}{l} a_1 \overset{\approx}{\Leftrightarrow} b_1, a_3 \overset{\approx}{\Leftrightarrow} b_1, \\ a_2 \overset{\approx}{\Leftrightarrow} b_2, a_1 \overset{\approx}{\Leftrightarrow} b_3, \\ b_1 \overset{\approx}{\Leftrightarrow} C, b_2 \overset{\approx}{\Leftrightarrow} C, \\ b_3 \overset{\approx}{\Leftrightarrow} C; \\ a_1 \sim a_2 \sim a_3, \\ b_1 \sim b_2 \sim b_3. \end{array}$	$\begin{array}{l} a_1 \overset{\approx}{\Leftrightarrow} b_1, a_3 \overset{\approx}{\Leftrightarrow} b_1, \\ a_2 \overset{\approx}{\Leftrightarrow} b_2, a_1 \overset{\approx}{\Leftrightarrow} b_3, \\ a \overset{\approx}{\Leftrightarrow} b, \quad b \overset{\approx}{\Leftrightarrow} C \\ b_3 \overset{\approx}{\Leftrightarrow} C; \\ a_1 \sim a_2 \sim a_3, \\ b_1 \sim b_2 \sim b_3. \end{array}$	$\begin{array}{l} a_1 \overset{\approx}{\Leftrightarrow} b_1, a_3 \overset{\approx}{\Leftrightarrow} b_1, \\ a_2 \overset{\approx}{\Leftrightarrow} b_2, a_1 \overset{\approx}{\Leftrightarrow} b_3, \\ a \overset{\approx}{\Leftrightarrow} b, \quad b \overset{\approx}{\Leftrightarrow} C \\ b_3 \overset{\approx}{\Leftrightarrow} C; \\ a_1 \sim a_2 \sim a_3, \\ b_1 \sim b_2 \sim b_3. \end{array}$
$\begin{array}{rc} \mathsf{i}\!\downarrow & \overline{a \vee \bar{a}} \\ \mathsf{w}\!\downarrow & \overline{a \vee a \vee \bar{a} \vee \bar{a}} \\ \mathsf{ac}\!\downarrow & \overline{a \vee a \vee \bar{a}} \\ \mathsf{ext}\!\downarrow & \overline{a \vee a \vee \bar{b}} \\ \mathsf{ext}\!\downarrow & \overline{a \vee b \vee \bar{b}} \\ \mathsf{ext}\!\downarrow & \overline{b \vee b \vee \bar{b}} \\ \mathsf{ac}\!\downarrow & \overline{b \vee \bar{b}} \\ \mathsf{ext}\!\downarrow & \overline{C \vee \bar{b}} \\ \mathsf{ext}\!\downarrow & \overline{C \vee \bar{C}} \end{array}$	$\begin{array}{rc} \mathsf{i}\!\downarrow & \overline{a \vee \bar{a}} \\ \mathsf{w}\!\downarrow & \overline{a \vee a \vee \bar{a} \vee \bar{a}} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{a \vee a \vee \bar{b}} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{a \vee b \vee \bar{b}} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{b \vee b \vee \bar{b}} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{C \vee \bar{b}} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{C \vee \bar{C}} \end{array}$	$\begin{array}{rc} \mathsf{i}\!\downarrow & \overline{a_1 \vee \bar{a}_1} \\ \mathsf{w}\!\downarrow & \overline{a_1 \vee a_2 \vee \bar{a}_3 \vee \bar{a}_1} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{a_1 \vee a_2 \vee \bar{b}_1} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{a_1 \vee b_2 \vee \bar{b}_1} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{b_3 \vee b_2 \vee \bar{b}_1} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{C \vee \bar{b}_1} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{C \vee \bar{C}} \end{array}$	$\begin{array}{rc} \mathsf{i}\!\downarrow & \overline{a_1 \vee \bar{a}_1} \\ \mathsf{w}\!\downarrow & \overline{a_1 \vee a_2 \vee \bar{a}_3 \vee \bar{a}_1} \\ \mathsf{sub}\!\downarrow & \overline{b_1 \vee a_2 \vee \bar{b}_1 \vee \bar{b}_1} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{b_1 \vee a_2 \vee \bar{b}_1} \\ \mathsf{sub}\!\downarrow & \overline{b_1 \vee b_2 \vee \bar{b}_1} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{b_1 \vee b_2 \vee \bar{b}_1} \\ \mathsf{sub}\!\downarrow & \overline{b_3 \vee b_2 \vee \bar{b}_3} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{b_3 \vee b_2 \vee \bar{b}_3} \\ \mathsf{sub}\!\downarrow & \overline{C \vee C \vee \bar{C}} \\ \widetilde{\mathsf{ext}}\!\downarrow & \overline{C \vee \bar{C}} \end{array}$	$\begin{array}{rc} \mathsf{i}\!\downarrow & \overline{a_1 \vee \bar{a}_1} \\ \mathsf{w}\!\downarrow & \overline{a_1 \vee a_2 \vee \bar{a}_3 \vee \bar{a}_1} \\ \mathsf{sub}\!\downarrow & \overline{b_1 \vee a_2 \vee \bar{b}_1 \vee \bar{b}_1} \\ \mathsf{c}\!\downarrow & \overline{b_1 \vee a_2 \vee \bar{b}_1} \\ \mathsf{sub}\!\downarrow & \overline{b_1 \vee b_2 \vee \bar{b}_1} \\ \mathsf{sub}\!\downarrow & \overline{b_3 \vee b_2 \vee \bar{b}_3} \\ \mathsf{sub}\!\downarrow & \overline{C \vee C \vee \bar{C}} \\ \mathsf{c}\!\downarrow & \overline{C \vee \bar{C}} \end{array}$

Fig. 3. Left to right: An example of an eKS derivation and constructions of Lemmas 5.3, 5.6, and reductions (5.5) and (5.6) of Lemma 5.8, resulting in an ẽsKS derivation without contractions on extension variables, a clever ẽsKS derivation, an intermediate ẽsKS derivation, and a sKS derivation, respectively. The upper row contains respectively strict or generalized extension axioms.

The next lemma says that every naive ẽKS proof with no contractions on extension variables can be transformed into a clever one of the same size. This time, however, the assigned set of extension axioms has to be transformed into a set of generalized ones.

LEMMA 5.6. *Let Π be a naive ẽsKS proof with conclusion B and with no contractions on extension variables. Then there is a clever ẽsKS proof Π' of size $|\Pi'| = |\Pi|$ with conclusion B and with no contractions on extension variables. The number of extension axioms of Π' is linear in $|\Pi|$.*

PROOF. In the given proof Π we proceed from top to bottom and whenever an extension variable occurrence a is introduced—this can happen in the conclusion of ai↓, or w↓, or $\widetilde{\mathsf{ext}}\!\downarrow$—we replace it by a fresh variable a'. In order to keep the proof a valid ẽsKS proof, we have to do two things:

(1) We have to trace this occurrence of a down in the proof and replace it everywhere by a'. Eventually this must reach the premise of an $\widetilde{\mathsf{ext}}\!\downarrow$-instance because a cannot occur in the conclusion of the proof. Since there is no contraction duplicating a, every rule instance remains valid, except for the $\widetilde{\mathsf{ext}}\!\downarrow$-instance in whose premise a' now occurs.
(2) In order to make this $\widetilde{\mathsf{ext}}\!\downarrow$-instance

$$\widetilde{\mathsf{ext}}\!\downarrow \frac{H\{a_1 \vee a_2 \vee \cdots \vee a_l \vee a' \vee a \vee a \vee \cdots \vee a\}}{H\{A\}}$$

valid again, where $a_1, a_2, \cdots, a_l$ are already renamed variables, we have to add an extension axiom. If a and a' are positive atoms, we add the axiom $a' \overset{\approx}{\Leftrightarrow} A$ and the equivalence $a' \sim a$. If a and a' are negative atoms, then we add $\bar{a}' \overset{\approx}{\Leftrightarrow} \bar{A}$ and the equivalence $\bar{a}' \sim \bar{a}$. This does not violate the conditions on sets of generalized extension axioms. If there are no occurrences of a left in the proof, we can remove $a \mathrel{\tilde{\Leftrightarrow}} A$ (or $\bar{a} \mathrel{\tilde{\Leftrightarrow}} \bar{A}$) from the set of extension axioms.

Now we have three cases.

— If we encounter an $\mathsf{ai}{\downarrow}$-instance with conclusion $F\{B \wedge [\bar{a} \vee a]\}$ where a is an extension variable, we replace it by an $\mathsf{ai}{\downarrow}$-rule with conclusion $F\{B \wedge [\bar{a}' \vee a']\}$, where a' is fresh. Then we perform Steps 1 and 2 above for the new occurrence of $\bar{a}'$ and the new occurrence of a'.

— If we encounter a $\mathsf{w}{\downarrow}$-instance with premise $F\{B\}$ and a conclusion $F\{B \vee C\}$, we perform Steps 1 and 2 above for each occurrence of an extension variable in C. In particular, if the same extension variable a appears more than once in C, then each occurrence is replaced by a new fresh variable.

— If we encounter an instance of $\widetilde{\mathsf{ext}}{\downarrow}$, then all extension variables in the premise of $\widetilde{\mathsf{ext}}{\downarrow}$ must already have been renamed (since we proceed from top to bottom in the proof) and belong to the same equivalence class of $\sim$. So, assume it is

$$\widetilde{\mathsf{ext}}{\downarrow}\,\frac{F\{b_1 \vee b_2 \vee \cdots \vee b_k\}}{F\{C\}} \tag{5.4}$$

As in the case for $\mathsf{w}{\downarrow}$, we have to perform Steps 1 and 2 above for each occurrence of an extension variable in C. As a consequence, the C in the conclusion is replaced by some formula C', whose extension variables are all fresh and mutually distinct. But this makes the instance (5.4) of $\widetilde{\mathsf{ext}}{\downarrow}$ invalid. In order to make it valid again, we have to add for every $i \in \{1, \ldots, k\}$ the extension axiom $b_i \mathrel{\tilde{\Leftrightarrow}} C'$ (or $\bar{b}_i \mathrel{\tilde{\Leftrightarrow}} \bar{C}'$). Again, this preserves the two conditions for sets of generalized extension axioms.

Then, the resulting proof Π' is clever, and clearly, no renaming changes the size of the proof, so that $|\Pi'| = |\Pi|$. The total number of new extension axioms is bounded by $2 \cdot n_{\mathsf{ai}\downarrow} + s_{\mathsf{w}\downarrow} + s_{\mathsf{ext}\downarrow}$, where $n_{\mathsf{ai}\downarrow}$ is the total number of $\mathsf{ai}{\downarrow}$ rules in Π, and $s_{\mathsf{w}\downarrow}$ and $s_{\mathsf{ext}\downarrow}$ are the total size of the formulas introduced in conclusions of $\mathsf{w}{\downarrow}$ and $\widetilde{\mathsf{ext}}{\downarrow}$, respectively. Clearly, the sum is $O(|\Pi|)$. □

Example 5.7. To continue Example 5.4, the third derivation in Figure 3 shows the result of applying Lemma 5.6.

LEMMA 5.8. *Let Π be a clever $\tilde{\mathsf{e}}\mathsf{sKS}$ proof with conclusion B. Then there is an sKS proof Π' with conclusion B and size $O(|\Pi|^{12})$.*

PROOF. This transformation is done in two steps. In the first one, we proceed from top to bottom and replace every instance of $\widetilde{\mathsf{ext}}{\downarrow}$ in Π, to obtain an intermediary $\tilde{\mathsf{e}}\mathsf{sKS}$ proof Π^*, as follows:

$$\widetilde{\mathsf{ext}}{\downarrow}\,\frac{F\{b_1 \vee \cdots \vee b_k \vee B_1 \vee \cdots \vee B_m\}}{F\{A\}} \quad\leadsto\quad \widetilde{\mathsf{ext}}{\downarrow}\,\frac{\mathsf{sub}{\downarrow}\,\dfrac{F\{b_1 \vee \cdots \vee b_k \vee B_1 \vee \cdots \vee B_m\}}{F'\{A \vee \cdots \vee A \vee B_1 \vee \cdots \vee B_m\}}}{F'\{A\}} \tag{5.5}$$

where the used substitution is $\{b_1 \mapsto A, \ldots, b_k \mapsto A\}$, and $F'\{\ \}$ is obtained from $F\{\ \}$ by applying this substitution. Since Π is clever, each b_i occurs at most once (in the form of $\bar{b}_i$) in $F\{\ \}$ and the path of this $\bar{b}_i$ ends in another $\widetilde{\mathsf{ext}}{\downarrow}$, which has as conclusion a formula from which $\bar{A}$ can be obtained by renaming extension variables occurring in A.

In particular, we have $B_i \sim B_j$ and $B_i \sim A$, for all $i, j \in \{1, \ldots, m\}$. Thus the instance of $\widetilde{\mathsf{ext}}{\downarrow}$ remains valid. Furthermore, in Π^*, all instances of $\widetilde{\mathsf{ext}}{\downarrow}$ are such that $k = 0$ and A does not contain two different occurrences of a same extension variable.

The transformation from Π to Π^* can increase the size of the proof. The length of Π^* is bound by $2 \cdot l$ where l is the length of Π, and the width of Π^* is bound by $w \cdot e \cdot f$ where w is the width of Π, and e is the maximal number of extension variables in a single formula in Π, and f is the maximal size of an extension formula appearing in Π. Since we have $e, f \leqslant w$, that entails $|\Pi^*|$ is $O(|\Pi|^3)$.

In the second step of our transformation, we remove all the resulting $\widetilde{\mathsf{ext}}{\downarrow}$-instances in Π^* as follows, again proceeding from top to bottom:

$$\widetilde{\mathsf{ext}}{\downarrow}\,\frac{F\{B_1 \vee B_2 \vee \cdots \vee B_m\}}{F\{A\}} \quad \leadsto \quad \begin{array}{c} \mathsf{sub}{\downarrow}\,\dfrac{F\{B_1 \vee B_2 \vee \cdots \vee B_m\}}{F'\{A \vee A \vee \cdots \vee A\}} \\ \{\mathsf{c}{\downarrow}\}\Big\| \\ F'\{A\} \end{array} \tag{5.6}$$

where the used substitution σ in the $\mathsf{sub}{\downarrow}$ is a renaming of extension variables that must exist by definition of $\widetilde{\mathsf{ext}}{\downarrow}$. Since σ changes the context $F\{\ \}$ into $F'\{\ \}$ it has an effect on the instances of $\widetilde{\mathsf{ext}}{\downarrow}$ below in the derivation:

$$\widetilde{\mathsf{ext}}{\downarrow}\,\frac{G\{C_1 \vee C_2 \vee \cdots \vee C_l\}}{G\{D\}} \quad \leadsto \quad \widetilde{\mathsf{ext}}{\downarrow}\,\frac{G'\{C'_1 \vee C'_2 \vee \cdots \vee C'_l\}}{G'\{D\}} \tag{5.7}$$

It remains to show that each of them remains a valid instance—the validity of the other rules is clearly not affected by the substitution. Now, note that σ is banal, i.e., just a renaming of extension variables occurring in some extension formulas. In particular, the image of such an extension formula under σ is another extension formula in the same equivalence class of $\sim$. Thus, every C'_i can still be substituted to D. Furthermore, if C'_i, C'_j share an extension variable, they must be the same, since every extension formula is fresh when introduced in Π. This means there is a substitution that can rewrite all C'_i into D. Thus, the instance of $\widetilde{\mathsf{ext}}{\downarrow}$ in the right of (5.7) remains valid if the one on the left is valid. This guarantees that we can perform (5.6) for all instances of $\widetilde{\mathsf{ext}}{\downarrow}$ in Π^*, and the resulting proof Π' is well defined.

The transformation $\Pi^* \mapsto \Pi'$ yields an increase in size which is the consequence of the increase in length alone, since all of the substitutions in (5.6) do not increase size. They are simply renamings of extension variables. The increase in length (using general contraction) is bounded by $e \cdot w$, where e stands for the number of $\widetilde{\mathsf{ext}}{\downarrow}$ rules in Π^*, and w for width of Π^*. With $e, w \leq |\Pi^*|$, one gets that the size of the derivation with $\widetilde{\mathsf{ext}}{\downarrow}$ removed is $O(|\Pi^*| + e \cdot w)$, that is, $O(|\Pi^*|^2)$.

Finally we can apply Proposition 3.2 to get a derivation in sKS. It is well known that this yields another quadratic increase in size of the derivation, [Brünnler and Tiu 2001], thus the overall size of Π' is $O(|\Pi^*|^4)$, and combined with the previous step, $O(|\Pi|^{12})$. □

Example 5.9. The fourth derivation in Figure 3 shows the result of exhaustively applying the reduction in (5.5) to the third derivation in that figure. Finally, the last derivation in that figure shows the result of the exhaustive application of (5.6). The full sequence of derivations in Figure 3 depicts the construction of an sKS proof from an eKS one.

THEOREM 5.10. sKS *p-simulates* eKS.

PROOF. As observed before, a given eKS proof Π is a naive $\tilde{\text{e}}$sKS proof. Now, we apply Lemmas 5.3, 5.6, and 5.8, giving us a sKS proof Π' with the same conclusion as Π and with size of $O(|\Pi|^{24})$. □

The main idea of the construction in this section is rather simple: diversify extension variables as much as possible, i.e. whenever two extension variables do not 'communicate' via structural rules, which is to say that they do not belong to a same connected component in the assigned proof net or atomic flow (graph) [Guglielmi and Gundersen 2008; Guglielmi et al. 2010], they should be named differently. We show that such a construction is possible, and we give sharp bounds on complexity. However, there is a simpler way to convince oneself that the construction is polynomial, since there is an important invariant in the construction: if Π is an eKS proof of A, every formula in every step of the transformation of Π to an sKS proof contains at most $|\Pi|^2$ occurrences of a same extension variable. In the same time, the total number of the extension variables introduced in the construction is polynomial (quadratic) in the size of Π.

6. FINAL REMARKS

In this paper we show a direct polynomial simulation of Frege systems with substitution in CoS with substitution, and we show that analytic CoS systems eKS and sKS with extension and substitution are p-equivalent. The Calculus of Structures is in focus of this work, as it is a first-class citizen for systems with both normalization and proof search. In fact, it is used as the basis of the *Profound* prover [Chaudhuri 2013a], which is an interactive theorem prover using subformula linking as an interaction method [Chaudhuri 2013b].

Moreover, in analytic systems, extension is naturally deep, reflecting the original Tseitin's transformation, making CoS the adequate framework for our discussion. Still, we note that both techniques demonstrated in our two proofs can be, mutatis mutandis, repeated in context of the prototypical representative of structural proof systems - Gentzen's LK, provided one allows extension rule to act deep inside a formula. We believe this fact to be a confirmation that both our results rely on features of structural systems in general.

Our result of direct simulation of sF in sSKS shows how substitution has the same power as extension in the presence of cut *using the techniques of structural systems alone*. Not only that it also gives a new proof of the p-equivalence of sF and eF using the simple, elegant steps from structural proof theory, it remedies a somewhat inferior status of structural proof theory, where facts about its complexity rely on results in other formalisms. Furthermore, while the result of polynomial simulation is not new, the fact that there is a polynomial transformation of sF in sSKS doesn't say anything about the simulation itself. In particular, it is possible that a polynomial transformation involves global transformation steps, as it is the case in Section 5. What we have shown is that the destructive effect of substitution in structural systems where it acts on entire sequents and prevents us from having access to the substituted formula, can be fixed by devising a clever substitution that can preserve access to the original formula. Furthermore, this is a *local* transformation of polynomial price.

The construction showing that SKS p-simulates Frege systems is very similar to the one showing that tree-like Frege systems p-simulate (dag-like) Frege systems [Krajíček 1996]. To show that SKS and tree-like Frege systems p-simulate each other is as straightforward as showing that SKS and Gentzen systems p-simulate each other [Brünnler and Tiu 2001]. This means that our construction of simulating sF in sSKS can also be used to give a direct proof that tree-like Frege systems with substitution can p-simulate dag-like Frege systems with substitution, which has been shown by other means in [Bonet and Galesi 1997].

One of the most important and very hard open problems in proof complexity is establishing the relation between cut and extension/substitution, usually formulated by asking if Frege systems p-simulate Frege systems with substitution. We already know that in the presence of cut, systems with extension and substitution are p-equivalent, and since [Straßburger 2012], we can ask the same question in cut-free systems. This is precisely the result of Section 5, pointing to the conclusion that the substitution vs. extension result is orthogonal to the presence of cut, and is not simply a consequence of a possible situation that Frege is the most economic proof system we have, i.e. as economical as eF or sF.

Assume for a second the opposite conclusion from what we have shown in Section 5, i.e., assume that substitution does not p-simulate extension in an analytic calculus of structures. In that case, cut would act as a p-equalizer for systems with extension and substitution, and would be capable of bridging the gap between the two in the absence of cut. Such a result would perhaps point to the possibility that Frege p-simulates Frege with substitution. However, the actual result of Section 5, provides no evidence in support of such claim.

In addition to the well-known and hard open problem of Frege vs. Frege with extension, there are others. In particular, one can formulate an analytic version of the problem: does KS p-simulate sKS or is there a class of tautologies witnessing separation? We strongly suspect latter to be the case, but negative complexity results in deep inference appear to be difficult, in general. One exception to that is a known fact [Bruscoli and Guglielmi 2009] that Statman tautologies [Statman 1978] have polynomial proofs in KS but no polynomial proof in cut-free LK. Another open problem is whether the separation of the two systems lifts to the case of sKS and LK with substitution.

Finally, a more pressing and maybe more delicate issue is *robustness* [Cook and Reckhow 1979], which says that any two Frege systems p-simulate each other, and therefore we are able to speak of *the* Frege system for classical logic. Robustness is enjoyed by any system where composition of derivations can be done at polynomial price, as it is the case with formalisms with cut. In particular, one can establish p-simulation results between Frege and calculus of structures *as formalisms*, relying on their robustness to abstract away from specific proof systems and axiomatizations of rules. However, systems without cut do not come equipped with a pre-defined notion of robustness, and it is not clear how such a notion should be formulated. The reason is that one has to define what it means to have an analytic proof system or even a cut-free system in the broadest sense. For example, it is well known that different cut-free sequent calculi *do not* p-simulate each other, not to speak of analytic tableaux, resolution, or truth tables, which are all incomparable with respect to p-simulation [D'Agostino 1992; Brünnler 2003b]. However, it has long been known [Guglielmi 2003; Brünnler and Tiu 2001], and recently been investigated in a systematic way [Das 2012], that KS can p-simulate truth tables, analytic tableaux, tree-like resolution, and tree-like cut-free sequent calculi. It is conjectured that it also p-simulates dag-like sequent calculi and dag-like resolution.

This makes KS a good candidate for *the* cut-free system. In particular the formulation of KS is independent of the presence of the constants **t** and **f** for *truth* and *fal-*

sum, respectively. This has first been observed in [Straßburger 2012] and formally proved in [Das 2013]. This proof can easily be extended to the presence of extension/substitution: the only critical case is when the extension formula is a constant, i.e., we have extension axioms $a_i \Leftrightarrow \mathbf{t}$ or $a_i \Leftrightarrow \mathbf{f}$. But in that pathological case the naïve method of eliminating extension can be applied without the exponential blow-up that happens in the general case.

Another important observation is related to the co-contraction rule $\mathsf{c}\!\uparrow$ of SKS which is analytic in the sense that all of the ingredients of the premise are present in the conclusion, but when added to KS, it allows for quasi-polynomial simulation of Frege systems [Jeřábek 2009; Bruscoli et al. 2010]. This gives us, *a priori*, four inference rules for *proof compression* by which KS can be augmented: cut, co-contraction, extension, and substitution. The contribution of this paper is to show that there is no difference between extension and substitution, with respect to p-simulation. As observed by Das[1], substitution can p-simulate atomic co-contraction $\mathsf{ac}\!\uparrow$ when co-weakening is present: just use the substitution $\sigma = \{a \mapsto a \wedge a\}$ (respectively $\sigma = \{a \mapsto a \vee a\}$), and then use a series of contractions and co-weakenings to undo the substitution in the context of the $\mathsf{ac}\!\uparrow$-instance to be simulated. However, it is not clear whether such a result can be obtained in the absence of co-weakening.

Finally, the relation between cut and substitution remains the most prominent open problem in this area.

Acknowledgments

The authors would like to thank Anupam Das for proofreading an early version of the paper. We would also like to thank Alessio Guglielmi, Samuel Buss, and anonymous reviewers for their suggestions on how to improve the presentation.

REFERENCES

Noriko H. Arai. 1996. Tractability of Cut-Free Gentzen Type Propositional Calculus with Permutation Inference. *Theor. Comput. Sci.* 170, 1-2 (1996), 129–144.

Maria Luisa Bonet and Nicola Galesi. 1997. Linear Lower Bounds and Simulations in Frege Systems with Substitutions. In *CSL'97 (LNCS)*, Mogens Nielsen and Wolfgang Thomas (Eds.), Vol. 1414. Springer, 115–128.

Kai Brünnler. 2003a. Atomic Cut Elimination for Classical Logic. In *CSL 2003 (Lecture Notes in Computer Science)*, M. Baaz and J. A. Makowsky (Eds.), Vol. 2803. Springer-Verlag, 86–97.

Kai Brünnler. 2003b. *Deep Inference and Symmetry for Classical Proofs*. Ph.D. Dissertation. Technische Universität Dresden.

Kai Brünnler. 2006. Cut Elimination inside a Deep Inference System for Classical Predicate Logic. *Studia Logica* 82, 1 (2006), 51–71.

Kai Brünnler and Alwen Fernanto Tiu. 2001. A Local System for Classical Logic. In *LPAR 2001 (LNAI)*, R. Nieuwenhuis and A. Voronkov (Eds.), Vol. 2250. Springer, 347–361.

Paola Bruscoli and Alessio Guglielmi. 2009. On the Proof Complexity of Deep Inference. *ACM Transactions on Computational Logic* 10, 2 (2009), 1–34. Article 14.

Paola Bruscoli, Alessio Guglielmi, Tom Gundersen, and Michel Parigot. 2010. A Quasipolynomial Cut-Elimination Procedure in Deep Inference via Atomic Flows and Threshold Formulae. In *LPAR-16 (LNCS)*, Vol. 6355. Springer-Verlag, 136–153.

Samuel R. Buss. 1991. The undecidability of k-provability. *Annals of Pure and Applied Logic* 53 (1991), 72–102.

Kaustuv Chaudhuri. 2013a. Profound: a linking-based interactive prover. (2013). Available at: http://chaudhuri.info/software/profound/.

[1] Personal communication.

Kaustuv Chaudhuri. 2013b. Subformula Linking as an Interaction Method. In *Proceedings of the 4th Conference on Interactive Theorem Proving (ITP) (Lecture Notes in Computer Science)*, Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie (Eds.), Vol. 7998. Springer, 386–401.

Kaustuv Chaudhuri, Nicolas Guenot, and Lutz Straßburger. 2011. The Focused Calculus of Structures. In *CSL'11 (LIPIcs)*, Marc Bezem (Ed.), Vol. 12. Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 159–173.

Stephen A. Cook and Robert A. Reckhow. 1979. The Relative Efficiency of Propositional Proof Systems. *The Journal of Symbolic Logic* 44, 1 (1979), 36–50.

Marcello D'Agostino. 1992. Are tableaux an improvement on truth-tables? *Journal of Logic, Language and Information* 1 (1992), 235–252.

Anupam Das. 2012. Complexity of Deep Inference via Atomic Flows. In *Computability in Europe (LNCS)*, S. Barry Cooper, Anuj Dawar, and Benedikt Löwe (Eds.), Vol. 7318. Springer-Verlag, 139–150.

Anupam Das. 2013. Rewriting with Linear Inferences in Propositional Logic. In *24th International Conference on Rewriting Techniques and Applications (RTA) (Leibniz International Proceedings in Informatics (LIPIcs))*, Femke van Raamsdonk (Ed.), Vol. 21. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 158–173.

Martin Dowd. 1985. Model-theoretic aspects of $\mathcal{P} \neq \mathcal{NP}$. (1985). Manuscript.

Gerhard Gentzen. 1934. Untersuchungen über das logische Schließen. I. *Mathematische Zeitschrift* 39 (1934), 176–210.

Alessio Guglielmi. 2003. Resolution in the Calculus of Structures. (2003). Note. On the web at: http://cs.bath.ac.uk/ag/p/AG10.pdf.

Alessio Guglielmi. 2007. A System of Interaction and Structure. *ACM Transactions on Computational Logic* 8, 1 (2007), 1–64.

Alessio Guglielmi. 2010. (2010). Email to the frogs mailing list, archived at http://article.gmane.org/gmane.science.mathematics.frogs/575/.

Alessio Guglielmi and Tom Gundersen. 2008. Normalisation Control in Deep Inference Via Atomic Flows. *Logical Methods in Computer Science* 4, 1:9 (2008), 1–36. http://arxiv.org/abs/0709.1205

Alessio Guglielmi, Tom Gundersen, and Lutz Straßburger. 2010. Breaking Paths in Atomic Flows for Classical Logic. In *LICS 2010*.

Alessio Guglielmi and Lutz Straßburger. 2001. Non-commutativity and MELL in the Calculus of Structures. In *Computer Science Logic, CSL 2001 (LNCS)*, Laurent Fribourg (Ed.), Vol. 2142. Springer-Verlag, 54–68.

Alessio Guglielmi and Lutz Straßburger. 2011. A system of interaction and structure V: the exponentials and splitting. *Mathematical Structures in Computer Science* 21, 3 (2011), 563–584.

Emil Jeřábek. 2009. Proof complexity of the cut-free calculus of structures. *Journal of Logic and Computation* 19, 2 (2009), 323–339.

Ozan Kahramanoğulları. 2006. Reducing Nondeterminism in the Calculus of Structures. In *LPAR 2006 (Lecture Notes in Artificial Intelligence)*, M. Hermann and A. Voronkov (Eds.), Vol. 4246. Springer-Verlag, 272–286. http://www.doc.ic.ac.uk/~ozank/Papers/reducingNondet.pdf

Jan Krajíček. 1996. *Bounded Arithmetic, Propositional Logic and Complexity Theory*. Cambridge University Press.

Jan Krajíček and Pavel Pudlák. 1989. Propositional Proof Systems, the Consistency of First Order Theories and the Complexity of Computations. *The Journal of Symbolic Logic* 54, 3 (1989), 1063–1079.

Richard Statman. 1978. Bounds for proof-search and speed-up in predicate calculus. *Annals of Mathematical Logic* 15 (1978), 225–287.

Lutz Straßburger. 2003. *Linear Logic and Noncommutativity in the Calculus of Structures*. Ph.D. Dissertation. Technische Universität Dresden.

Lutz Straßburger. 2012. Extension without Cut. *Annals of Pure and Applied Logic* 163, 12 (2012), 1995–2007.

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

G. S. Tseitin. 1968. On the complexity of derivation in propositional calculus. *Zapiski Nauchnykh Seminarou LOMI* 8 (1968), 234–259.