

Extension without cut

Lutz Straßburger^{a,b}

^a INRIA Saclay–Île-de-France, France

^b École Polytechnique, LIX, Rue de Saclay, 91128 Palaiseau Cedex, France

ARTICLE INFO

Article history:

Received 20 August 2009

Accepted 31 July 2012

Available online 14 August 2012

Communicated by J.M.E. Hyland

MSC:

03B05

03F05

03F07

03F20

Keywords:

Deep inference

Frege systems

Proof complexity

Cut elimination

Propositional pigeonhole principle

Balanced tautologies

ABSTRACT

In proof theory one distinguishes sequent proofs with cut and cut-free sequent proofs, while for proof complexity one distinguishes Frege systems and extended Frege systems. In this paper we show how deep inference can provide a uniform treatment for both classifications, such that we can define cut-free systems with extension, which is neither possible with Frege systems, nor with the sequent calculus. We show that the propositional pigeonhole principle admits polynomial-size proofs in a cut-free system with extension. We also define cut-free systems with substitution and show that the cut-free system with extension p -simulates the cut-free system with substitution.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

For studying proof complexity (for propositional classical logic) one essentially distinguishes between two kinds of proof systems: *Frege systems* and *extended Frege systems* [9]. Roughly speaking, a Frege system consists of a set of axioms and *modus ponens*, and in an extended Frege system one can also use “abbreviations”, i.e., fresh propositional variables abbreviating arbitrary formulas appearing in the proof. Clearly, any extended Frege proof can be converted into a Frege proof by systematically replacing the abbreviations by the formulas they abbreviate, at the cost of an exponential increase of the size of the proof. Surprisingly, this distinction is not investigated from the proof theoretic viewpoint.

On the other hand, in proof theory one also distinguishes between two kinds of proof systems: those *with cut* and those *without cut*. In a well-designed proof system, it is always possible to convert a proof with cuts into a cut-free proof, at the cost of an exponential increase of the size of the proof (see, e.g., [25]). The cuts are usually understood as “the use of auxiliary lemmas inside the proof”. The main tool for investigating the cut and its elimination from a proof is Gentzen’s sequent calculus [11].

The two proof classifications are usually not studied together. In fact, every Frege system contains cut because of the presence of *modus ponens*. Hence, there is no such thing as a “cut-free Frege system”, or a “cut-free extended Frege system”. Similarly, there are no “extended Gentzen systems”, because it does not make sense to speak of abbreviations in the sequent

E-mail address: lutz@lix.polytechnique.fr.

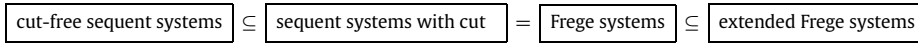


Fig. 1. Classification of proof systems.

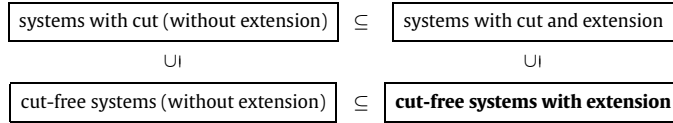


Fig. 2. Refined classification of proof systems.

calculus, where formulas are decomposed along their main connectives during proof search.¹ This can be summarized by the classification of proof systems shown in Fig. 1, where $S_1 \subseteq S_2$ means that S_2 includes S_1 (and therefore S_2 p-simulates S_1).

There are classes of tautologies that admit no polynomial-size proofs in cut-free sequent calculus [21] (and related systems, like resolution [14] and tableaux). But no such class is known for systems with cut or for extended Frege systems. The question whether there is a short, i.e., polynomial-size, proof of every tautology A is equivalent to the question whether **NP** is equal to **coNP**.

The contributions of this paper can be summarized as follows:

- (i) I provide a deductive system in which extension is independent from the cut, i.e., we can now study cut-free systems with extension.² Fig. 2 shows the refined classification of proof systems. I use as formalism the *calculus of structures* [12,13,4]. Thus, this paper is a continuation of the work by Bruscoli and Guglielmi [5], who observed that by using *deep inference* one can bring the extension rule to a deductive formalism which has originally been designed to study cut-elimination.
- (ii) I also present a cut-free system with substitution and investigate the relation between substitution and extension in a cut-free setting.
- (iii) In order to provide evidence that it indeed makes sense to study extension (or substitution) independently from cut, I will show polynomial-size proofs for the propositional pigeonhole principle (PHP) without cut. At the same time, I propose a new class of tautologies (called QHQ), that have similar properties as the PHP w.r.t. proof complexity, but have the additional property of being *balanced*, i.e., every atom occurs exactly once positive and exactly once negative.

Sections 2–4 of this paper contain preliminaries on proof systems in general and the calculus of structures in particular. Then, Sections 5–7 are dedicated to points (i)–(iii) above.

2. Preliminaries on proof systems

Following [9], we define a *proof system* to be a surjective **PTIME**-function $S: \Sigma^* \rightarrow \mathcal{T}$ where Σ is some finite alphabet (and Σ^* the set of all finite words over Σ) and \mathcal{T} is the set of all Boolean tautologies. An element $\pi \in \Sigma^*$ is called a *proof* and $S(\pi)$ its *conclusion*. We denote by $|\pi|$ the size of π , i.e., the number of symbols in π . Given two proof systems $S_1: \Sigma_1^* \rightarrow \mathcal{T}$ and $S_2: \Sigma_2^* \rightarrow \mathcal{T}$, we say that S_2 *p-simulates* S_1 iff there is a polynomial p such that for every proof $\pi_1 \in \Sigma_1^*$ there is a proof $\pi_2 \in \Sigma_2^*$ of the same conclusion (i.e., $S_2(\pi_2) = S_1(\pi_1)$) such that $|\pi_2| \leq |p(\pi_1)|$. We say that S_1 and S_2 are *p-equivalent* iff they p-simulate each other. A proof system $S: \Sigma^* \rightarrow \mathcal{T}$ is *polynomially bounded* iff there is a polynomial p such that for every tautology $T \in \mathcal{T}$ there is a proof $\pi \in \Sigma^*$ with $S(\pi) = T$ and $|\pi| \leq p(|T|)$. If $|\pi| \leq p(|T|)$ for some $\pi \in \Sigma^*$ with $S(\pi) = T$, we also say that π is a *short proof* of T . Thus, a polynomially bounded proof system is one in which every tautology has a short proof w.r.t. some fixed bounding polynomial p . The question whether there is a polynomially bounded proof system is equivalent to the question whether the complexity class **NP** is closed under complement:

Theorem 2.1. *There exists a polynomially bounded proof system if and only if **NP** = **coNP** [9].*

For the sake of simplicity, let us consider for the rest of the paper only formulas in negation normal form. More precisely, formulas are generated from a countable set $\mathcal{A} = \{a, b, c, \dots\}$ of propositional variables and their negations $\bar{\mathcal{A}} = \{\bar{a}, \bar{b}, \bar{c}, \dots\}$ via the binary connectives \wedge and \vee , called *and* and *or*, respectively.³ I denote formulas by capital Latin letters (A, B, C, \dots).

¹ The extension discussed in this paper should not be confused with the notion of “definition” in the sequent calculus LKDe [1], in which the abbreviation may occur in the endsequent of the proof.

² Technically speaking, Haken’s extended resolution [14] is a cut-free system with extension, but his system is not suited to study cut elimination. And it is not clear how to incorporate Haken’s extension into the recent work on resolution and cut elimination [2,8].

³ For simplicity, I do not introduce special symbols for the units *truth* and *false*. Note that these units can be recovered by the formulas $p_0 \vee \bar{p}_0$ and $p_0 \wedge \bar{p}_0$, respectively, where p_0 is a fresh propositional variable.

Negation is defined for all formulas via the de Morgan laws: $\bar{\bar{a}} = a$ and $\overline{A \wedge B} = \bar{B} \vee \bar{A}$ and $\overline{A \vee B} = \bar{B} \wedge \bar{A}$. It follows immediately that $\bar{\bar{A}} = A$ for all formulas A . The elements of the set $\mathcal{A} \cup \bar{\mathcal{A}}$ are also called *literals*. We can write $A \Rightarrow B$ for $\bar{A} \vee B$ and $A \Leftrightarrow B$ for $[\bar{A} \vee B] \wedge [\bar{B} \vee A]$.

3. Preliminaries on the calculus of structures

I assume the reader to be familiar with sequent calculus or natural deduction systems [11], in which inference rules decompose formulas along their main connectives. On the other hand, in the *calculus of structures* [12,13,4], inference rules are allowed to do arbitrary rewriting deep inside formulas. In this paper, I use the following rule schemes (to be applied on formulas in negation normal form):

$$\begin{array}{c} \text{ai} \downarrow \frac{F\{B\}}{F\{B \wedge [\bar{a} \vee a]\}} \quad \text{s} \frac{F\{A \wedge [B \wedge C]\}}{F\{(A \wedge B) \vee C\}} \\ \\ \text{w} \downarrow \frac{F\{B\}}{F\{B \vee A\}} \quad \text{ac} \downarrow \frac{F\{a \vee a\}}{F\{a\}} \quad \text{m} \frac{F\{(A \wedge B) \vee (C \wedge D)\}}{F\{[A \vee C] \wedge [B \vee D]\}} \end{array} \quad (1)$$

where A, B, C , and D must be seen as formula variables, and a is a propositional variable or its negation. These rules are called (*atomic*) *identity*, *switch*, *weakening*, (*atomic*) *contraction*, and *medial*, respectively. The rules in (1) are written in the style of inference rule schemes in proof theory but they behave as rewrite rules in term rewriting, i.e., they can be applied *deep* inside any (positive) formula context $F\{ \}$. To ease readability of large formulas, I will use $[]$ for brackets around disjunctions and $()$ for brackets around conjunctions. The rewriting rules in (1) are applied modulo associativity and commutativity for \wedge and \vee . More precisely, we will do rewriting modulo the equational theory generated by

$$\begin{array}{ll} A \wedge (B \wedge C) = (A \wedge B) \wedge C & A \wedge B = B \wedge A \\ A \vee [B \vee C] = [A \vee B] \vee C & A \vee B = B \vee A \end{array} \quad (2)$$

Because of this, we can systematically omit superfluous parentheses in order to ease readability; e.g., instead of $A \wedge ((B \wedge C) \wedge D)$ we write $A \wedge B \wedge C \wedge D$. A *derivation* is a rewrite path via (1) modulo (2). Here is an example:

$$\begin{array}{l} 2*\text{ac} \downarrow \frac{([\bar{b} \vee \bar{b}] \wedge [\bar{b} \vee \bar{b}]) \vee (b \wedge [a \vee a])}{([\bar{b} \vee \bar{b}] \wedge \bar{b}) \vee (b \wedge a)} \\ \text{ai} \downarrow \frac{([\bar{b} \vee \bar{b}] \wedge (\bar{b} \wedge [\bar{a} \vee a])) \vee (b \wedge a)}{([\bar{b} \vee \bar{b}] \wedge (\bar{b} \wedge \bar{a}) \vee a) \vee (b \wedge a)} \\ \text{s} \frac{([\bar{b} \vee \bar{b}] \wedge (\bar{b} \wedge \bar{a}) \vee a) \vee (b \wedge a)}{([\bar{b} \vee \bar{b}] \wedge [a \vee (\bar{a} \wedge \bar{b})]) \vee (b \wedge a)} \\ = \frac{([\bar{b} \vee \bar{b}] \wedge [a \vee (\bar{a} \wedge \bar{b})]) \vee (b \wedge a)}{(\bar{b} \wedge [a \vee (\bar{a} \wedge \bar{b})]) \vee (b \wedge a)} \\ \text{ac} \downarrow \frac{(\bar{b} \wedge [a \vee (\bar{a} \wedge \bar{b})]) \vee (b \wedge a)}{[(\bar{b} \wedge a) \vee (\bar{a} \wedge \bar{b})] \vee (b \wedge a)} \\ \text{s} \frac{[(\bar{b} \wedge a) \vee (\bar{a} \wedge \bar{b})] \vee (b \wedge a)}{[(\bar{b} \wedge a) \vee (\bar{a} \wedge \bar{b})] \vee (b \wedge a)} \end{array} \quad (3)$$

The notation $n*r$ is used to indicate that there are n applications of the rule r . In the hope of helping the reader, I sometimes use a “fake inference rule”

$$= \frac{A}{B} \quad (4)$$

governed by the side condition that $A = B$ under the equivalence relation generated by (2).

Remark 3.1. Instead of doing rewriting modulo, one could equivalently add four inference rules

$$\begin{array}{llll} =_1 \frac{F\{(A \vee B) \vee C\}}{F\{A \vee (B \vee C)\}} & =_2 \frac{F\{(A \wedge B) \wedge C\}}{F\{A \wedge (B \wedge C)\}} & =_3 \frac{F\{A \vee B\}}{F\{B \vee A\}} & =_4 \frac{F\{A \wedge B\}}{F\{B \wedge A\}} \end{array} \quad (5)$$

Computationally there is no difference between the two approaches since the equivalence modulo $=$ can be checked in time $O(n \log n)$.

In order to obtain proofs without hypotheses, we need an axiom, which is in our case just a variant of the rule $\text{ai} \downarrow$:

$$\text{ai} \downarrow \frac{}{\bar{a} \vee a} \quad (6)$$

The rule in (6) cannot be applied inside a context $F\{ \}$, but it is in spirit the same rule as $\text{ai}\downarrow$ in (1), and I use therefore the same name. Given a system S , we write

$$\text{S}\|_{\pi_1}^A \quad \text{and} \quad \text{S}\|_{\pi_2}^B$$

to denote a derivation π_1 in the system S from premise A to conclusion B , and a proof π_2 in the system S without premise and with conclusion B , respectively. I write KS to denote the system shown in (1), together with the rule in (6). A proof in KS uses the axiom (6) exactly once.

Remark 3.2. The original formulation of KS in [4] uses explicit units \mathbf{t} and \mathbf{f} for *truth* and *false*, respectively, and thus contains more rules and equations to deal with them. If we denote by KS^+ the system with units, and by KS^- the system without units, then we have that KS^+ and KS^- are p-equivalent under the translation mentioned in Footnote 3. This can easily be shown by using the equations $B \wedge \mathbf{t} = B = B \vee \mathbf{f}$ and $B \wedge \mathbf{f} = \mathbf{f}$ and $B \vee \mathbf{t} = \mathbf{t}$ (see also [10]). Since many Frege systems are given without explicit units, and Gentzen's original LK comes without units, it might be helpful to see a presentation of KS that does not rely on the presence of units. Anyhow, everything that is said in this paper does also hold for the variant of KS with units.

The following two propositions have first been proved in [4]:

Proposition 3.3. *The rules*

$$\text{i}\downarrow \frac{}{A \vee A} \quad \text{i}\downarrow \frac{F\{B\}}{F\{B \wedge [\bar{A} \vee A]\}} \quad \text{c}\downarrow \frac{F\{A \vee A\}}{F\{A\}} \quad \text{d}\downarrow \frac{F\{[A \vee C] \wedge [B \vee C]\}}{F\{(A \wedge B) \vee C\}}$$

are derivable in KS . More precisely, KS p-simulates $\text{KS} \cup \{\text{i}\downarrow, \text{c}\downarrow, \text{d}\downarrow\}$.

The rules $\text{i}\downarrow$ and $\text{c}\downarrow$ are the general (non-atomic) versions of $\text{ai}\downarrow$ and $\text{ac}\downarrow$, respectively.

Proposition 3.4. *The system KS p-simulates cut-free sequent calculus.*

The converse is not true, i.e., cut-free sequent calculus cannot p-simulate KS . A counterexample can be found in [5], where Bruscoli and Guglielmi show that the example used by Statman [21] to prove an exponential lower bound for cut-free sequent calculus admits polynomial-size proofs in KS . This situation changes when we add the cut rule, which is dual to the identity rule

$$\text{ai}\uparrow \frac{F\{(a \wedge \bar{a}) \vee B\}}{F\{B\}} \quad (7)$$

The system $\text{KS} \cup \{\text{ai}\uparrow\}$ will in the following be denoted by SKS . The following two propositions are also due to [4]:

Proposition 3.5. *The rules*

$$\text{i}\uparrow \frac{F\{(A \wedge \bar{A}) \vee B\}}{F\{B\}} \quad \text{c}\uparrow \frac{F\{A\}}{F\{A \wedge A\}} \quad \text{w}\uparrow \frac{F\{A \wedge B\}}{F\{B\}} \quad (8)$$

are derivable in SKS . More precisely, SKS p-simulates $\text{SKS} \cup \{\text{i}\uparrow, \text{c}\uparrow, \text{w}\uparrow\}$.

Proposition 3.6. *SKS is p-equivalent to every sequent system with cut.*

Finally, let us mention the following theorem, stating soundness, completeness, cut elimination, and the deduction theorem for KS .

Theorem 3.7. *For any formulas A and B , we have:*

$$\text{The formula } A \Rightarrow B \text{ is a valid implication.} \quad \text{iff} \quad \text{KS}\|_{\bar{A} \vee B}^A \quad \text{iff} \quad \text{SKS}\|_B^A$$

This does not only hold for classical logic, but also for linear logic and modal logic (for a proof see [3,23]).

4. Relation between calculus of structures and Frege systems

Frege systems (also known as *Hilbert systems* or *Hilbert–Frege systems* or *Hilbert–Ackermann systems* [15,16]), consist of a set of axioms (more precisely, axiom schemes) and a set of inference rules, which in the case of classical propositional logic only contains *modus ponens*:

$$\text{modus ponens} \frac{A \quad A \Rightarrow B}{B}$$

I assume the reader to be familiar with Frege systems, and I will not go into further details. The important facts are that the set of axioms in a Frege system has to be sound and complete, and that all Frege systems *p*-simulate each other [9]. We also immediately have the following theorem:

Theorem 4.1. *SKS is *p*-equivalent to every Frege system.*

This follows immediately from Proposition 3.6 and a result by [9]. In [5] one can find a direct proof. Because it will be needed later, I sketch here the basic idea. For *p*-simulating a Frege system *F* with SKS, we first exhibit an SKS proof for every axiom in *F*. Then we proceed by induction on the length of the proof π in *F* and keep all formulas appearing in π in a conjunction $F_1 \wedge F_2 \wedge \dots \wedge F_n$. Now we can simulate *modus ponens*:

$$\text{modus ponens} \frac{A \quad \bar{A} \vee B}{B} \quad \rightsquigarrow \quad \begin{array}{c} \text{s} \frac{A \wedge [\bar{A} \vee B]}{(A \wedge \bar{A}) \vee B} \\ \text{i}\uparrow \\ B \end{array}$$

Note that we might need to duplicate a formula F_i by using *c*↑. Finally we remove the superfluous copies by using *w*↑. Conversely, we show that a Frege system can *p*-simulate SKS by exhibiting for every rule

$$\text{r} \frac{A}{B}$$

a Frege proof of $\bar{A} \vee B$. Then we show by induction that for every context $F\{ \}$ also $\overline{F\{A\}} \vee F\{B\}$ has a Frege proof. Then the application of an inference rule in SKS can be simulated by *modus ponens*.

5. Extension

Let us now turn to the actual interest of this paper, the extension rule (first formulated by Tseitin [26]), which allows us to use abbreviations in the proof. I.e., there is a finite set of fresh and mutually distinct propositional variables a_1, \dots, a_n which can abbreviate formulas A_1, \dots, A_n , that obey the side condition that for all $1 \leq i \leq n$, the variable a_i does not appear in A_1, \dots, A_i . Extension can easily be integrated in a Frege system by simply adding the formulas $a_i \Leftrightarrow A_i$, for $1 \leq i \leq n$, to the set of axioms. In that case we speak of an *extended Frege system* [9]. In the sequent calculus one could add these formulas as non-logical axioms, with the consequence that cut-elimination would not hold anymore. This very idea is used by Bruscoli and Guglielmi in [5] for adding extension to a system in the calculus of structures: instead of starting a proof from no premises, they use the conjunction

$$[\bar{a}_1 \vee A_1] \wedge [\bar{A}_1 \vee a_1] \wedge \dots \wedge [\bar{a}_n \vee A_n] \wedge [\bar{A}_n \vee a_n] \quad (9)$$

of all extension formulas as premise. Let us write *xSKS* to denote the system SKS with the extension incorporated this way, i.e., a proof of a formula *B* in *xSKS* is a derivation

$$\frac{[\bar{a}_1 \vee A_1] \wedge [\bar{A}_1 \vee a_1] \wedge \dots \wedge [\bar{a}_n \vee A_n] \wedge [\bar{A}_n \vee a_n]}{\text{SKS} \parallel \pi} B \quad (10)$$

where

$$\begin{array}{l} \text{the propositional variables } a_1, \dots, a_n \text{ are mutually distinct, and for all } 1 \leq i \leq n, \\ \text{the variable } a_i \text{ does not appear in } A_1, \dots, A_i \text{ nor in } B. \end{array} \quad (11)$$

Theorem 5.1. *xSKS is *p*-equivalent to every extended Frege system.*

The proof can be found in [5], and is almost literally the same as for Theorem 4.1.

It should be clear that *xSKS* crucially relies on the presence of cut, in the same way as extended Frege system rely on the presence of *modus ponens*: The premise of (10) contains the variables a_1, \dots, a_n , which do not appear in the conclusion *B*.

Thus, the derivation in (10) must contain cuts. This raises the question whether the virtues of extension can also be used in a cut-free system.⁴ For this, let us for every extension axiom $a_i \Leftrightarrow \bar{a}_i$ add the following two rules (we use the same name for both of them):

$$\text{ext}\downarrow \frac{F\{a_i\}}{F\{\bar{a}_i\}} \quad \text{and} \quad \text{ext}\downarrow \frac{F\{\bar{a}_i\}}{F\{a_i\}} \quad (12)$$

We write eKS to denote the system $\text{KS} \cup \{\text{ext}\downarrow\}$ and we write eSKS for $\text{SKS} \cup \{\text{ext}\downarrow\}$. Note that the rule $\text{ext}\downarrow$ is not sound. Consider for example the extension axiom $a \Leftrightarrow b \wedge c$ where a abbreviates $b \wedge c$. Applying it to $a \vee \bar{a}$ (which is a tautology) yields $(b \wedge c) \vee \bar{a}$ (which is *not* a tautology). Nonetheless, we allow to apply (12) in an arbitrary context $F\{ \}$, provided that condition (11) is satisfied. Then we have the following:

Theorem 5.2. *The systems eKS and eSKS are sound and complete for classical propositional logic.*

Proof. Completeness of both systems follows from completeness of KS, and soundness of eSKS follows from Theorem 5.3 below and Theorem 5.1 above. This entails soundness of eKS. \square

Theorem 5.3. *The systems eSKS and xSKS are p-equivalent.*

Proof. Given a proof π of a formula B in xSKS, we can construct

$$\begin{array}{c} \{\text{ai}\downarrow\} \parallel \pi_2 \\ [\bar{a}_1 \vee a_1] \wedge [\bar{a}_1 \vee a_1] \wedge \dots \wedge [\bar{a}_n \vee a_n] \wedge [\bar{a}_n \vee a_n] \\ \{\text{ext}\downarrow\} \parallel \pi_1 \\ [\bar{a}_1 \vee A_1] \wedge [\bar{A}_1 \vee a_1] \wedge \dots \wedge [\bar{a}_n \vee A_n] \wedge [\bar{A}_n \vee a_n] \\ \text{SKS} \parallel \pi \\ B \end{array} \quad (13)$$

where π_1 consists of $2n$ instances of $\text{ext}\downarrow$ and π_2 of $2n$ instances of $\text{ai}\downarrow$. Hence, eSKS p-simulates xSKS. For the converse, assume we have an eSKS proof π of a formula B . We can put every line of π in conjunction with the formula (9), and add a coweakening $w\uparrow$ (see Proposition 3.5) at the bottom:

$$\begin{array}{c} [\bar{a}_1 \vee A_1] \wedge [\bar{A}_1 \vee a_1] \wedge \dots \wedge [\bar{a}_n \vee A_n] \wedge [\bar{A}_n \vee a_n] \\ \text{eSKS} \parallel \pi \\ B \end{array} \quad \rightsquigarrow \quad \begin{array}{c} \text{eSKS} \parallel \pi' \\ [\bar{a}_1 \vee A_1] \wedge [\bar{A}_1 \vee a_1] \wedge \dots \wedge [\bar{a}_n \vee A_n] \wedge [\bar{A}_n \vee a_n] \wedge B \\ w\uparrow \\ B \end{array}$$

The instances of $\text{ext}\downarrow$ in π' can now be removed as follows:

$$\begin{array}{c} \text{ext}\downarrow \frac{\dots \wedge [\bar{a}_i \vee A_i] \wedge \dots \wedge F\{a_i\}}{\dots \wedge [\bar{a}_i \vee A_i] \wedge \dots \wedge F\{\bar{a}_i\}} \quad \rightsquigarrow \quad \begin{array}{c} c\uparrow \frac{\dots \wedge [\bar{a}_i \vee A_i] \wedge \dots \wedge F\{a_i\}}{\dots \wedge [\bar{a}_i \vee A_i] \wedge [\bar{a}_i \vee A_i] \wedge \dots \wedge F\{a_i\}} \\ \{\text{s}\} \parallel \pi_s \\ \dots \wedge [\bar{a}_i \vee A_i] \wedge \dots \wedge F\{a_i \wedge [\bar{a}_i \vee A_i]\} \\ s \\ \dots \wedge [\bar{a}_i \vee A_i] \wedge \dots \wedge F\{(a_i \wedge \bar{a}_i) \vee A_i\} \\ \text{ai}\uparrow \\ \dots \wedge [\bar{a}_i \vee A_i] \wedge \dots \wedge F\{A_i\} \end{array} \end{array} \quad (14)$$

where $F\{ \}$ is an arbitrary (positive) context, and the existence of π_s (which contains only instances of the rule s) can be shown by an easy induction on $F\{ \}$ (see e.g., Lemma 4.3.20 in [23]). The length of π_s is bound by the depth of $F\{ \}$. Note the crucial use of the cut rule in (14). \square

System eKS gives us a way of adding extension to a deductive system independently from cut. To show that extension without cut is potentially useful for giving short proofs for some of the standard benchmark tautologies, we give in Section 7 polynomial-size proofs of the propositional pigeonhole principle in eKS.

Remark 5.4. When we say “independent from cut”, we have to clarify what “cut” means. The way we added extension to KS to get eKS is clearly independent from the chosen language. E.g., it does not matter whether we chose a presentation

⁴ One could allow to add a disjunction of formulas $a_i \wedge \bar{a}_i$ to the conclusion, in the same way as we add a conjunction of $[\bar{a}_i \vee A_i] \wedge [\bar{A}_i \vee a_i]$ to the premise [5]. Some readers might consider this to be cut-free, but the question remains whether we can obtain cut-freeness without changing the notions of derivation and proof.

with or without units: if we define eKS^- and eKS^+ by adding $\text{ext}\downarrow$ to KS^- and KS^+ , respectively (see Remark 3.2), then one can easily show that eKS^- and eKS^+ p -simulate each other (if the units appear inside the extension formulas A_i then they can be removed using $B \wedge \mathbf{t} = B = B \vee \mathbf{f}$ and $B \wedge \mathbf{f} = \mathbf{f}$ and $B \vee \mathbf{t} = \mathbf{t}$, and if $A_i = \mathbf{t}$ or $A_i = \mathbf{f}$ then this extension axiom can be eliminated without increasing the size of the proof). However, the power of the rule $\text{ext}\downarrow$ depends on the other rules that are present. For example, in order to make Theorem 5.3 work, the rules $\text{ai}\downarrow$ and s should be derivable in the chosen system. Furthermore, for the polynomial-size proofs of the propositional pigeonhole principle in Section 7 we will need associativity and commutativity of conjunction. More precisely, for completeness of KS only the rules $=_1$ and $=_3$ in (5) would be necessary [24], but for Section 7 we also need rules $=_2$ and $=_4$ (see Remark 3.1).

6. Substitution

Let us next consider systems with substitution. A *substitution* is a function σ from the set \mathcal{A} of propositional variables to the set \mathcal{F} of formulas, such that $\sigma(a) = a$ for almost all $a \in \mathcal{A}$. We can define $\sigma(A)$ inductively for all formulas via $\sigma(A \wedge B) = \sigma(A) \wedge \sigma(B)$ and $\sigma(A \vee B) = \sigma(A) \vee \sigma(B)$ and $\sigma(\bar{A}) = \overline{\sigma(A)}$. Following the tradition, we write $A\sigma$ for $\sigma(A)$. For example, if $A = a \vee b \vee b$ and $\sigma = \{a \mapsto a \wedge b, b \mapsto a \vee \bar{c}\}$ then $A\sigma = (a \wedge b) \vee (\bar{a} \wedge c) \vee a \vee \bar{c}$. We can define the inference rule for substitution

$$\text{sub}\downarrow \frac{A}{A\sigma} \quad (15)$$

Note that the rule $\text{sub}\downarrow$ cannot be applied inside a context $F\{ \}$. Thus, it is exactly the same rule as in Frege systems and in strong contrast to all other rules in deep inference. Let us define $\text{sSKS} = \text{SKS} \cup \{\text{sub}\downarrow\}$ and $\text{sKS} = \text{KS} \cup \{\text{sub}\downarrow\}$. The following has been proved in [5]:

Theorem 6.1. *sSKS is p -equivalent to any Frege system with substitution.*

However, contrary to the previous cases, there is no immediate easy proof of Theorem 6.1, because the substitution rule is stronger in Frege systems than in SKS . The reason is that in Frege systems one can, after a substitution σ has been applied to a formula A , reuse the original A as well as the substituted version $A\sigma$.

Thus, to prove Theorem 6.1, Bruscoli and Guglielmi use in [5] the result by Krajíček and Pudlák [19] on the p -equivalence of Frege system with extension and Frege system with substitution.

We give here a direct proof of the p -equivalence of sSKS and xSKS (and eSKS).

Theorem 6.2. *sSKS p -simulates xSKS.*

Proof. This proof can already be found in [5]. For a given xSKS proof π of a formula B , we construct

$$\begin{aligned} & i\downarrow \frac{}{(\bar{a}_n \wedge A_n) \vee (\bar{A}_n \wedge a_n) \vee \dots \vee (\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1) \vee ([\bar{a}_1 \vee A_1] \wedge [\bar{A}_1 \vee a_1] \wedge \dots \wedge [\bar{a}_n \vee A_n] \wedge [\bar{A}_n \vee a_n])} \\ & \quad \text{SKS} \parallel \pi' \\ & = \frac{(\bar{a}_n \wedge A_n) \vee (\bar{A}_n \wedge a_n) \vee \dots \vee (\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1) \vee B}{(\bar{a}_n \wedge A_n) \vee (\bar{A}_n \wedge a_n) \vee (\bar{a}_{n-1} \wedge A_{n-1}) \vee (\bar{A}_{n-1} \wedge a_{n-1}) \vee \dots \vee (\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1) \vee B} \\ & \quad \text{sub}\downarrow \\ & \quad 2*i\uparrow \frac{(\bar{a}_n \wedge A_n) \vee (\bar{A}_n \wedge a_n) \vee (\bar{a}_{n-1} \wedge A_{n-1}) \vee (\bar{A}_{n-1} \wedge a_{n-1}) \vee \dots \vee (\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1) \vee B}{(\bar{a}_{n-1} \wedge A_{n-1}) \vee (\bar{A}_{n-1} \wedge a_{n-1}) \vee \dots \vee (\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1) \vee B} \\ & \quad \text{sub}\downarrow \\ & \quad \quad \vdots \\ & \quad \quad 2*i\uparrow \frac{}{(\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1) \vee B} \\ & \quad \quad \text{sub}\downarrow \\ & \quad \quad 2*i\uparrow \frac{(\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1) \vee B}{B} \end{aligned} \quad (16)$$

where π' is obtained from π by putting every formula in disjunction with

$$(\bar{a}_n \wedge A_n) \vee (\bar{A}_n \wedge a_n) \vee \dots \vee (\bar{a}_1 \wedge A_1) \vee (\bar{A}_1 \wedge a_1)$$

The derivation (16) is a valid derivation in sSKS because of condition (11). Note that we proceed backwards in eliminating the a_i in order to keep the size of the proof polynomial. \square

For the other direction, the basic idea is to simulate the substitution inference step from A to $A\sigma$ by many extension inference steps, one for each occurrence of a variable a with $\sigma(a) \neq a$ in A . Consider for example:

$$\begin{array}{ccccccc}
\text{SKS} \Vdash \pi_{k+1,1} & & \text{SKS} \Vdash \pi_{k+1,2} & & \text{SKS} \Vdash \pi_{k+1,3} & & \text{SKS} \Vdash \pi_{k+1,k+1} \\
\text{sub} \downarrow \frac{B_{k,1}}{B_{k,1} \sigma_{k,1}} & & \text{sub} \downarrow \frac{B_{k,2}}{B_{k,2} \sigma_{k,2}} & & \text{sub} \downarrow \frac{B_{k,3}}{B_{k,3} \sigma_{k,3}} & & \text{sub} \downarrow \frac{B_{k,k+1}}{B_{k,k+1} \sigma_{k,k+1}} \\
\text{SKS} \Vdash \pi_{k,1} & & \text{SKS} \Vdash \pi_{k,2} & & \text{SKS} \Vdash \pi_{k,3} & & \text{SKS} \Vdash \pi_{k,k} \\
\vdots & & \vdots & & \vdots & & \vdots \\
\text{SKS} \Vdash \pi_{3,1} & & \text{SKS} \Vdash \pi_{3,2} & & \text{SKS} \Vdash \pi_{3,3} & & \text{SKS} \Vdash \pi_{3,k} \\
\text{sub} \downarrow \frac{B_{2,1}}{B_{2,1} \sigma_{2,1}} & \rightsquigarrow & \text{sub} \downarrow \frac{B_{2,2}}{B_{2,2} \sigma_{2,2}} & \rightsquigarrow & \text{sub} \downarrow \frac{B_{2,3}}{B_{2,3} \sigma_{2,3}} & \rightsquigarrow \dots \rightsquigarrow & \text{sub} \downarrow \frac{B_{2,3}}{B_{2,3} \sigma_{2,3}} \\
\text{SKS} \Vdash \pi_{2,1} & & \text{SKS} \Vdash \pi_{2,2} & & \text{SKS} \Vdash \pi_{2,2} & & \text{SKS} \Vdash \pi_{2,2} \\
\text{sub} \downarrow \frac{B_{1,1}}{B_{1,1} \sigma_{1,1}} & & \text{sub} \downarrow \frac{B_{1,2}}{B_{1,2} \sigma_{1,2}} & & \text{sub} \downarrow \frac{B_{1,2}}{B_{1,2} \sigma_{1,2}} & & \text{sub} \downarrow \frac{B_{1,2}}{B_{1,2} \sigma_{1,2}} \\
\text{SKS} \Vdash \pi_{1,1} & & \text{SKS} \Vdash \pi_{1,1} & & \text{SKS} \Vdash \pi_{1,1} & & \text{SKS} \Vdash \pi_{1,1} \\
B & & B & & B & & B
\end{array}$$

Fig. 3. Renaming propositional variables in an sSKS proof.

$$\begin{array}{ccc}
\text{sub} \downarrow \frac{\text{SKS} \Vdash \pi_2}{F\{a \vee (b \wedge c) \vee \bar{a}\}} & \rightsquigarrow & \text{ext} \downarrow \frac{\text{SKS} \Vdash \pi_2}{F\{a \vee (b \wedge c) \vee \bar{a}\}} \\
\text{SKS} \Vdash \pi_1 & & \text{ext} \downarrow \frac{F\{(a \wedge c) \vee (b \wedge c) \vee \bar{a}\}}{F\{(a \wedge c) \vee (b \wedge [a \vee c]) \vee \bar{a}\}} \\
B & & B
\end{array} \quad (17)$$

where the used substitution is $\{a \mapsto a \wedge c, c \mapsto a \vee c\}$ and the context $F\{\}$ does not contain any occurrences of a or c . The problem with this is that the result will, in general, not be a valid proof because both conditions in (11) might be violated. For this reason we first have to rename the variables a and c in π_2 :

$$\begin{array}{ccc}
\text{sub} \downarrow \frac{\text{SKS} \Vdash \pi'_2}{F\{a' \vee (b \wedge c') \vee \bar{a}'\}} & \rightsquigarrow & \text{ext} \downarrow \frac{\text{SKS} \Vdash \pi'_2}{F\{a' \vee (b \wedge c') \vee \bar{a}'\}} \\
\text{SKS} \Vdash \pi_1 & & \text{ext} \downarrow \frac{F\{(a \wedge c) \vee (b \wedge c') \vee \bar{a}'\}}{F\{(a \wedge c) \vee (b \wedge [a \vee c]) \vee \bar{a}'\}} \\
B & & B
\end{array} \quad (18)$$

Here a and c have been replaced everywhere in π_2 by fresh variables a' and c' , respectively. The new substitution is $\{a' \mapsto a \wedge c, c' \mapsto a \vee c\}$, which can be replaced by instances of extension, without violating (11).

Theorem 6.3. eSKS p -simulates sSKS.

Proof. Let π be an sSKS proof of a formula B . Suppose π contains k instances of $\text{sub} \downarrow$, and let $\sigma_{1,1}, \dots, \sigma_{k,1}$ be the k substitutions used in them. Then π is of the shape as shown in the left-most derivation in Fig. 3. In the following, we use $\mathcal{A}_{i,j}$ to denote the set of variables a with $\sigma_{i,j}(a) \neq a$. As explained above, we can now iteratively rename the propositional variables in $\mathcal{A}_{1,1}, \dots, \mathcal{A}_{k,1}$, starting from the bottommost instance of $\text{sub} \downarrow$, as indicated in Fig. 3. The result of this renaming is shown in the rightmost derivation in Fig. 3 and has the property that

for all i with $1 \leq i \leq k$, we have that no variable in $\mathcal{A}_{i,i+1}$ appears in any of $\pi_{1,1}, \pi_{2,2}, \dots, \pi_{i,i}$. (19)

Let $\mathcal{A}_{i,i+1} = \{a_{i,1}, \dots, a_{i,m_i}\}$, and let $A_{i,h} = \sigma_{i,i+1}(a_{i,h})$. We now have $n = m_1 + m_2 + \dots + m_k$ extension variables, defined via

$$\text{ext} \downarrow \frac{a_{i,h}}{A_{i,h}} \quad \text{and} \quad \text{ext} \downarrow \frac{\bar{a}_{i,h}}{\bar{A}_{i,h}}$$

If we give the index pair (i, h) the lexicographic ordering, it immediately follows from (19) that condition (11) is fulfilled. Hence, we can trivially replace each instance of $\text{sub}\downarrow$ by a sequence of instances of $\text{ext}\downarrow$, whose number is bound by the size of the $B_{i,i+1}$. Hence, the size of the resulting eKS proof is at most quadratic in the size of π . \square

Note that the transformation in the proof of Theorem 6.3 does not involve any cuts. Hence, we have also proved the following:

Theorem 6.4. eKS p -simulates sKS.

Remark 6.5. The possible interest of sKS has already been mentioned in [5], but up to now it is unknown whether sKS can p -simulate eKS, although I conjecture this to be the case.

7. Pigeonhole principle and balanced tautologies

In this section we see two classes of tautologies which both admit polynomial-size proofs in eKS and sKS. The first one is the propositional pigeonhole principle. The second one is a variation which has the property that every member of the class is a balanced tautology. A formula A is *balanced* if every propositional variable occurring in A occurs exactly twice, once positive and once negated. For example,

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

is balanced (and a tautology), whereas

$$a \vee a \vee (\bar{a} \wedge \bar{a}) \quad \text{and} \quad a \wedge \bar{a} \wedge b$$

are not balanced. I use the notation $\bigwedge_{0 \leq i \leq n} F_i$ as abbreviation for $F_0 \wedge \dots \wedge F_n$, and similarly for \bigvee . Furthermore, for a literal a , I abbreviate the formula $a \vee \dots \vee a$ by a^n , if there are n copies of a . Consider now

$$\text{PHP}_n = \bigwedge_{0 \leq i \leq n} \bigvee_{1 \leq j \leq n} p_{i,j} \Rightarrow \bigvee_{0 \leq i < m \leq n} \bigvee_{1 \leq j \leq n} (p_{i,j} \wedge p_{m,j}) \quad (20)$$

This formula is called the propositional pigeonhole principle because it expresses the fact that if there are $n+1$ pigeons and only n holes and every pigeon is in a hole then at least one hole contains two pigeons, provided one reads the propositional variable $p_{i,j}$ as “pigeon i sits in hole j ”.

The formulas (20) have been well investigated from the viewpoint of proof complexity. In [9] they were presented as a candidate for separating Frege systems and extended Frege systems (w.r.t. p -simulation). But Buss [7] has shown that PHP_n admits a polynomial-size proof in a Frege system (and therefore in SKS) for every n .

I will here show that in eKS as well as in sKS we have cut-free polynomial-size proofs for (20). For this I use a new class of tautologies which also admit polynomial-size proofs in eKS, and which are defined as follows:

$$\text{QHQ}_n = \bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} \left[\bigvee_{1 \leq k \leq i} \bar{q}_{i,j,k} \vee \bigvee_{i < k \leq n} q_{k,j,i+1} \right] \quad (21)$$

Here are the first three examples:

$$\text{QHQ}_1 = q_{1,1,1} \vee \bar{q}_{1,1,1}$$

$$\begin{aligned} \text{QHQ}_2 = & ([q_{1,1,1} \vee q_{2,1,1}] \wedge [q_{1,2,1} \vee q_{2,2,1}]) \vee ([\bar{q}_{1,1,1} \vee q_{2,1,2}] \wedge [\bar{q}_{1,2,1} \vee q_{2,2,2}]) \\ & \vee ([\bar{q}_{2,1,1} \vee \bar{q}_{2,1,2}] \wedge [\bar{q}_{2,2,1} \vee \bar{q}_{2,2,2}]) \end{aligned}$$

$$\begin{aligned} \text{QHQ}_3 = & ([q_{1,1,1} \vee q_{2,1,1} \vee q_{3,1,1}] \wedge [q_{1,2,1} \vee q_{2,2,1} \vee q_{3,2,1}] \wedge [q_{1,3,1} \vee q_{2,3,1} \vee q_{3,3,1}]) \\ & \vee ([\bar{q}_{1,1,1} \vee q_{2,1,2} \vee q_{3,1,2}] \wedge [\bar{q}_{1,2,1} \vee q_{2,2,2} \vee q_{3,2,2}] \wedge [\bar{q}_{1,3,1} \vee q_{2,3,2} \vee q_{3,3,2}]) \\ & \vee ([\bar{q}_{2,1,1} \vee \bar{q}_{2,1,2} \vee q_{3,1,3}] \wedge [\bar{q}_{2,2,1} \vee \bar{q}_{2,2,2} \vee q_{3,2,3}] \wedge [\bar{q}_{2,3,1} \vee \bar{q}_{2,3,2} \vee q_{3,3,3}]) \\ & \vee ([\bar{q}_{3,1,1} \vee \bar{q}_{3,1,2} \vee \bar{q}_{3,1,3}] \wedge [\bar{q}_{3,2,1} \vee \bar{q}_{3,2,2} \vee \bar{q}_{3,2,3}] \wedge [\bar{q}_{3,3,1} \vee \bar{q}_{3,3,2} \vee \bar{q}_{3,3,3}]) \end{aligned}$$

The tautologies QHQ_n are balanced. This means that the size of a proof in KS (or related systems) of such a tautology is directly related to the number of applications of $\text{ac}\downarrow$. Furthermore, all proofs that we show here do not contain any weakening. This makes this class interesting for investigating the gap between linear logic and classical logic [20,22].

The formulas QHQ_1 and QHQ_2 are easily provable in $\text{KS} \setminus \{\text{ac}\downarrow\}$. One might be tempted to conjecture that $\text{KS} \setminus \{\text{ac}\downarrow\}$ or $\text{eKS} \setminus \{\text{ac}\downarrow\}$ is already complete for the class of balanced tautologies. But unfortunately, this is not the case. The smallest counterexample known to me is QHQ_3 . Every possible application of $\text{ai}\downarrow$, s , m , or $\text{w}\downarrow$ leads to a non-tautologous formula. Thus also the extension rule is of no use. (The same is true for all formulas QHQ_n with $n \geq 3$.)

This is not surprising under the view of the following theorem, which says that balanced tautologies are not easier to prove than other tautologies.

Theorem 7.1. *The set of balanced tautologies is **coNP**-complete.*

Proof. We can reduce provability of general tautologies to provability of balanced tautologies. For a formula B , we let B' be the formula obtained from B by doing the following replacement for every propositional variable a occurring in B : Let n be the number of occurrences of a in positive form in B , and let m be the number of occurrences of \bar{a} in B . If $n \geq 1$ and $m \geq 1$, then introduce $n \cdot m$ fresh propositional variables $a_{i,j}$ for $1 \leq i \leq n$ and $1 \leq j \leq m$. Now replace for every $1 \leq i \leq n$ the i th occurrence of a by $a_{i,1} \vee \dots \vee a_{i,m}$, and replace for every $1 \leq j \leq m$ the j th occurrence of \bar{a} by $\bar{a}_{1,j} \vee \dots \vee \bar{a}_{n,j}$. If $n = 0$, then introduce m fresh variables a_1, \dots, a_m and replace the j th \bar{a} by $\bar{a}_j \wedge a_j$. If $m = 0$, proceed similarly (cf. Footnote 3). Then B' is balanced, and its size is quadratic in the size of B . Furthermore, B' is a tautology if and only if B is a tautology. This can be seen as follows: Any KS-proof of B can be transformed into a KS-proof of B' by propagating the replacements of literals through the proof; atomic contractions $\text{ac}\downarrow$ are replaced by general contractions $\text{c}\downarrow$, and identities $\text{ai}\downarrow$ by weakenings and identities:

$$\text{ai}\downarrow \frac{F\{B\}}{F\{B \wedge [\bar{a} \vee a]\}} \quad \rightsquigarrow \quad (m+n-2)*\text{w}\downarrow \frac{\text{ai}\downarrow \frac{F\{B\}}{F\{B \wedge [\bar{a}_{1,j} \vee \dots \vee \bar{a}_{n,j}]\}}}{F\{B \wedge [\bar{a}_{1,j} \vee \dots \vee \bar{a}_{n,j} \vee a_{i,1} \vee \dots \vee a_{i,m}]\}}$$

Conversely, an SKS-proof of B' can be transformed into an SKS-proof of B by forgetting the indices and adding a sufficient number of contractions $\text{c}\downarrow$ and coweakenings $\text{w}\uparrow$

$$\begin{array}{ccc} F\{a \vee \dots \vee a\} & F\{\bar{a} \vee \dots \vee \bar{a}\} & \\ \text{c}\downarrow \parallel & \text{c}\downarrow \parallel & \text{w}\uparrow \frac{F\{\bar{a} \wedge a\}}{F\{a\}} \quad \text{w}\uparrow \frac{F\{\bar{a} \wedge a\}}{F\{\bar{a}\}} \\ F\{a\} & F\{\bar{a}\} & \end{array}$$

at the bottom of the derivation. (Thus, by coweakening-elimination, also a KS-proof of B' can be transformed into a KS-proof of B .) \square

Let us now reduce PHP_n to QHQ_n . We first replace the implication by disjunction and negation, and then apply associativity and commutativity of \vee :

$$\begin{aligned} \text{PHP}_n &= \bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} \bar{p}_{i,j} \vee \bigvee_{0 \leq i < n} \bigvee_{i < m \leq n} \bigvee_{1 \leq j \leq n} (p_{i,j} \wedge p_{m,j}) \\ &= \bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} \bar{p}_{i,j} \vee \bigvee_{0 \leq i \leq n} \bigvee_{1 \leq j \leq n} \bigvee_{i < m \leq n} (p_{i,j} \wedge p_{m,j}) \\ &= \bigvee_{0 \leq i \leq n} \left[\bigwedge_{1 \leq j \leq n} \bar{p}_{i,j} \vee \bigvee_{1 \leq j \leq n} \bigvee_{i < m \leq n} (p_{i,j} \wedge p_{m,j}) \right] \end{aligned}$$

Now consider the following class of formulas (where $\bar{p}_{i,j}^i$ abbreviates $\bar{p}_{i,j} \vee \dots \vee \bar{p}_{i,j}$ with i copies of $\bar{p}_{i,j}$):

$$\text{PHP}'_n = \bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} \left[\bar{p}_{i,j}^i \vee \bigvee_{i < m \leq n} p_{m,j} \right]$$

We have for each n a derivation from PHP'_n to PHP_n of length $O(n^3)$:

$$\begin{aligned} &= \frac{\text{PHP}'_n}{\bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} [\bar{p}_{i,j}^i \vee \bigvee_{i < m \leq n} p_{m,j}]} \\ &\quad \frac{n(n+1)/2*\text{ai}\downarrow}{\bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} [\bar{p}_{i,j}^i \vee \bigvee_{i < m \leq n} (\bar{p}_{i,j} \vee p_{i,j}) \wedge p_{m,j}]} \\ &\quad \frac{n(n+1)/2*s}{\bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} [\bar{p}_{i,j}^i \vee \bar{p}_{i,j}^{n-i} \vee \bigvee_{i < m \leq n} (p_{i,j} \wedge p_{m,j})]} \\ &= \frac{\bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} [\bar{p}_{i,j}^n \vee \bigvee_{i < m \leq n} (p_{i,j} \wedge p_{m,j})]}{\bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} [\bar{p}_{i,j} \vee \bigvee_{i < m \leq n} (p_{i,j} \wedge p_{m,j})]} \\ &\quad \frac{n(n+1)(n-1)*\text{ac}\downarrow}{\bigvee_{0 \leq i \leq n} \bigwedge_{1 \leq j \leq n} [\bar{p}_{i,j} \vee \bigvee_{i < m \leq n} (p_{i,j} \wedge p_{m,j})]} \\ &\quad \frac{n(n+1)*s}{\bigvee_{0 \leq i \leq n} [\bigwedge_{1 \leq j \leq n} \bar{p}_{i,j} \vee \bigvee_{1 \leq j \leq n} \bigvee_{i < m \leq n} (p_{i,j} \wedge p_{m,j})]} \\ &= \text{PHP}_n \end{aligned}$$

Remark 7.2. Since PHP'_n is just an instance of QHQ_n with $q_{i,j,k} = p_{i,j}$, every polynomial-size proof of QHQ_n yields also a polynomial-size proof of PHP_n . On the other hand, with the substitution (found by an anonymous referee)

$$p_{i,j} \mapsto \bigwedge_{1 \leq k \leq i} q_{i,j,k} \wedge \bigwedge_{i < k \leq n} \bar{q}_{k,j,i+1}$$

Fig. 4. Derivation from $\text{QH}Q_{n-1}$ to $\text{QH}Q_n$

⁵ To distinguish between the propositional variable occurrences in QHQ_n and the occurrences QHQ_{n-1} , we use q' for those in QHQ_{n-1} . This is more legible than adding yet another index to the q .

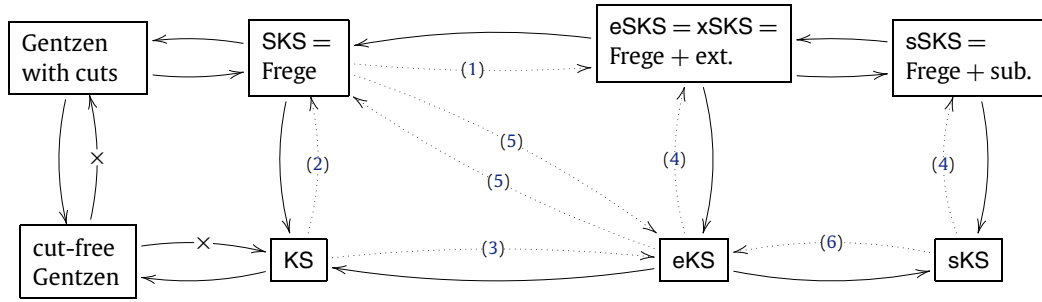


Fig. 5. Classification of propositional proof systems.

$$\text{ext} \downarrow \frac{q'_{i,j,k}}{[q_{i,j,k} \vee q_{n,j,k}] \wedge [\bar{q}_{n,j,i+1} \vee q_{i,n,k}]} \quad \text{ext} \downarrow \frac{\bar{q}'_{i,j,k}}{(\bar{q}_{i,j,k} \wedge \bar{q}_{n,j,k}) \vee (q_{n,j,i+1} \wedge \bar{q}_{i,n,k})} \quad (23)$$

In [17], Japaridze provides another cut-free polynomial-size proof of PHP_n . His system of *deep cirquents* uses a form of sharing instead of extension or substitution.

8. Conclusions and future work

This paper provides more new open problems than it provides answers. Fig. 5 shows a refined version of Fig. 2 (see also [5]). A solid arrow $A \longrightarrow B$ means that A p-simulates B , the notation $A \not\sim B$ means that A does not p-simulate B , and a dotted arrow $A \cdots \longrightarrow B$ means that it is not known whether A p-simulates B or not. The open problems indicated by these dotted arrows are surprisingly difficult:

1. The question whether SKS p-simulates eSKS is equivalent to the question whether Frege systems p-simulate extended Frege systems. This question has already been asked in [9], and is one of the most important open problems in the area of proof complexity.
2. I conjecture that KS does not p-simulate SKS (see also [5] and [6]).
3. I also conjecture that KS does not p-simulate eKS. More precisely, it is conjectured that KS cannot provide polynomial-size proofs of the formulas PHP_n (or QHQ_n), whereas this is possible in SKS (as shown in [7]) as well as in eKS (as shown in Section 7). However, so far, no technique has been developed for showing that something *cannot be done* in KS.
4. This is the question whether extension or substitution can simulate the behavior of the cut. It is one of the contributions of this paper that this question can now be asked. I conjecture that the answer is positive, but it is not clear how to prove it. Note that the naive cut elimination procedures fail in the presence of extension. Even if we manage to modify the technicalities such that we get a cut elimination procedure for eSKS, it is not clear how to avoid the exponential blow-up usually caused by cut elimination.
5. The questions whether extension without cut is as powerful as the cut without extension, and vice-versa, can be seen as the little brothers of (1).
6. It has already been shown in [9] that under the presence of cut substitution p-simulates extension, but without cut, this question is not trivial.

Remark 8.1. The general cocontraction rule $\text{c}\uparrow$ (see Proposition 3.5) can be reduced to its atomic version

$$\text{ac}\uparrow \frac{F\{a\}}{F\{a \wedge a\}}$$

if the medial rule m (see (1)) is present [4]. It has recently been shown [18,6] that the system $\text{KS} + \text{ac}\uparrow$ quasi-polynomially simulates SKS, and it is conjectured that this result can be improved to a polynomial simulation. Furthermore, one can show that sKS (and therefore also eKS) p-simulates $\text{KS} + \text{ac}\uparrow$. The two results together could provide an answer for one direction of (5). This also raises the question whether $\text{KS} + \text{ac}\uparrow$ can p-simulate eKS. In any case, we have here four ways of proof compression—cocontraction, cut, extension, and substitution—and they can all be studied independently in KS.

Acknowledgements

I thank Paola Bruscoli, Anupam Das, Alessio Guglielmi, and Tom Gundersen for fruitful discussions and helpful comments improving the readability of the paper.

References

- [1] M. Baaz, S. Hetzl, A. Leitsch, C. Richter, H. Spohr, Proof transformation by CERES, in: MKM'06, in: *Lecture Notes in Comput. Sci.*, vol. 4108, Springer, 2006, pp. 82–93.
- [2] M. Baaz, A. Leitsch, Towards a clausal analysis of cut-elimination, *J. Symbolic Comput.* 41 (3–4) (2006) 381–410.
- [3] K. Brännler, Deep inference and symmetry for classical proofs, Ph.D. thesis, Technische Universität Dresden, 2003.
- [4] K. Brännler, A.F. Tiu, A local system for classical logic, in: R. Nieuwenhuis, A. Voronkov (Eds.), *LPAR 2001*, in: *Lecture Notes in Artificial Intelligence*, vol. 2250, Springer, 2001, pp. 347–361.
- [5] P. Bruscoli, A. Guglielmi, On the proof complexity of deep inference, *ACM Trans. Comput. Log.* 10 (2) (2009) 1–34, article 14.
- [6] P. Bruscoli, A. Guglielmi, T. Gundersen, M. Parigot, A quasipolynomial cut-elimination procedure in deep inference via atomic flows and threshold formulae, in: *LPAR-16*, in: *Lecture Notes in Comput. Sci.*, vol. 6355, Springer-Verlag, 2010, pp. 136–153.
- [7] S.R. Buss, Polynomial size proofs of the propositional pigeonhole principle, *J. Symbolic Logic* 52 (4) (1987) 916–927.
- [8] A. Ciabattoni, A. Leitsch, Towards an algorithmic construction of cut-elimination procedures, *Math. Structures Comput. Sci.* 18 (1) (2008) 81–105.
- [9] S.A. Cook, R.A. Reckhow, The relative efficiency of propositional proof systems, *J. Symbolic Logic* 44 (1) (1979) 36–50.
- [10] A. Das, On the proof complexity of cut-free bounded deep inference, in: K. Brännler, G. Metcalfe (Eds.), *Automated Reasoning with Analytic Tableaux and Related Methods – 20th International Conference, TABLEAUX 2011*, in: *Lecture Notes in Comput. Sci.*, vol. 6793, Springer, 2011, pp. 134–148.
- [11] G. Gentzen, Untersuchungen über das logische Schließen. I, *Math. Z.* 39 (1934) 176–210.
- [12] A. Guglielmi, A system of interaction and structure, *ACM Trans. Comput. Log.* 8 (1) (2007) 1–64.
- [13] A. Guglielmi, L. Straßburger, Non-commutativity and MELL in the calculus of structures, in: L. Fribourg (Ed.), *Computer Science Logic, CSL 2001*, in: *Lecture Notes in Comput. Sci.*, vol. 2142, Springer-Verlag, 2001, pp. 54–68.
- [14] A. Haken, The intractability of resolution, *Theoret. Comput. Sci.* 39 (1985) 297–308.
- [15] D. Hilbert, Die logischen Grundlagen der Mathematik, *Math. Ann.* 88 (1922) 151–165.
- [16] D. Hilbert, W. Ackermann, *Grundzüge der theoretischen Logik*, Grundlehren Math. Wiss., vol. XXVII, Verlag von Julius Springer, 1928.
- [17] G. Japaridze, Cirquent calculus deepened, *J. Logic Comput.* 18 (6) (2008) 983–1028.
- [18] E. Jeřábek, Proof complexity of the cut-free calculus of structures, *J. Logic Comput.* 19 (2) (2009) 323–339.
- [19] J. Krajíček, P. Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations, *J. Symbolic Logic* 54 (3) (1989) 1063–1079.
- [20] F. Lamarche, Exploring the gap between linear and classical logic, *Theory Appl. Categ.* 18 (18) (2007) 473–535.
- [21] R. Statman, Bounds for proof-search and speed-up in predicate calculus, *Ann. Math. Logic* 15 (1978) 225–287.
- [22] L. Straßburger, On the axiomatisation of Boolean categories with and without medial, *Theory Appl. Categ.* 18 (18) (2007) 536–601.
- [23] L. Straßburger, Linear logic and noncommutativity in the calculus of structures, Ph.D. thesis, Technische Universität Dresden, 2003.
- [24] L. Straßburger, From deep inference to proof nets via cut elimination, *J. Logic Comput.* 21 (4) (2011), <http://dx.doi.org/10.1093/logcom/exp047>, first published online: August 10, 2009.
- [25] A.S. Troelstra, H. Schwichtenberg, *Basic Proof Theory*, 2nd edition, Cambridge University Press, 2000.
- [26] G.S. Tseitin, On the complexity of derivation in propositional calculus, *Zap. Nauchn. Semin. LOMI* 8 (1968) 234–259.