On the Power of Substitution in the Calculus of Structures

Novak Novaković* Lutz Straßburger†

November 8, 2013

Abstract

In this paper we give a direct and simple 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 extended Frege systems. In the second part of the paper, we then show that the cut-free calculus of structures with substitution is p-equivalent to the cut-free calculus of structures with extension.

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 [CR79], Cook and Reckhow have shown that Frege systems with substitution can p-simulate Frege systems with extension, and 10 years later, Krajíček and Pudlák have shown in [KP89] 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 [BG09] have shown that also deep inference proof systems, like the calculus of structures (CoS) [Gug07, BT01, GS01], can provide a natural framework for studying extension and substitution. As shown in [BG09], 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 first class proof formalism coming with methods for proof search [Kah06, CGS11, Cha13] and proof normalization [Brü03a, Brü06, SG11, GS11]. This means that we can now study cut-free proof systems with extension and substitution [Str12].

The purpose of this paper is to fill two gaps that have been left open in the previous work [BG09, Str12] 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 [BG09], 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. These translation carry 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 [Gug10]. 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 [Str12] 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 [KP89].

2. In [Str12], 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.

---

*Partly supported by the ANR, project “STRUCTURAL”, and by the Ministry of Education and Science of Serbia, project ON 174026
†Partly supported by the ANR, project “STRUCTURAL”
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 $A\ell = \{a, b, c, \ldots\}$ be a countable set of propositional variables, also called atoms, and let $\overline{A}\ell = \{\overline{a}, \overline{b}, \overline{c}, \ldots\}$ be the assigned set of negated atoms. We refer to elements of $A\ell$ and $\overline{A}\ell$ as literals. The set of Boolean propositional formulas $\text{Form}$ whose elements are denoted by capital Latin letters $(A, B, C, \ldots)$ is the smallest language over the alphabet $A\ell \cup \overline{A}\ell \cup \{\wedge, \vee, (, ), [ , ]\}$, such that $A\ell, \overline{A}\ell \subset \text{Form}$, and if $A, B \in \text{Form}$, then $(A \wedge B) \in \text{Form}$ and $[A \vee B] \in \text{Form}$. 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 the Boolean negation as non-primitive. For an atom $a$, its negation is defined as its assigned negated atom $\overline{a}$. Then the definition is extended to arbitrary formulas by de Morgan laws: $\overline{a} = a$ and $\overline{A \wedge B} = \overline{A} \vee \overline{B}$ and $\overline{A \vee B} = \overline{A} \wedge \overline{B}$. This entails $\overline{\overline{A}} = A$ for all $A$. Implication $A \Rightarrow B$ is defined as $\overline{A} \vee B$ and equivalence $A \Leftrightarrow B$ as $[\overline{A} \vee B] \wedge [\overline{B} \vee A]$.

Proof systems We adopt a general view of proof systems as presented in [CR79]. A proof system is defined as a surjective $\text{PTIME}$ function $S : \Sigma^* \rightarrow T$, from a set of finite words $\Sigma^*$ over a signature $\Sigma$ to the set $T$ of all propositional tautologies. The assignment $S : \Pi \mapsto S(\Pi)$ assigns to an element of $\Sigma^*$, called a proof, its conclusion. A size of a proof is a function $|\cdot| : \Sigma^* \rightarrow \mathbb{N}$, assigning to a proof $\Pi$ the number $|\Pi|$ of symbols in $\Pi$. For proof systems $S_1 : \Sigma_1^* \rightarrow T$ and $S_2 : \Sigma_2^* \rightarrow T$ 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 $\Sigma_1^*$ can be assigned proofs $\Sigma_2^*$ of same conclusions whose size is dominated by a fixed polynomial in the size of $\Sigma_1^*$ 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 of the form

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

$2$
where $B_1, \ldots, B_n, B$ are formula variables. 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 generally attributed to Frege as they were introduced in their full generality in Frege’s ground-breaking [Fre79], but they also appear in literature as Hilbert-Frege, Hilbert or Hilbert-Ackermann systems [Hil22, HA28]. 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):

\[
\begin{align*}
\text{AX-1:} & \quad \bar{A} \lor [\bar{B} \lor A] \\
\text{AX-2:} & \quad (A \land (B \lor \bar{C})) \lor [(A \land \bar{B}) \lor [\bar{A} \lor C]] \\
\text{AX-3:} & \quad (B \land A) \lor [(B \land \bar{A}) \lor B]
\end{align*}
\]

where $A$, $B$, and $C$ are formula variables, and a single inference rule modus ponens, $\text{MP}$:

\[
\begin{array}{c}
\text{MP} \\
\hline
A \lor B \\
\hline
B
\end{array}
\]

Besides the essential properties of soundness and completeness of the Frege system for classical propositional logic, it has been shown in [CR79] that all Frege systems for the logic $p$-simulate each other. That allows us to think of the system $\text{FREGE}$ 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.** Every Frege system is $p$-equivalent to sequent calculus for classical propositional logic with cut. [CR79]

**Extension** The notion of extension in Frege systems, due to Tseitin [Tse68], comes from the idea of using abbreviations in a proof. The concept can be formalized as follows. An extended Frege system is a Frege system whose set of axioms $Ax$ is augmented by the extension axioms of the form

\[
a_i \iff A_i, \quad 1 \leq i \leq k;
\]

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 $j < i$. We call the $a_i$ extension variables and the $A_i$ extension formulas. We write $xFREGE$ 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 $\sigma : At \rightarrow Form$ from the set of atoms to the set of formulas, such that $\sigma(a) = a$ holds on all but finitely many atoms in $At$. The reader should notice that there is no constraint put on the nature of the map $\sigma$, as it is the case with extension. To have substitution in a Frege system amounts to adding an inference rule, called the substitution rule

\[
\begin{array}{c}
\text{sub}_{\sigma} \hline
A \\
\hline
\sigma A
\end{array}
\]

(2.3)

to the system. We refer to $\text{FREGE}$ augmented by the substitution rule as $sFREGE$.

**Theorem 2.2.** $sFREGE$ $p$-simulates $xFREGE$. [CR79]

**Theorem 2.3.** $xFREGE$ $p$-simulates $sFREGE$. [KP89]

### 3 Preliminaries on Calculus of Structures

**Inference rules** The paradigm of deep inference, materialized in calculus of structure [BT01, Gug07, GS01], stems from the idea that one is allowed to apply inference rules arbitrarily deep inside a formula, to the contrast with sequent calculus or natural deduction [Gen34] where rules are always applied on the
outermost connectives. In this paper we follow the formulations as given in [Str12]. We use the following rule schemata:

\[
\begin{align*}
\text{ai} & \downarrow \quad F\{B\} \quad F\{B \land [\overline{a} \lor a]\}, \quad F\{B\} \text{ is allowed to be empty} \\
\text{m} & \downarrow \quad F\{(A \land B) \lor (C \land D)\} \quad F\{F\{B\} \land [B \lor D]\} \\
\text{s} & \downarrow \quad F\{[A \lor B] \land C\} \quad F\{F\{A \land C\} \lor B\} \\
\text{w} & \downarrow \quad F\{B\} \quad F\{B \land A\} \\
\text{ac} & \downarrow \quad F\{a \lor a\} \quad F\{a\}.
\end{align*}
\]

(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 rules in (3.1) are called (atomic) identity, switch, medial, weakening and (atomic) contraction, respectively. On the set Form of formulas we define the relation = to be the smallest congruence generated by

\[
\begin{align*}
A \land (B \land C) &= (A \land B) \land C \\
A \land [B \land C] &= [A \land B] \land C \\
A \lor (B \lor C) &= [A \lor B] \lor C \\
A \lor [B \lor C] &= [A \lor B] \lor C
\end{align*}
\]

(3.2)

Then, we add another inference rule

\[
\frac{F\{A\}}{F\{B\}}
\]

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

\[
A \quad s\|\quad B
\]

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

\[
A \quad s\|\quad B
\]

for a derivation in the system \(S\) with no premise and with conclusion \(B\). In this case we also say that \(\Pi\) is a proof of \(B\).

**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 [BT01] differs from ours; it relies on the presence of units for disjunction and conjunction in syntax, \(f\) and \(t\), respectively. It is argued in [Str12] how our presentation is only a mild variation to the presentation of KS in [BT01], 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.** The system KS is sound and complete for classical logic, i.e. for any propositional formula is a tautology iff there is a KS proof of it. [BT01]

**Proposition 3.2.** The inference rules

\[
\begin{align*}
\text{i} & \downarrow \quad F\{B\} \quad F\{B \land [\overline{A} \lor A]\} \\
\text{c} & \downarrow \quad F\{A \lor A\} \quad F\{A\}
\end{align*}
\]

are derivable in KS, where in \(\text{i}\) the premise \(F\{B\}\) is allowed to be empty. Moreover, KS p-simulates KS \(\cup\{\text{i, c}\}\). [BT01]

The rules \(\text{i}\) and \(\text{c}\) are the non-atomic versions of identity and contraction rules, respectively.

**Proposition 3.3.** The system KS p-simulates cut-free sequent calculus. But the opposite does not hold. [BT01, BG09]
Cut and system SKS  The (atomic) cut rule in deep inference systems is dual to the (atomic) identity

\[
\frac{F\{B \land (\bar{a} \land a)\}}{ai\uparrow} F\{B\}.
\] (3.4)

We refer to the system \(KS \cup \{ai\uparrow\}\) as \(SKS\).

Again, this definition of the system \(SKS\) is a mild modification of the original definition of \(SKS\) found in [BT01]. 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.** The following rules are derivable in \(SKS\)

\[\begin{align*}
\frac{F\{B \lor (\bar{a} \land a)\}}{ci\uparrow} F\{B\} \\
\frac{F\{A\}}{wi\uparrow} F\{A \land B\} \quad & F\{A \land B\}
\end{align*}\]

Moreover, \(SKS\) p-simulates \(SKS \cup \{i\uparrow, c\uparrow, w\uparrow\}\). [BT01]

**Proposition 3.5.** There is an \(SKS\) derivation from \(A\) to \(B\) if and only if \(A \Rightarrow B\) is a tautology. [BT01]

**Theorem 3.6.** \(SKS\) and \(FREGE\) are p-equivalent. [BG09]

Note that this follows from Theorem 2.1 and the p-equivalence of \(SKS\) and sequent calculus. But Bruscoli and Guglielmi give in [BG09] a direct construction. To show how \(SKS\) can be p-simulated in \(FREGE\), it suffices to first exhibit a \(FREGE\) proof of \(A \Rightarrow B\) for every \(SKS\) rule \(F\{A\}\) r \(− − − − \) \(F\{B\}\). Then, it can be shown by induction on the size of the context \(F\{\}\) that there is a \(FREGE\) 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 \(FREGE\) in \(SKS\) will be discussed in detail in Section 4.

**Proposition 3.7.** \(xSKS\) and \(xFREGE\) are p-equivalent. [BG09]

The second way of adding extension to \(SKS\), proposed in [Str12], is to add for every extension axiom \(a_i \Leftrightarrow A_i\) the two rules

\[
\begin{align*}
\text{ext}_i\downarrow F\{a_i\} & \quad F\{A_i\} \\
\text{ext}_{\bar{a}_i}\downarrow F\{\bar{a}_i\} & \quad F\{\bar{A}_i\}
\end{align*}\] (3.5)

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

**Theorem 3.8.** \(xSKS\) and \(eSKS\) are p-equivalent. [Str12]

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

\[
\frac{A}{\sigma A \quad \text{sub}_\downarrow}.
\] (3.6)

for a given a substitution \(\sigma : A \rightarrow Form\). 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 \(KS \cup \{\text{sub}\downarrow\}\), and \(sSKS\) to be \(SKS \cup \{\text{sub}\downarrow\}\).

The following have been shown previously via simple direct constructions:

**Theorem 3.9.** \(sSKS\) p-simulates \(xSKS\). [BG09]

**Theorem 3.10.** \(eSKS\) p-simulates \(sSKS\). [Str12]
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.** sFREGE p-simulates sSKS. [BG09]

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.** sFREGE, xFREGE, 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 sFREGE in any of sSKS, xSKS, or eSKS. This has lead to the assumption that substitution in the calculus of structures is “morally” the same as extension, and an a priori weaker concept than substitution in Frege systems [Gug10]. In the following section we show that this is not justified. We show that sSKS p-simulates sFREGE by giving a direct construction which follows the scheme of the p-simulation of FREGE in SKS (Theorem 3.6).

### 4 Substitution in Frege and CoS

Let us start by recalling the simple construction by Bruscoli and Guglielmi [BG09] for translating a FREGE-proof into an SKS-proof, with a polynomial blow-up. This is done in three steps. First, we observe that every axiom $A$ in the Frege system has an SKS proof $\Pi_A$ of size $O(|A|^2)$. Second, from a given FREGE-proof $A_1, A_2, \ldots, A_n$, we proceed by induction on $n$ to produce an SKS-proof $\Pi$ of the conjunction $A_1 \land A_2 \land \cdots \land A_n$. This is done as follows. Assume by induction hypothesis an SKS-proof $\Pi'$ of the conjunction $A_1 \land A_2 \land \cdots \land A_{n-1}$. If $A_n$ is an axiom, we immediately obtain $\Pi$ by combining $\Pi'$ and the proof $\Pi_{A_n}$ of $A_n$. If $A_n$ is obtained by applying modus ponens to some $A_i$ and $A_j$ with $A_j = A_i \Rightarrow A_n$ and $0 < i, j < n$, then we obtain $\Pi$ from $\Pi'$ as follows:

$$\begin{align*}
2 \ast &\quad \frac{A_1 \land \cdots \land A_i \land \cdots \land [A_i \lor A_n] \land \cdots \land A_{n-1}}{A_1 \land \cdots \land A_i \land \cdots \land [A_i \lor A_n] \land \cdots \land A_{n-1} \land A_j \land [A_j \lor A_n]} \\
&\quad \frac{s\Pi}{A_1 \land \cdots \land A_j \land \cdots \land [A_j \lor A_n] \land \cdots \land A_{n-1} \land A_n}
\end{align*}$$

(4.1)

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

It has been shown in [BG09] (for xSKS) and [Str12] (for eSKS), how this argument easily carries over when extension is present. However, as observed by Bruscoli [Gug10], 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 $\sigma$, then in the FREGE-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 $A_1 \land \cdots \land A_i \land \cdots \land A_{n-1}$ is subject to the substitution, and a simple use of the $\ast$-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 use the following idea. Let $\sigma$ be a substitution used in the FREGE-proof, and let $\sigma'$ be a substitution obtained from $\sigma$ as follows:

$$\sigma' = \{ a \mapsto a \land B \mid a \mapsto B \in \sigma \}$$

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

$$\begin{align*}
\sigma' A_i, \\
A_i \quad \text{and} \quad \sigma A_i
\end{align*}$$

(4.2)
by using a series of \( w \)-applications we can get depending on whether we chose to delete the new \( B \)-occurrences, or the superfluous \( a \)-occurrences:

\[
\begin{align*}
\frac{F(a \land B)}{F(a)} & \quad \text{or} \quad \frac{F(a \land B)}{F(B)}
\end{align*}
\]

Of course this does not work because \( \sigma' \) sends \( \bar{a} \) to \( \bar{a} \lor \bar{B} \), and there is no way of getting back \( \bar{a} \) nor \( \bar{B} \) by a \( w \)-rule or any other sound inference rule. But by using a slightly more complicated substitution than \( \sigma' \), we can obtain something similar to (4.2). For every substitution \( \sigma \) used in the sFREGE-proof we pick a fresh propositional variable \( x_\sigma \). Now we assign to \( \sigma \) the substitution \( \sigma^* \) as follows:

\[
\sigma^* = \{ a \mapsto [x_\sigma \lor a] \land [x_\sigma \lor B] \mid a \mapsto B \in \sigma \}
\]  

(4.3)

This has the following crucial property:

**Lemma 4.1.** Let \( A \) be a formula and \( \sigma \) be a substitution and let \( x_\sigma \) be a fresh propositional variable. Then there are two SKS-derivations

\[
\sigma^* A \land x_\sigma \quad \text{and} \quad \sigma^* A \land \bar{x}_\sigma
\]

(4.4)

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

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

\[
\begin{align*}
\frac{[x_\sigma \lor a] \land [x_\sigma \lor B] \land x_\sigma}{w}
& \quad \text{and} \quad \frac{[x_\sigma \lor B] \land \bar{x}_\sigma}{a}, \\
\frac{[x_\sigma \land \bar{a}] \land [x_\sigma \land \bar{B}] \land x_\sigma}{m}
& \quad \text{and} \quad \frac{[x_\sigma \land \bar{B}] \land \bar{x}_\sigma}{a}.
\end{align*}
\]

(4.5)

and

\[
\begin{align*}
\frac{[x_\sigma \land \bar{a}] \land [x_\sigma \land \bar{B}] \land x_\sigma}{w}
& \quad \text{and} \quad \frac{[x_\sigma \land \bar{B}] \land \bar{x}_\sigma}{a}, \\
\frac{[x_\sigma \lor a] \land [x_\sigma \lor B] \land x_\sigma}{m}
& \quad \text{and} \quad \frac{[x_\sigma \lor B] \land \bar{x}_\sigma}{a}.
\end{align*}
\]

(4.6)

Note the crucial use of the \( m \)-rule that allows us to overcome the problem of the naive approach using \( \sigma' \) 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 \( \sigma \). The additional occurrence of \( x_\sigma \) (resp. \( \bar{x}_\sigma \)) is provided by the following derivation, which exists for every formula \( D \) and context \( C \{ \} \):

\[
\begin{align*}
\frac{C(D) \land x}{\text{ac}^\downarrow} \\
\frac{\{s\} \parallel \Pi, \quad C(D \land x) \land x}{\parallel}
\end{align*}
\]

(4.7)

where \( x \) is either \( x_\sigma \) or \( \bar{x}_\sigma \), and where \( \Pi_e \) consists only of instances of \( s \), and its length is linear in the depth of \( D \) in \( C \{ \} \). In our case, this is \( O(|A|) \). Furthermore, since the number of variables affected by \( \sigma \) in \( A \) is smaller than \( |A| \), we have that the length of the overall derivations is \( O(|A|^2) \). Finally, the size of each line in the overall derivation is smaller than or equal to \( |\sigma^* A| + 2 \).

We can now use this lemma to perform the inductive step above to obtain \( \Pi \) from \( \Pi' \) as follows (where
$A_n$ is obtained from $A_i$ by applying $\sigma$:

\[
\begin{align*}
\Pi' & = A_1 \land \cdots \land A_i \land \cdots \land A_{n-1} \\
\Pi'_{\downarrow} & = A_1 \land \cdots \land A_i \land \cdots \land A_{n-1} \\
\Pi_{\downarrow} & = A_1 \land \cdots \land A_i \land \cdots \land A_{n-1} \land A_i \\
\Pi & = A_1 \land \cdots \land A_i \land \cdots \land A_{n-1} \land A_i \\
\end{align*}
\]

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

We now have a direct proof of the following:

**Theorem 4.2.** sSKS $p$-simulates sFREGE.

**Proof.** Given an sFREGE-proof $A_1, A_2, \ldots, A_m$, where each $A_k$ is either an axiom, or obtained via the substitution rule from some $A_i$ with $1 \leq i < k$, or obtained via modus ponens from some $A_i$ and $A_j = A_i \equiv A_k$ with $1 \leq i, j < k$. We construct an sSKS-proof $\Pi$ of $A_n$ of the following shape:

\[
\begin{align*}
\Pi' & = A_1 \land \cdots \land A_2 \land \cdots \land A_n \\
\Pi_{\downarrow} & = A_1 \land \cdots \land A_2 \land \cdots \land A_n \\
\Pi & = A_1 \land \cdots \land A_2 \land \cdots \land A_n \\
\end{align*}
\]

where $\Pi$ 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 sFREGE-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 $O(m^2)$. Abandoning general rules, i.e., replacing $\rightarrow, \downarrow$, and $\rightarrow$ by their atomic versions $\rightarrow, \rightarrow$, and $\rightarrow$, respectively, increases the estimate for the size to $O(m^2)$. Removing all instances of $\rightarrow$ (i.e., replacing them by derivations consisting of $\rightarrow, \rightarrow, \rightarrow, \rightarrow$, and $\rightarrow$) does not increase that estimate. \hfill \Box

## 5 Extension and substitution in cut-free systems

The work in \([Str12]\) has shown how extension and substitution can be used in cut-free systems. Furthermore, a careful inspection of the proof of Theorem \([5.10]\) shows that it is also works in the cut-free case:

**Theorem 5.1.** eKS $p$-simulates sSKS. \([Str12]\)

However, the other direction remained open in \([Str12]\). 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 sSKS also p-simulates eKS. The actual difficulty is that if we naively replace an instance of $\text{ext}_\downarrow$ by an instance of $\text{sub}_\downarrow$:

\[
\text{ext}_\downarrow \frac{F\{a\}}{F\{A\}} \leadsto \text{sub}_\downarrow \frac{F\{a\}}{\sigma F\{a\}}
\]

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.

**Example 5.2.** Let $a_1 \equiv a_2 \lor a_3$, $a_2 \equiv a_3 \lor a_3$, $a_3 \equiv a_3$, $a_4 \equiv A$ 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.
$a_1 \leftrightarrow a_2 \lor a_2 \leftrightarrow a_3 \lor a_3 \ldots, a_n \leftrightarrow A$

\[\begin{array}{c}
\text{ext} \downarrow \quad S\{a_1 \lor a_1\} \\
\text{c} \downarrow \quad S\{a_1 \lor a_2 \lor a_2\}
\end{array}\]

\[\begin{array}{c}
\text{ext} \downarrow \quad S\{a_1 \lor a_2\} \\
\text{c} \downarrow \quad S\{a_1 \lor a_3 \lor a_3\}
\end{array}\]

\[\begin{array}{c}
\text{c} \downarrow \quad S\{a_1 \lor a_n \lor a_n\} \\
\text{ext} \downarrow \quad S\{a_1 \lor a\}
\end{array}\]

\[\begin{array}{c}
\text{c} \downarrow \quad S\{A \lor A\} \\
\text{c} \downarrow \quad S\{a_1 \lor a_1\}
\end{array}\]

\[\begin{array}{c}
\text{sub} \downarrow \quad S\{a_2 \lor a_2 \lor a_2\} \\
\text{c} \downarrow \quad S\{a_2 \lor a_2\}
\end{array}\]

\[\begin{array}{c}
\text{sub} \downarrow \quad S\{a_3 \lor a_3 \lor a_3 \lor a_3\} \\
\text{c} \downarrow \quad S\{a_3 \lor a_3 \lor a_3 \lor a_3\}
\end{array}\]

\[\begin{array}{c}
\text{c} \downarrow \quad S\{a_2 \lor a_2\} \\
\text{sub} \downarrow \quad S\{a_n \lor a_n \lor a_n \lor a_n\} \\
\text{c} \downarrow \quad S\{a_n \lor a_n \lor a_n \lor a_n\}
\end{array}\]

\[\begin{array}{c}
\text{c} \downarrow \quad S\{A \lor A \lor A\} \\
\text{c} \downarrow \quad S\{A \lor A\}
\end{array}\]

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

To overcome this problem, we basically transform the whole derivation so 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) causes only a limited increase of the size of the proof. This is achieved by a rather aggressive renaming of extension variable occurrences in the derivation.

For doing this, we need to extend the notion of extension. 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 $\preceq$ is a transitive and reflexive relation on $\mathcal{E}$. We write $a \sim b$ if $a \preceq b$ and $b \preceq a$. We call a substitution $\sigma$ 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 $B \sim C$ if there is a banal $\sigma$ such that $\sigma B = \sigma C$.

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

$$a_i \rightarrow A_i, \quad 1 \leq i \leq k; \quad (5.2)$$

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 $a_j \not\preceq a_i$.
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 $a \rightarrow B$ and $a \rightarrow C$, as long as $B$ and $C$ are in a same equivalence class under $\sim$.

In addition to adopting a more flexible view on extension axioms, we need to define a variant of the extension rule (3.5):

$$\begin{array}{c}
\text{ext} \downarrow \quad F\{b_1 \lor b_2 \lor \cdots \lor b_k \lor B_1 \lor B_2 \lor \cdots \lor B_m\} \\
\text{c} \downarrow \quad F\{A\}
\end{array}\quad (5.3)$$

where $m, k \geq 0$ and

- for all $i \in \{1, \ldots, k\}$ we have either $b_i \rightarrow A$ or $\bar{b}_i \rightarrow \bar{A}$ 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 $B_i \sim B_j$. 

9
• there is a banal substitution $\sigma$ such that for all $j \in \{1, \ldots, m\}$ we have $\sigma B_j = A$.

An occurrence of a formula $A$ in a derivation is said to be fresh in that derivation if no extension variables in $A$ occur above it. We call a formula diversified, if it contains no two different occurrences of a same extension variable.

An instance of $\text{ext}_{\downarrow}$ 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 $\text{ext}_{\downarrow}$ clever if $m = 0$, all $b_i$ in (5.3) are pairwise distinct, and $A$ is fresh and diversified. And we call an instance of $\text{ext}_{\downarrow}$ finished if $k = 0$ and $A$ is diversified.

We define $\tilde{\text{esKS}}$ to be the system obtained from $\text{skKS}$ by adding the $\text{ext}_{\downarrow}$-rule and allowing a generalized set of extension axioms. We call a derivation $\Pi$ in $\tilde{\text{esKS}}$

• naive if all instances of $\text{ext}_{\downarrow}$ in $\Pi$ are naive, the set of extension axioms is strict, and there is no instance of $\text{sub}_{\downarrow}$ in $\Pi$.

• $\text{e-contraction-free}$ if the contraction rule $\text{ac}_{\downarrow}$ is never applied to an extension variable in $\Pi$.

• clever if

1. every instance of $\text{ext}_{\downarrow}$ in $\Pi$ is clever,
2. there is no instance of $\text{sub}_{\downarrow}$ in $\Pi$, and
3. every extension variable occurs at most twice in each line of $\Pi$, 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 $\Pi$ to an instance of $\text{ai}_{\downarrow}$.

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

**Lemma 5.3.** Let $\Pi$ be a naive $\tilde{\text{esKS}}$ proof with conclusion $B$. Then there is a naive e-contraction-free $\tilde{\text{esKS}}$ proof $\Pi'$ with conclusion $B$ and size $O(|\Pi|^2)$. Furthermore, $\Pi'$ has the same extension axioms as $\Pi$.

**Proof.** To obtain $\Pi'$, we permutate all $\text{ac}_{\downarrow}$ on extension variables (or negated extension variables) down in the derivation (see also [Brü03]) as follows. Consider the rule instance $r$ immediately below such a contraction. There are two cases. If $r$ does not affect the literal to be duplicated in $\text{ac}_{\downarrow}$, we can trivially permutate the two:

\[
\begin{array}{c}
\text{ac}_{\downarrow} \quad F\{a \lor a\} \\
\text{r} \quad F\{a\} \\
\text{ac}_{\downarrow} \quad F\{a\} \\
\end{array}
\sim
\begin{array}{c}
\text{r} \quad F'\{a \lor a\} \\
\text{ac}_{\downarrow} \quad F'\{a\} \\
\end{array}
\]

Otherwise, if $r$ affects the duplicated literal, we must have that $r$ is $\text{ext}_{\downarrow}$ and we have the following situation:

\[
\begin{array}{c}
\text{ac}_{\downarrow} \quad F\{a \lor \cdots a \lor a \lor \cdots a\} \\
\text{ext}_{\downarrow} \quad F\{a \lor \cdots a \lor a \lor \cdots a\} \\
\end{array}
\sim
\begin{array}{c}
\text{ext}_{\downarrow} \quad F\{a \lor \cdots a \lor a \lor \cdots a\} \\
\end{array}
\]

Since the conclusion of the proof does not contain any extension variables, all $\text{ac}_{\downarrow}$ on extension variables must eventually disappear this way. Now notice that the size increasing step is permutating the contraction with non-$\text{ext}_{\downarrow}$ 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 $\Pi$, then we have $h, c \leq |\Pi|$, and the size of $\Pi'$ is dominated by $|\Pi| + c \cdot h$, which is $O(|\Pi|^2)$.

**Example 5.4.** Figure 3 shows an example of our construction. The first derivation in that figure is a proof in $\text{eKS}$ 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 $\tilde{\text{esSKS}}$ (which is $\text{skKS}$ extended with $\text{ext}_{\downarrow}$) because in the presence of cocontraction

\[
\begin{array}{c}
c\uparrow \quad F\{A\} \\
\text{ac}\uparrow \quad F\{a \land a\} \\
\end{array}
\]

permuting down $\text{ac}_{\downarrow}$ leads to an exponential blow-up of the size of the proof.
In the given proof Π we proceed from top to bottom and whenever an extension variable occurs—reductions (5.5) and (5.6) of Lemma 5.8, resulting in an e-contraction free, a clever ˜esKS derivation, an intermediate ˜esKS derivation, and a sks derivation, respectively. The upper row contains respective strict or generalized extension axioms.

The next lemma says that every naive e-contraction-free ˜esKS 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 generalized one.

Lemma 5.6. Let Π be a naive e-contraction-free ˜esKS proof with conclusion B. Then there is a clever e-contraction-free ˜esKS proof Π′ with conclusion B and |Π′| = |Π|. The number of extension axioms of Π′ is linear in |Π|.

Proof. In the given proof Π we proceed from top to bottom and whenever and extension variable occurrence a is introduced—this can happen in the conclusion of ai, or w, or ext— we replace it by a fresh variable a’. In order to keep the proof a valid ˜esKS 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 ext-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 ext-instance in whose premise a’ now occurs.

2. In order to make this ext-instance

\[
\text{ext} \quad \frac{H\{a_1 \lor a_2 \lor \cdots \lor a_i \lor a' \lor a \land a \land \cdots \land a\}}{H\{A\}}
\]

valid again, where a_1, a_2, \ldots, a_i are already renamed variables, we have to add an extension axiom. If a and a’ are positive atoms, we add the axiom a’ ⊨ A and the equivalence a' ∼ a. If a and a’ are negative atoms, then we add a’ ⊨ A and the equivalence a' ∼ a. This does not violate the conditions on generalized sets of extension variables. If there are no occurrences of a left in the proof, we can remove a ⊨ A or a ⊨ A from the set of extension axioms.

Now we have three cases.

- If we encounter an ai-rule with conclusion \( F\{B \land [a \lor a] \} \) where a is an extension variable, we replace it by an ai-rule with conclusion \( F\{B \land [a' \lor a'] \} \), where a’ is fresh. Then we perform Steps 1 and 2 above for the new occurrence of a’ and the new occurrence of a'.

- If we encounter a w-rule with premise F\{B\} and a conclusion F\{B \lor 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.

\[
\begin{array}{|c|c|}
\hline
a \sim b, & b \sim C \\
\hline
a \sim b, & b \sim C \\
\hline
\end{array}
\]
Example 5.7. To continue Example 5.4, the third derivation in Figure 3 shows the result of applying replace every instance of \( \bar{\cdot} \) in \( \Pi \). Since we have \( \bar{\cdot} \) in the conclusion replaced by some formula \( C' \), which is fresh and diversified. But this makes the instance (5.4) of \( \Pi \) invalid. In order to make it valid again, we have to add for every \( i \in \{1, \ldots, k\} \) the extension axiom \( b_i \Rightarrow C' \). Again, this preserves the two conditions for generalized sets of extension axioms.

Then, the resulting proof \( \Pi' \) 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 \( 2 \cdot n_{ai} + s_{\Pi} + s_{k\Pi} \), where \( n_{ai} \) is the total number of \( \bar{\cdot} \), \( s_{\Pi} \) is the total size of the axioms introduced in conclusions of \( \Pi \) and \( k \Pi \), and \( s_{k\Pi} \) are the total size of the formulas introduced in conclusions of \( \Pi \) and \( k \Pi \), 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 5.8.

Lemma 5.8. Let \( \Pi \) be a clever \( \bar{\cdot} \Pi \) proof with conclusion \( B \). Then there is an \( \bar{\cdot} \Pi \) proof \( \Pi' \) 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 \( \Pi \) in \( \Pi \) to obtain an intermediary \( \bar{\cdot} \Pi \) proof \( \Pi'' \), as follows:

\[
\begin{align*}
\text{ext} \downarrow & \frac{F\{b_1 \lor b_2 \lor \cdots \lor b_k \lor B_1 \lor \cdots \lor B_m\}}{F\{A\}} \quad \leadsto \quad \text{sub} \downarrow & \frac{F\{b_1 \lor b_2 \lor \cdots \lor b_k \lor B_1 \lor \cdots \lor B_m\}}{F\{A\} \lor \cdots \lor \lor \cdots} \\
\end{align*}
\]

where the used substitution is \( \{b_1 \leftrightarrow A, \ldots, b_k \leftrightarrow A\} \), and \( F''\{\} \) is obtained from \( F\{\} \) by applying this substitution. Since \( \Pi \) is clever, each \( b_i \) occurs at most once (in the form of \( b_i \)) in \( F\{\} \) and the path of this \( b_i \) ends in another \( \text{ext} \downarrow \), which has as conclusion a formula from which \( A \) 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 \( \Pi \) remains valid. Furthermore, in \( \Pi'' \), all instances of \( \text{ext} \downarrow \) must be finished.

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

In the second step of our transformation, we remove all finished \( \text{ext} \downarrow \)-instances in \( \Pi'' \) as follows, again proceeding from top to bottom:

\[
\begin{align*}
\text{ext} \downarrow & \frac{F\{B_1 \lor B_2 \lor \cdots \lor B_m\}}{F\{A\}} \quad \leadsto \quad \text{sub} \downarrow & \frac{F\{B_1 \lor B_2 \lor \cdots \lor B_m\}}{F'\{A \lor \cdots \lor \cdots \} \lor \cdots \lor \cdots} \\
\end{align*}
\]

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

\[
\begin{align*}
\text{ext} \downarrow & \frac{G\{C_1 \lor C_2 \lor \cdots \lor C_i\}}{G\{D\}} \quad \leadsto \quad \text{ext} \downarrow & \frac{G'\{C_1' \lor C_2' \lor \cdots \lor C_i'\}}{G'\{D\}} \\
\end{align*}
\]

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 \( \sigma \) 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 \( \sigma \) 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 \( \Pi \). This means there is a substitution that can rewrite all \( C_i' \) into \( D \).
Thus, the instance of $\text{ext} \downarrow$ 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 $\text{ext} \downarrow$ in $\Pi^*$, and the resulting proof $\Pi'$ 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 $\text{ext} \downarrow$ rules in $\Pi^*$, and $w$ for width of $\Pi^*$. With $e, w \leq |\Pi^*|$, one gets that the size of the derivation with $\text{ext} \downarrow$ removed is $O(|\Pi^*| + e \cdot w)$, that is, $O(|\Pi^*|^2)$.

Finally we can apply Proposition 5.2 to get a derivation in $\text{sKS}$. It is well known that this yields another quadratic increase in size of the derivation, [BT01], thus the overall size of $\Pi'$ is $O(|\Pi^*|^3)$, 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 $\text{sKS}$ proof from an $\text{eKS}$ one.

Theorem 5.10. $\text{sKS}$ $p$-simulates $\text{eKS}$.

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

References


