Linearization of proofs in propositional Hilbert systems

Karel Chvalovský

Institute of Computer Science, Academy of Sciences of the Czech Republic,
Pod Vodárenskou věží 271/2, 182 07 Prague 8, Czech Republic

e-mail: karel@chvalovsky.cz

December 5, 2012

Abstract

We show that any proof in a propositional Hilbert-style proof system with modus ponens as the only rule and B and B′ among axioms can be transformed into a linear proof. A proof is linear if only assumptions or instances of axioms are allowed as minor premises in modus ponens. Moreover, we show that if B or B′ is provable then we can add at most two axioms which ensure linearization, but do not change the set of provable formulae.

1 Introduction

Hilbert-style proof systems usually have only few deduction rules and many axioms. For numerous (non-classical) propositional logics and their proof systems the only needed rule is modus ponens. It means that substitution is in such cases handled implicitly. The rule of modus (ponendo) ponens says that from φ (the minor premise) and $\varphi \to \psi$ (the major premise) derive ψ. As there are usually more suitable choices for the actual proof search, Hilbert-style proof systems are most importantly used in metamathematics. For such purposes, it is sometimes useful that only some types of proofs have to be considered.

The motivation of this paper is to show that a natural class of linear proofs is sufficient to prove any provable formula in any propositional Hilbert-style proof system with modus ponens as the only rule and well known prefixing B and suffixing B′

(B) $(\varphi \to \psi) \to \big((\chi \to \varphi) \to (\chi \to \psi)\big)$

(B′) $(\varphi \to \psi) \to \big((\psi \to \chi) \to (\varphi \to \chi)\big)$

among axioms. We say that a proof is linear if we can take only assumptions or substitution instances of axioms as minor premises.

Furthermore, we show that it suffices to have any of these two axioms representing the transitivity of the implication together with another formula, which is provable from it, among axioms. Therefore if we have a system in which B or B′ is provable, then by adding at most two axioms we obtain a system which proves the very same formulae, but any provable formula has also a linear proof. This applies for many Hilbert-style proof systems, as B or B′ is provable in numerous propositional logics—from very weak to intuitionistic and classical logic.

The basic idea is presented in Figure 1, where proofs are shown as labelled trees, see Definition 2.2. We have a proof of r in p, $p \to q$, and $q \to r$ which is not linear. However, using the axiom B we can transform it into a linear proof. Similarly we can use the axiom B′, see Figure 2.

Although we are interested in the rule of modus ponens, we use C. A. Meredith's condensed detachment, see [3, 1], which combines modus ponens with substitution, in order to simplify some technical issues. Namely, we can get rid of substitutions in our proofs.

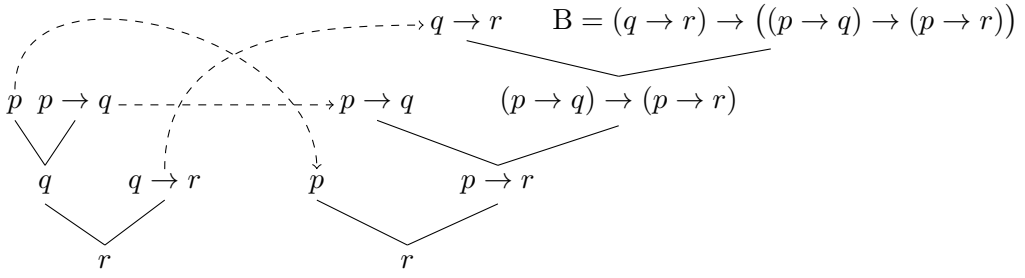

Figure 1: Linearization of proofs using B

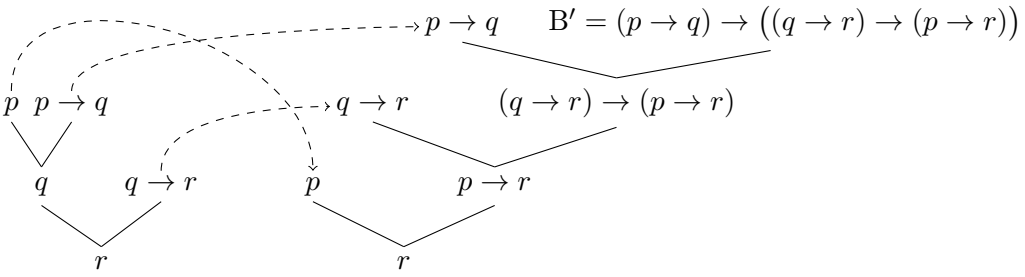

Figure 2: Linearization of proofs using B′

1.1 Outline of this paper

Necessary definitions are given in Section 2. In Section 3 we show how to transform any proof into a linear proof using B and B′. The following section studies some other formulae suitable for the linearization of proofs. We show that is suffices to have B′ and a formula, later called B'_1, which is itself provable using only B′, to linearize proofs. In Section 5 we present a set of formulae $\mathcal{B}(n, m)$, for $n, m > 0$, which generalize B and all have linear proofs using B and B′. We can use these formulae to transform a linear proof of φ and linear proof of $\varphi \to \psi$ into a linear proof of ψ in the similar way as in Figure 1. Hence we obtain an alternative method for transforming general proofs into linear proofs. In Section 6 we show that B and a formula, later called $\mathcal{B}(2) = \mathcal{B}(2, 1)$ and provable using only B, are sufficient to prove any $\mathcal{B}(n, m)$, for $n, m > 0$. In Section 7 we show that for any proof $\mathcal{P}$ there is a formula which encodes the structure of $\mathcal{P}$ and have a linear proof using B and B′. The consequences for proof systems with the rule of modus ponens instead of condensed detachment are discussed in Section 8.

2 Preliminaries

Some basic notions from the theory of logical calculi are used. Let us fix a countably infinite set of variables *Var* and define the set of formulae *Fml* as usual given that the only connective we are interested in is the implication. Nevertheless, all the results hold even in setting with other connectives as long as modus ponens (condensed detachment) is the only deduction rule. To shorten notation, we usually associate parentheses to the right, e.g. $p \to q \to r$ is strictly speaking $(p \to (q \to r))$.

A *substitution* σ is a function $\sigma\colon \mathit{Var} \to \mathit{Fml}$. We say that a substitution σ is a *renaming* if $\sigma\colon \mathit{Var} \to \mathit{Var}$ is a bijection. The result of an application of a substitution σ on a formula φ, denoted $\sigma(\varphi)$, and composition of substitutions is defined as usual. A formula ψ is a *variant of a formula* φ, abbreviated by $\psi \equiv \varphi$, if there is a renaming σ such that $\psi = \sigma(\varphi)$, i.e. $\varphi = \sigma^{-1}(\psi)$. Moreover, we say that a substitution σ is a *variant of a substitution* δ if

there is a renaming θ such that $\sigma = \delta \circ \theta$, i.e. $\delta = \sigma \circ \theta^{-1}$.

A *unification* of a set of formulae $F = \{\varphi_1, \ldots, \varphi_n\}$ is such a substitution σ that $\sigma(\varphi_1) = \cdots = \sigma(\varphi_n)$. If such a substitution exists we say that F is unifiable. Due to the Unification Theorem of Robinson [4], for any unifiable set of formulae F there exists a most general unifier of F. A *most general unifier* (m.g.u.) σ of F is such a unification that for any other unification δ of F, there is a substitution θ such that $\sigma \circ \theta = \delta$. All the most general unifiers, if they exist, are the same up to renaming—they are variants of each other. Since this difference will be unimportant for us we shall write the m.g.u. instead of a m.g.u.

2.1 Hilbert-style proof systems

Hilbert-style proof systems usually consist of a set of many axioms and few deduction rules. The only axioms we are interested in are related to the transitivity of the implication.

In our paper we discuss two deduction rules: modus ponens and condensed detachment. When having modus ponens there are two basic ways how to handle substitutions. Usually the set of axioms is understood as a set of axiom schemata, meaning they are closed under substitutions, so called implicit substitution. The other way is to have substitution as an explicit rule. However, there is one more approach, which enables us to virtually get rid of substitutions in our proofs. We can use the rule of condensed detachment by C.A. Meredith, see [3, 1], which combines the rule of modus ponens with the minimal amount of substitution.

2.1.1 The rule of condensed detachment

Roughly speaking, the rule of condensed detachment gives us the most general formula we can obtain from φ and $\chi \to \psi$ by modus ponens using necessary substitutions. However, some technical details have to be solved.

Definition 2.1 (Condensed Detachment)**.** Let us have two formulae φ and $\chi \to \psi$. We produce a variant of φ called φ', which does not have a common variable with $\chi \to \psi$. If there is the m.g.u. σ of φ' and χ, then produce a variant σ' of σ such that no new variable in $\sigma'(\chi)$ occurs in ψ. The condensed detachment of φ and $\chi \to \psi$ is $\sigma'(\psi)$. Otherwise, the condensed detachment of φ and $\chi \to \psi$ is not defined.

It is evident that the condensed detachment of φ and $\chi \to \psi$ is defined uniquely up to variants (renaming) and for this purpose we shall handle formulae which are variants of each other as the same formulae without mentioning this fact explicitly.

Moreover, we shall slightly abuse the fact that only the structure of a formula is important, and not the exact names of variables. Therefore, we use the same variable name in several formulae during proofs although these variables are not the same, but meaning should be clear from the context.

As substitution is contained in the rule of condensed detachment there is no need to have axioms closed under substitutions. This means that our prefixing B and suffixing B′ are defined as:

(B) $(p \to q) \to (r \to p) \to r \to q$

(B′) $(p \to q) \to (q \to r) \to p \to r$

Definition 2.2. A **D**-*proof* of a formula φ is a finite rooted tree labelled by formulae such that the root is labelled by φ, leaves are labelled by axioms, and if a non-leaf node is labelled by ψ then χ and $\xi \to \theta$ are all its children such that the condensed detachment of χ and $\xi \to \theta$ is ψ. We say that a proof is linear if χ can only be a leaf.

We call a formula φ (linear) **D**-provable if there is a (linear) **D**-proof of φ. Linear **D**-proofs can be written as $\alpha_1(\alpha_2(\ldots(\alpha_{n-1}\alpha_n)\ldots))$, where α_i, $1 \le i \le n$, are axioms. As all parentheses are superfluous in such notation we shall omit them and write just $\alpha_1\alpha_2\ldots\alpha_n$. In the same sense we shall use this notation also for derivations, where α_i are general formulae not necessarily axioms. Sometimes we shall also use α^n meaning $\underbrace{\alpha\ldots\alpha}_{n}$.

Let us emphasize that axioms play the crucial role in this paper. Nevertheless, the only requirement we have is that some particular axioms are included. Therefore, we do not talk about axioms explicitly. We only specify which axioms are required—φ has a linear proof using B and B′ means that an implicit set of axioms contains B and B′.

2.1.2 The rule of modus ponens

As our main aim is to discuss more common systems with modus ponens we provide some standard definitions. Contrary to the systems with the rule of condensed detachment, which itself includes substitution, we incorporate substitution into the definition of proof. Thus we in fact understand axioms as axiom schemata.

Definition 2.3. An **MP**-*proof* of a formula φ in a theory Γ is a finite rooted tree labelled by formulae such that the root is labelled by φ, leaves are labelled by substitution instances of axioms or members of Γ, and if a non-leaf node is labelled by ψ then χ and $\chi \to \psi$ are all its children. We say that a proof is linear if χ can only be a leaf.

Let us emphasize that in the definition of **D**-proof we don't allow theories, because we shall not need them. We call a formula φ (linear) **MP**-provable in Γ if there is a (linear) **MP**-proof of φ in Γ. We say that a formula φ is (linear) **MP**-provable if φ is (linear) **MP**-provable in $\emptyset$. The same notation for writing linear **MP**-proofs is imposed as for **D**-proofs.

The classical result, probably first explicitly shown in [2], connects **D**-provability and **MP**-provability for systems with the same set of axioms.

Theorem 2.1. *Let $\mathcal{P}$ be an* **MP**-*proof in $\Gamma = \emptyset$. Then there is a* **D**-*proof $\mathcal{P}'$ such that every step in $\mathcal{P}$ is a substitution instance of a step in $\mathcal{P}'$.*

The opposite direction, which is more important for our purposes, comes easily from the fact that the rule of condensed detachment can be simulated by modus ponens and substitution, which can be easily propagated to the leaves.

Lemma 2.2. *If φ has a (linear)* **D**-*proof then any substitution instance of φ has a (linear)* **MP**-*proof.*

Although we use only condensed detachment in the following sections, all the proofs can be directly restated and proved taking modus ponens as the only rule, see Section 8. However, the implicit handling of substitutions by the rule of condensed detachment makes our proofs simpler. Therefore, with the exception of Section 8, we use words proof and provable instead of **D**-proof and **D**-provable.

3 Linearization of proofs using B and B′

In this section we show that any proof can be easily transformed into a linear proof using the axioms B and B′. Let us remark that we use words proof and provable instead of **D**-proof and **D**-provable in this and the following sections as condensed detachment is our only deduction rule.

First, we show that given a proof of φ which is the condensed detachment of ψ and χ, where ψ has a linear proof and χ is an axiom (leaf), we can obtain a linear proof of φ. This provides a linearization of the most basic non-linear proofs. Therefore we directly generalize constructions in Figures 1 and 2.

Lemma 3.1. *Let $n > 0$ and α_i, for $1 \leq i \leq n$, and β be axioms. If $(\alpha_1 \dots \alpha_n)\beta$ is a proof of φ then there is a linear proof of φ using* B′.

Proof. We prove it by induction on n. If $n = 1$ we already have a linear proof. Let us have $n > 1$ and assume that the lemma holds for $n - 1$. We already know that $\alpha_1\beta(\alpha_2 \dots \alpha_n)\mathrm{B}'$ is a proof of φ, see Figure 2. By the induction hypothesis there is a linear proof of $(\alpha_2 \dots \alpha_n)\mathrm{B}'$ and hence a linear proof of φ. It follows that $\alpha_1\beta\alpha_2\mathrm{B}' \dots \alpha_n\mathrm{B}'$ is a linear proof of φ. □

The next and main step provides a construction which enables us to obtain a linear proof of φ from a proof of φ, where φ is obtained in the last step by the rule of condensed detachment from ψ and χ which both have linear proofs.

Lemma 3.2. *Let $n > 0$, $m > 0$, and α_i, for $1 \leq i \leq n$, and β_j, for $1 \leq j \leq m$, be axioms. If $(\alpha_1 \dots \alpha_n)\beta_1 \dots \beta_m$ is a proof of φ then there is also a linear proof of φ using* B *and* B′.

Proof. We prove it by induction on n. If $n = 1$ then we already have a linear proof. Let us have $n > 1$ and assume that the lemma holds for $n - 1$. Using the transformation from Figure 1 we get that $\alpha_1(\alpha_2 \dots \alpha_n)(\beta_1 \dots \beta_m)\mathrm{B}$ is a proof of φ. Using Lemma 3.1 there is a linear proof $\mathcal{P}$ of $(\beta_1 \dots \beta_m)\mathrm{B}$ and hence using the induction hypothesis on $(\alpha_2 \dots \alpha_n)\mathcal{P}$ we get also a linear proof of φ. □

Note. It is evident that in the previous lemma we can also use B′ instead of B, for $n > 2$, and thus sometimes obtain a shorter proof—an application of Lemma 3.1 on a proof roughly doubles its length.

Corollary 3.3. *Let ψ and $\chi \to \theta$ have linear proofs and the condensed detachment of ψ and $\chi \to \theta$ be φ. Then φ has a linear proof using* B *and* B′.

We immediately obtain the main theorem of this section which says that any proof can be transformed into a linear one using axioms B and B′.

Theorem 3.4. *Any proof of φ can be transformed into a linear proof of φ using* B *and* B′.

Proof. Let us have a proof $\mathcal{P}$ of φ with depth d. As proofs are labelled trees, we can identify a vertex v with a sub-tree (proof) which has v as its root. All vertexes (if exist) of depth d and $d-1$ are linear proofs. If there is any vertex v of depth $d-2$ which is not a linear proof then its children are linear proofs. So we can use Corollary 3.3 to obtain a linear proof v' and we can replace v by v'. This way we transform $\mathcal{P}$ into a new proof $\mathcal{P}'$. Although using the previous construction the depth of $\mathcal{P}'$ can grow significantly the number of nodes which are not linear proofs decrease by one. As the original proof $\mathcal{P}$ has a finite number of (such) vertexes we finaly obtain a linear proof. □

Corollary 3.5. *Let $\mathcal{A}$ be a set of axioms in which* B *and* B′ *are provable. Then any formula φ provable using $\mathcal{A} \cup \{\mathrm{B}, \mathrm{B}'\}$ has a proof using $\mathcal{A}$ and linear proof using $\mathcal{A} \cup \{\mathrm{B}, \mathrm{B}'\}$.*

4 Linear proofs using B′ and B'_1

In this paper we do not address the length of linear proofs at all. However, as all the proofs are constructive it is not difficult to obtain some upper bounds. Obviously such considerations depend on the given set of axioms. Since our motivations are metamathematical, we study simple axioms rather than axioms providing the shortest possible proofs. Nevertheless, an obvious example of an axiom which provides shorter proofs is

(B'_1) $(p \to q \to r) \to (s \to q) \to p \to s \to r$

The idea behind the use of the axiom B'_1 is in Figure 3, cf. Figures 1 and 2. It is easy to check that $(\mathrm{B}'\mathrm{B}')\mathrm{B}'\mathrm{B}'$ is a proof of B'_1. Actually, the axiom B'_1 gives us an alternative proof of Lemma 3.2.

Lemma 4.1. *Let $n > 0$, $m > 0$, and α_i, for $1 \leq i \leq n$, and β_j, for $1 \leq j \leq m$, be axioms. If $(\alpha_1 \dots \alpha_n)\beta_1 \dots \beta_m$ is a proof of φ then there is also a linear proof of φ using* B′ *and* B'_1.

Proof. We prove it by induction on n. If $n = 1$ then we already have a linear proof. If $m = 1$ then we can use Lemma 3.1. Let us have $n, m > 1$ and assume that the lemma holds for $n - 1$. Using the transformation from Figure 3 we get that $\alpha_1\beta_1(\alpha_2 \dots \alpha_n)(\beta_2 \dots \beta_m)\mathrm{B}'_1$ is a proof of φ. Using Lemma 3.1 there is a linear proof $\mathcal{P}$ of $(\beta_2 \dots \beta_m)\mathrm{B}'_1$ and hence using the induction hypothesis on $(\alpha_2 \dots \alpha_n)\mathcal{P}$ we get also a linear proof of φ. □

Theorem 4.2. *Any proof of φ can be transformed into a linear proof of φ using* B′ *and* B'_1.

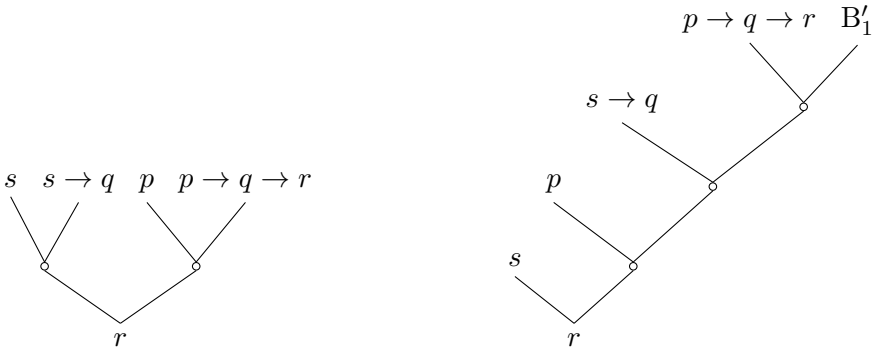

Figure 3: Linearization of proofs using B'_1

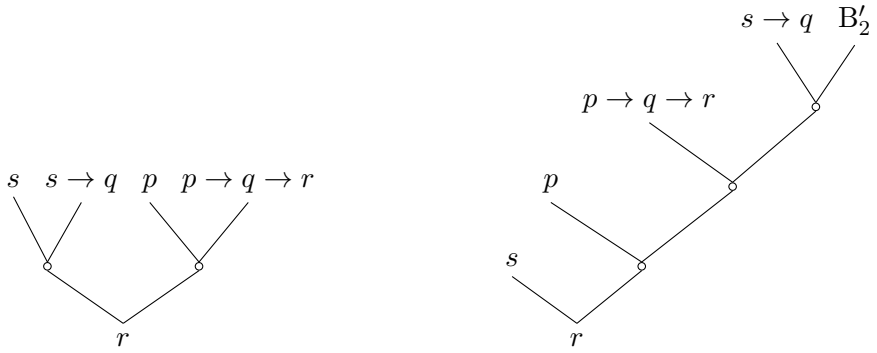

Figure 4: Linearization of proofs using B'_2

Let us remark that the previous theorem is obtained similarly to Theorem 3.4. We would like to emphasize that we used only Lemmata 3.1 and 4.1. These lemmata require axioms B' and B'_1. As B'_1 is provable using B', we can add B' and B'_1 as axioms into any system in which B' is provable without obtaining new provable formulae.

Corollary 4.3. *Let $\mathcal{A}$ be a set of axioms in which B' is provable. Then any formula φ provable using $\mathcal{A} \cup \{\mathrm{B}', \mathrm{B}'_1\}$ has a proof using $\mathcal{A}$ and linear proof using $\mathcal{A} \cup \{\mathrm{B}', \mathrm{B}'_1\}$.*

Likewise, we can obtain other axioms. The axiom B'_2, which is $\mathrm{BB}'\mathrm{B}'$, offers transformations as in Figure 4.

(B'_2) $(s \to q) \to (p \to q \to r) \to p \to s \to r$

Thus we can "switch" $\alpha_2 \dots \alpha_n$ and $\beta_2 \dots \beta_m$ in the proof of Lemma 4.1 which can produce shorter proofs if $m < n$. More importantly, we can also use B'_3, which is $\mathrm{B}'_2\mathrm{B}'_2\mathrm{B}'_2$, see Figure 5.

(B'_3) $(p \to t) \to (s \to q) \to (t \to q \to r) \to p \to s \to r$

We can now directly linearize $(\alpha_2 \dots \alpha_n)(\beta_2 \dots \beta_m)\mathrm{B}'_1$ in the proof of Lemma 4.1 starting by $\alpha_2\beta_2\mathrm{B}'_1(\alpha_3 \dots \alpha_n)(\beta_3 \dots \beta_m)\mathrm{B}'_3$ and then using B'_3 repeatedly.

Obviously, we can effectively combine all these three new axioms in the proof of Lemma 4.1. Similarly, we can propose other analogous axioms—an inspiration can be found also in the rest of this paper. An obvious example would be formulae which enable us to make more linearization steps in a single step, cf. formulae defined in the following section.

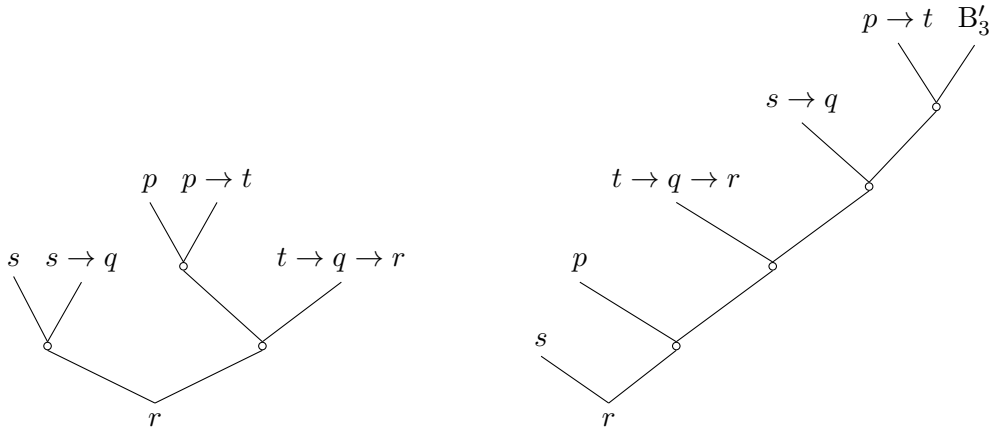

Figure 5: Linearization of proofs using B'_3

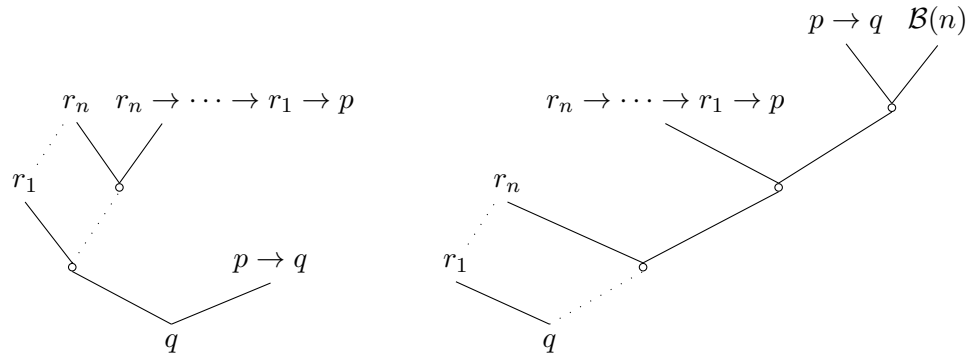

Figure 6: Linearization of proofs using $\mathcal{B}(n)$

5 Generalizations of the axiom B

The linearization in Section 3 was based on Lemmata 3.1 and 3.2, where we construct a linear proof using B′ and B, respectively. However, we can define sets of formulae which generalize the axiom B and directly linearize proofs as in Lemmata 3.1 and 3.2.

Let us define a set of formulae $\mathcal{B}(n)$, which resemble more general prefixing, and show that all of them have linear proofs.

Definition 5.1. Let $n > 0$ then we define a formula $\mathcal{B}(n)$ as

$$(p \to q) \to (r_n \to \cdots \to r_1 \to p) \to r_n \to \cdots \to r_1 \to q$$

We see that $\mathcal{B}(1)$ is B. The idea behind $\mathcal{B}(n)$ is to make transformation in Figure 6 possible. Thus we have to take all $\mathcal{B}(n)$ as axioms or prove that they have linear proofs.

Lemma 5.1. *Let $n > 0$ then the formula $\mathcal{B}(n)$ has a linear proof using* B *and* B′*.*

Proof. We know that $\mathcal{B}(1)$ is B. For $n > 1$ evidently holds that $\mathcal{B}(k)\mathcal{B}(l)$B, if $k + l = n$, for any $k, l > 0$, is a proof of $\mathcal{B}(n)$. Therefore B$\mathcal{B}(n-1)$B is a proof of $\mathcal{B}(n)$ and $\mathcal{B}(n-1)$B has a linear proof by Lemma 3.1. □

Using the previous lemma we can show that the application of condensed detachment on a formula which has a linear proof and an axiom produces a formula which also has a linear proof. In different words, it is an alternative to Lemma 3.1.

Lemma 5.2. *Let $n > 0$ and α_i, for $1 \leq i \leq n+1$, and β be formulae. If $(\alpha_1 \dots \alpha_{n+1})\beta$ is a proof of φ then $\alpha_1 \dots \alpha_n \alpha_{n+1} \beta \mathcal{B}(n)$ is also a proof of φ.*

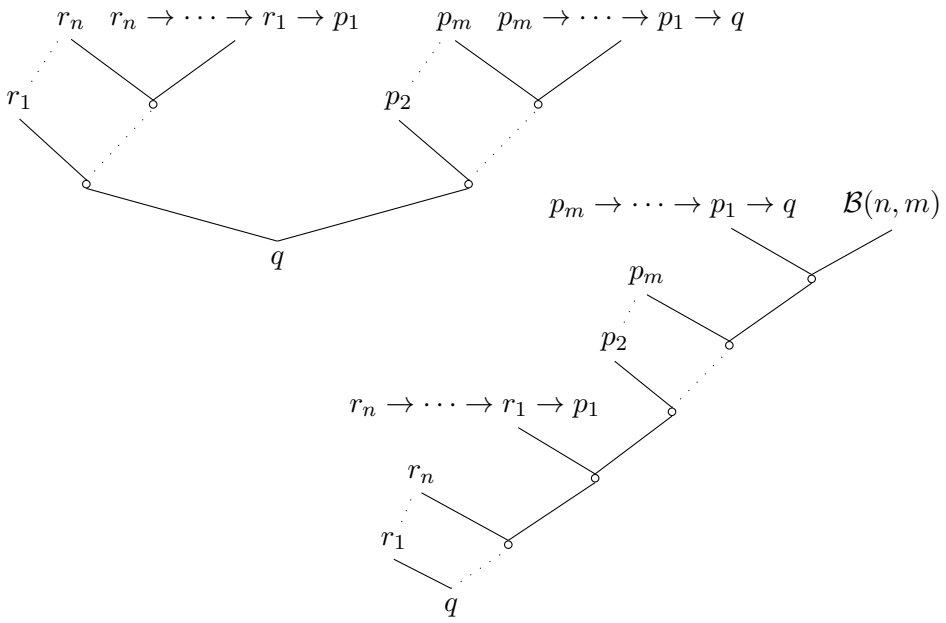

Figure 7: Linearization of proofs using $\mathcal{B}(n,m)$

Proof. The formula $\mathcal{B}(n)$ is used just to encode the proof. Let us have any $n > 0$ and assume that $p, q, r_1, \ldots, r_n$ do not occur in $\alpha_1, \ldots, \alpha_{n+1}, \beta$. The following pairs have to be unified:

$$\{\beta, p \to q\}, \{\alpha_{n+1}, r_n \to \cdots \to r_1 \to p\}, \{\alpha_n, r_n\}, \ldots, \{\alpha_1, r_1\}$$

From the shape of $(\alpha_1 \ldots \alpha_{n+1})\beta$, see Figure 6, all these unifications are possible. Thus $\mathcal{B}(n)$ ensures that the result of $(\alpha_1 \ldots \alpha_{n+1})\beta$, namely φ, is unified with q as Figure 6 shows. □

A generalization of the previous lemma follows. First, we define one more set of formulae $\mathcal{B}(n,m)$ and then prove it works as we need.

Definition 5.2. Let $n > 0$ and $m > 0$ then we define a formula $\mathcal{B}(n,m)$ as

$$(p_m \to \cdots \to p_1 \to q) \to p_m \to \cdots \to p_2 \to (r_n \to \cdots \to r_1 \to p_1) \to r_n \to \cdots \to r_1 \to q$$

It is easy to see that $\mathcal{B}(n,1)$ is $\mathcal{B}(n)$. The main point is that $\mathcal{B}(n,m)$ enables us to transform the condensed detachment of two formulae with linear proofs into a linear proof of the resulting formula. In different words, we can make the transformation in Figure 7 and therefore provide an alternative to Lemma 3.2.

Lemma 5.3. *Let $n > 0$ and $m > 0$ then the formula $\mathcal{B}(n,m)$ has a linear proof using* B *and* B′.

Proof. Let us have $n > 0$ and $m > 0$. It is easy to see that we can prove $\mathcal{B}(n,m)$ using $(\ldots(\mathcal{B}(n)\underbrace{B)\ldots\mathrm{B}}_{m-1})$. As $\mathcal{B}(n)$ has a linear proof by Lemma 5.1 it suffices to use $(m-1)$-times Lemma 5.2 (or 3.1). □

Lemma 5.4. *Let $n > 0$, $m > 0$, and α_i, for $1 \leq i \leq n+1$, and β_j, for $1 \leq j \leq m$, be formulae. If $(\alpha_1 \ldots \alpha_{n+1})\beta_1 \ldots \beta_m$ is a proof of φ then $\alpha_1 \ldots \alpha_{n+1}\beta_1 \ldots \beta_m\mathcal{B}(n,m)$ is also a proof of φ.*

Proof. The formula $\mathcal{B}(n,m)$ is again used just to encode the proof. The proof is similar to Lemma 5.2 with the only exception that the following pairs have to be unified:

$$\{\beta_m, p_m \to \cdots \to p_1 \to q\}, \{\beta_{m-1}, p_m\}, \ldots, \{\beta_1, p_2\},$$
$$\{\alpha_{n+1}, r_n \to \cdots \to r_1 \to p_1\}, \{\alpha_n, r_n\}, \ldots, \{\alpha_1, r_1\}$$

All these unifications are possible given $(\alpha_1 \ldots \alpha_{n+1})\beta_1 \ldots \beta_m$ is possible and all the variables occurring in $\mathcal{B}(n,m)$ do not occur in $\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_m$. It follows that the result of $(\alpha_1 \ldots \alpha_{n+1})\beta_1 \ldots \beta_m$, namely φ, unifies with q. □

As a consequence of this lemma we can easily (as in Theorem 3.4) show that any proof can be transformed into a linear proof if we have B and B′ among axioms and condensed detachment as the only deduction rule.

We claimed that we obtained alternatives to Lemmata 3.1 and 3.2, but we used these lemmata in our proofs. This will be clarified in the following section.

6 Linear proofs using B and $\mathcal{B}(2)$

Clearly, any formulae $\mathcal{B}(n)$ and $\mathcal{B}(n,m)$ are provable using B. An obvious question to ask is whether they have linear proofs using only B. This is not the case as it is easy to show that B^6 proves the very same formula as B^{10} and hence there are only finitely[1] many formulae (up to variants) provable by linear proofs from B.

If we take all $\mathcal{B}(n)$ as axioms we obtain a system which proves the very same formulae as the system with the only axiom B. However, as the previous section shows it suffices to have linear proofs of all $\mathcal{B}(n)$ to prove that any provable formula has a linear proof, because we then obtain linear proofs of all $\mathcal{B}(n,m)$. An immediate question is whether there is a finite set of formulae which has the same properties. We show that it suffices to have $B = \mathcal{B}(1)$ and $\mathcal{B}(2)$, namely

$$(p \to q) \to (s \to r \to p) \to s \to r \to q,$$

to prove every $\mathcal{B}(n)$ using only linear proofs.

We define three sets of auxiliary formulae $\varphi(n)$, $\psi(n)$, and $\chi(n)$, which all have linear proofs using B and $\mathcal{B}(2)$.

Definition 6.1. For $n > 0$ we define the formula $\varphi(n)$ as

$$(p_0 \to q) \to (p_1 \to r_1 \to p_0) \to \cdots \to (p_n \to r_n \to p_{n-1}) \to p_n \to r_n \to \cdots \to r_1 \to q$$

and by abuse of notation $\varphi(0)$ be the empty string.

Let us remark we sometimes write that we apply a formula φ on a formula ψ. This usually means $\varphi\psi$ as we are looking for linear proofs. The following proofs are not difficult, but tend to be too technical and tedious. Therefore they will only be indicated briefly.

Lemma 6.1. *For $n > 0$ we have that $\mathcal{B}(2)^{\frac{n(n+1)}{2}}$ is a proof of $\varphi(n)$.*

Proof. For $n = 1$ we have $\mathcal{B}(2)$ which is $\varphi(1)$. Let us assume that the lemma holds for n. Then we have to prove that $\mathcal{B}(2)^{n+1}\varphi(n)$ is a proof of $\varphi(n+1)$.

Applying $\mathcal{B}(2)$ on $\varphi(n)$ we get

$$(p_1 \to r_1 \to p \to q) \to (p_2 \to r_2 \to p_1) \to \cdots \to (p_n \to r_n \to p_{n-1}) \to$$
$$p_n \to r_n \to \cdots \to r_1 \to (s \to r \to p) \to s \to r \to q$$

[1] Clearly, if modus ponens is our deduction rule then there are infinitely many provable formulae due to substitutions. However, as no $\mathcal{B}(n+1)$ is a substitution instance of $\mathcal{B}(n)$ it also holds that only $\mathcal{B}(1)$, $\mathcal{B}(2)$, and $\mathcal{B}(3)$ have linear proofs using B as the only axiom. These proofs are B, B^3, and B^8, respectively.

Let us note that similar result does not hold for B′. Let us define $\theta(n)$, for $n > 0$, as $(p \to q) \to (((\ldots(q \to r_1)\ldots) \to r_n) \to ((\ldots(p \to r_1)\ldots) \to r_n))$ if n is odd and $(p \to q) \to (((\ldots(p \to r_1)\ldots) \to r_n) \to ((\ldots(q \to r_1)\ldots) \to r_n))$ if n is even. It is easy to prove that B'^{2^n-1} is $\theta(n)$.

and another application leads to $\varphi(2)$, for $n = 1$, or

$$(p_2 \to r_2 \to p \to q) \to (p_3 \to r_3 \to p_2) \to \cdots \to (p_n \to r_n \to p_{n-1}) \to \\ p_n \to r_n \to \cdots \to r_2 \to (p \to u \to v) \to (s \to r \to p) \to s \to r \to u \to q$$

It is not difficult to see that repeating this we get that $\mathcal{B}(2)^{n+1}\varphi(n)$ is $\varphi(n+1)$. □

Definition 6.2. For $n > 1$ we define the formula $\psi(n)$ as

$$(p_1 \to p_0) \to (p_2 \to p_1) \to \cdots \to (p_n \to p_{n-1}) \to p_n \to p_0$$

Lemma 6.2. *For $n > 1$ we have that $\mathrm{B}^{n-1}\varphi(n-2)$ is a proof of $\psi(n)$.*

Proof. For $n = 2$ we see that $\psi(2)$ is B. Otherwise, let us have $\mathrm{B}\varphi(n-2)$ which is

$$(p_1 \to r_1 \to p \to q) \to (p_2 \to r_2 \to p_1) \to \cdots \to (p_{n-2} \to r_{n-2} \to p_{n-3}) \to \\ p_{n-2} \to r_{n-2} \to \cdots \to r_1 \to (r \to p) \to r \to q$$

Now we see that $\mathrm{B}^2\varphi(1)$ is $\psi(3)$ and generally that repeating the application of B for $(n-1)$-times gives us $\psi(n)$. □

Definition 6.3. For $n > 0$ we define the formula $\chi(n)$ as

$$(p \to q \to r) \to p \to (s_{2n} \to \cdots \to s_1 \to q) \to s_{2n} \to \cdots \to s_1 \to r$$

Lemma 6.3. *For $n > 0$ we have that $\mathcal{B}(2)^n\psi(n+1)$ is a proof of $\chi(n)$.*

Proof. We immediately see that $\mathcal{B}(2)\psi(2)$ is $\chi(1)$. Let us take $\mathcal{B}(2)\psi(m)$, for $m > 2$, which is

$$(p_2 \to p \to q) \to (p_3 \to p_2) \to \cdots \to (p_m \to p_{m-1}) \to p_m \to (s \to r \to p) \to s \to r \to q$$

and we see that the repeated application of $\mathcal{B}(2)$ for $(m-1)$-times leads to $\chi(m-1)$. □

The previous construction leads to the lemma we are looking for, which is a trivial consequence of the fact that all $\chi(n)$, for $n > 0$, have linear proofs.

Lemma 6.4. *For any $n > 0$ the formula $\mathcal{B}(n)$ has a linear proof using* B *and $\mathcal{B}(2)$.*

Proof. As $\mathcal{B}(1) = \mathrm{B}$ and $\mathcal{B}(2)$ are axioms we only need to show that the theorem holds for $n > 2$. Let $m > 1$ then we immediately see that $\mathrm{B}\chi(m-1)$ is $\mathcal{B}(2m-1)$ and $\mathcal{B}(2)\chi(m-1)$ is $\mathcal{B}(2m)$. □

In the very same way as in the previous section we now can prove any $\mathcal{B}(m,n)$, as only $\mathcal{B}(n)$ and B are needed. Thus any proof can be transformed into a linear one using only B and $\mathcal{B}(2)$, which can be proved from B.

Theorem 6.5. *Any proof of φ can be transformed into a linear proof of φ using* B *and $\mathcal{B}(2)$.*

Corollary 6.6. *Let $\mathcal{A}$ be a set of axioms in which* B *is provable. Then any formula φ provable in $\mathcal{A} \cup \{\mathrm{B}, \mathcal{B}(2)\}$ has a proof in $\mathcal{A}$ and linear proof in $\mathcal{A} \cup \{\mathrm{B}, \mathcal{B}(2)\}$.*

7 A special form of linearization

The previous constructions of linear proofs have the property that axioms used to transform a proof occur between leaves of the original proof. We show using B and B′ that we can produce a linear proof which does not have this property.

The following construction is based on the properties of B and B′ demonstrated in Figures 1 and 2. Namely, the order of leaves is preserved using B, but B′ makes an alteration in the order of leaves possible. These properties of B and B′ are crucial in the following construction.

Theorem 7.1. *If φ has a non-linear proof $\mathcal{P}$ and $\alpha_1, \ldots, \alpha_n$ are all leaves in $\mathcal{P}$ from left to right then there is a linear proof $\alpha_1 \ldots \alpha_n \beta_1 \ldots \beta_m$ of φ, where β_i, for $1 \leq i \leq m$, are only* B *or* B′.

Proof. The proof is similar to Theorem 3.4, but we have to change the construction in order to ensure that our invariant holds.

We have two linear proofs $\gamma_1 \ldots \gamma_k \ldots \gamma_{k'}$ and $\delta_1 \ldots \delta_l \ldots \delta_{l'}$ which prove some formulae ψ_1 and ψ_2. The condensed detachment of these formulae is ψ. We want a linear proof of ψ with properties given by the theorem. Meaning $\gamma_1, \ldots, \gamma_k, \delta_1, \ldots, \delta_l$ is a subsequence of $\alpha_1, \ldots, \alpha_n$ and $\gamma_{k+1}, \ldots, \gamma_{k'}, \delta_{l+1}, \ldots, \delta_{l'}$ are B or B′. Thus there is i such that $\alpha_i = \gamma_1, \ldots, \alpha_{i+k-1} = \gamma_k$ and $\alpha_{i+k} = \delta_1, \ldots, \alpha_{i+k+l-1} = \delta_l$. Moreover, we can assume that $k > 1$ and $l > 0$.

Let us assume that $l' = l = 1$. Hence $\gamma_1 \ldots \gamma_{k-1}(\gamma_k \ldots \gamma_{k'})\delta_1\mathcal{B}(k-1)$ is a proof of ψ. If $k = k'$ we are done. Otherwise $\gamma_1 \ldots \gamma_k(\delta_1\mathcal{B}(k-1))(\gamma_{k+1} \ldots \gamma_{k'})$B′ and $\gamma_1 \ldots \gamma_k\delta_1\mathcal{B}(k-1)((\gamma_{k+1} \ldots \gamma_{k'})$B′$)$B are also proofs of ψ. This case is completed by using our standard argument to find a linear proof of $\mathcal{B}(k-1)((\gamma_{k+1} \ldots \gamma_{k'})$B′$)$B, which only consists of B and B′.

For $l' > 1$ the argument requires one more step. We can use the previous construction, but instead of δ_1 we now have $\delta_1 \ldots \delta_l \ldots \delta_{l'}$. Thus we have $\gamma_1 \ldots \gamma_k(\delta_1 \ldots \delta_l \ldots \delta_{l'})\chi$, where χ is some proof which consists only of B and B′. If $l' = l$ then we can prove $(\delta_1 \ldots \delta_l)\chi$ by $\delta_1 \ldots \delta_l\chi\mathcal{B}(l-1)$ and find a linear proof of $\chi\mathcal{B}(l-1)$. If $l' > l$ then we prove $(\delta_1 \ldots \delta_l \ldots \delta_{l'})\chi$ by $\delta_1 \ldots \delta_l(\delta_{l+1} \ldots \delta_{l'})\chi\mathcal{B}(l)$ and find a linear proof of $(\delta_{l+1} \ldots \delta_{l'})\chi\mathcal{B}(l)$, which consists only of B and B′. □

The previous theorem in other words says that for any proof $\mathcal{P}$ there is a formula with a linear proof using B and B′ which faithfully encodes the structure of $\mathcal{P}$.

Corollary 7.2. *If φ has a proof $\mathcal{P}$ and $\alpha_1, \ldots, \alpha_n$ are all leaves in $\mathcal{P}$ from left to right then there exists $m \geq 0$ and a sequence $\beta_1, \ldots, \beta_m$ of axioms* B *and* B′ *such that $\alpha_1 \ldots \alpha_n \beta_1 \ldots \beta_m$ is a linear proof of φ.*

Corollary 7.3. *If φ has a proof $\mathcal{P}$ and $\alpha_1, \ldots, \alpha_n$ are all leaves in $\mathcal{P}$ from left to right then there is a formula ψ such that $\alpha_1 \ldots \alpha_n \psi$ is a proof of φ and ψ has a linear proof using only* B *and* B′.

8 The rule of modus ponens

In this section all the results are restated in the setting with the only deduction rule being modus ponens. However, this is not difficult as we know that we can simulate the rule of condensed detachment by the rules of modus ponens and substitution. Moreover, all the substitutions can be propagated to the leaves of a proof. Therefore it suffices to have the implicit substitution.

The only difference is that we can have assumptions. However, all of them occur in our transformed proofs only as minor premises and therefore all the proofs with modus ponens work analogously to the proofs with condensed detachment. It follows that we can in a fairly straightforward way restate all the previous results.

To simplify notation, we use in the whole section provability and proof instead of **MP**-provability and **MP**-proof. Let us also assume that we have any of the following pairs among axioms

- B and B′,
- B′ and B'_1, or
- B and $\mathcal{B}(2)$

as we proved in the previous sections that any of them is sufficient for linearization.

Corollary 8.1. *If φ and $\varphi \to \psi$ have linear proofs in Γ then ψ has a linear proof in Γ.*

Corollary 8.2 (Theorems 3.4, 4.2, and 6.5)**.** *If φ has a proof in Γ then there is a linear proof of φ in Γ.*

Let us note that the (new) linear proof has the same number of occurrences of axioms/premises as the original proof with the exception of the axioms needed for the linearization itself.

Corollary 8.3. *If φ is provable in Γ then there is a sequence $\psi_1, \ldots, \psi_n$ of assumptions or substitution instances of axioms such that $\psi_1 \to \cdots \to \psi_n \to \varphi$ is an assumption or substitution instance of an axiom.*

All the previous statements hold if any of three given pairs of formulae is among axioms. The following corollary, which is a more special version of the previous one, requires both the axioms B and B′.

Corollary 8.4 (Theorem 7.1)**.** *Let $\psi_1, \ldots, \psi_n$ be the sequence of leaves from right to left in a non-linear proof of φ in Γ. Then there is $m \geq 0$ and a sequence $\chi_1, \ldots, \chi_m$ of substitution instances of axioms* B *and* B′ *such that $\chi_1 \to \cdots \to \chi_m \to \psi_1 \to \cdots \to \psi_n \to \varphi$ is a substitution instance of an axiom.*

Corollary 8.5. *Let $\psi_1, \ldots, \psi_n$ be the sequence of leaves from right to left in a non-linear proof of φ in Γ. Then $\psi_1 \to \cdots \to \psi_n \to \varphi$ has a linear proof using* B *and* B′.

Acknowledgements

The author would like to thank to Anupam Das for some useful discussions and Emil Jeřábek for calling author's attention to Corollary 8.3. The work was supported by grant P202/10/1826 of the Czech Science Foundation and by the long-term strategic development financing of the Institute of Computer Science (RVO 67985807).

References

[1] J. Roger Hindley and David Meredith. Principal type-schemes and condensed detachment. *Journal of Symbolic Logic*, 55(1):90–105, 1990.

[2] J. A. Kalman. Condensed detachment as a rule of inference. *Studia Logica*, 42(4):443–451, 1983.

[3] E. J. Lemmon, C. A. Meredith, D. Meredith, A. N. Prior, and I. Thomas. *Calculi of pure strict implication.* Canterbury University College, 1956.

[4] J. A. Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12(1):23–41, January 1965.